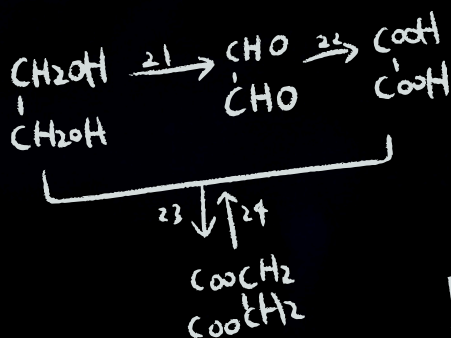


EMERGING TRENDS IN

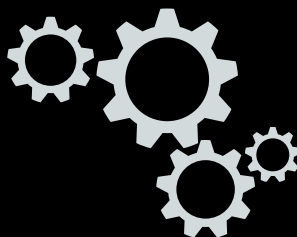
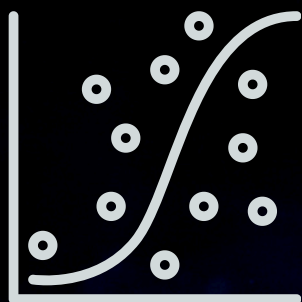
SCIENCE & TECHNOLOGY

VOL - 1

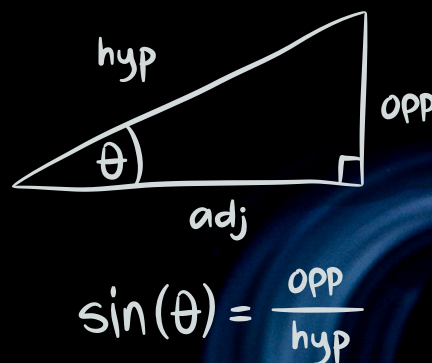
JUNE 2026



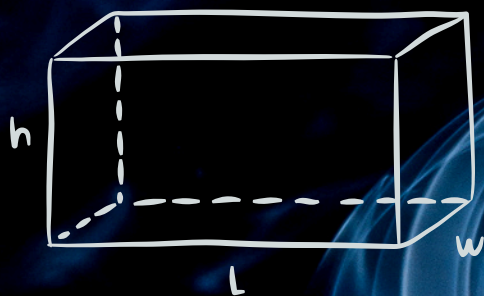
$$F = \frac{Gm_1m_2}{r^2}$$



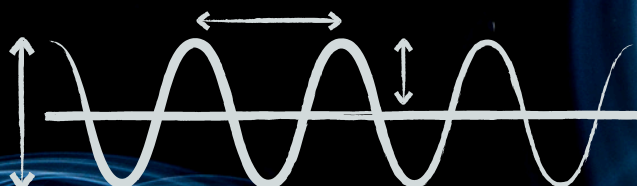
$$E = m \cdot c^2$$



$$W = Fd \cos(\theta)$$



$$V = Lwh$$



DR. DEENA NATH GUPTA

EDITOR IN CHIEF



JPTM



JPTM PUBLICATIONS

Emerging Trends in Science and Technology

Vol-1

Edited By

Dr. Deena Nath Gupta

Associate Professor

Maharishi School of Engineering and Technology,
Maharishi University of Information Technology, Noida

JPTM PUBLICATIONS

(A UNIT OF JPTM EDUCATION, RESEARCH & PUBLICATION SERVICES)

Barhaj, Deoria, U.P.– 274601, India

Website: www.jptm.in

Copyright

Copyright © 2026 JPTM PUBLICATIONS

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the publisher or individual author. Any person who does an unauthorised act in relation to this publication may be liable to criminal prosecution and civil claims for damages.

Book Details

Title: Emerging Trends in Science and Technology Vol-1

Editor: Dr. Deena Nath Gupta

Volume: First

Month and Year: June, 2026

ISBN (Print): 978-81-999970-0-4

ISBN (Online / PDF / eBook): 978-81-999970-1-1

Language: English

DOI: 10.67389/jptm.0626.etstv1

Publisher

JPTM PUBLICATIONS

(A UNIT OF JPTM EDUCATION, RESEARCH & PUBLICATION SERVICES)

Barhaj, Deoria, U.P.– 274601, India

Website: www.jptm.in

Email: publisher@jptm.in

Printing

Printed and bound in India.

Printed at: Tech Udyam Solutions Private Limited (Printster.in),

S-548A, 1st Floor, School Block,

Shakarpur, Laxmi Nagar,

Delhi, 110092, India

Price : Rs. 899/-

First published in 2026

Disclaimer

The views expressed by the authors in the book published by JPTM Publications (a unit of JPTM EDUCATION, RESEARCH & PUBLICATION SERVICES), Barhaj, Deoria, U.P. – 274601, India, are their own. They do not necessarily reflect the views of the publishers, and the editors will not be responsible in any way for any liability arising from the content/text of the book.

About the Series

Emerging Trends in Science and Technology is an edited volume that presents contemporary research, innovative methodologies, and technological advancements across diverse domains of science, engineering, and interdisciplinary studies. The book serves as a comprehensive platform for researchers, academicians, industry professionals, and students to explore recent developments that address current scientific and technological challenges.

The chapters included in this volume cover a broad spectrum of topics, including artificial intelligence, machine learning, Internet of Things (IoT), cybersecurity, data science, cloud computing, sustainable technologies, communication systems, advanced computing, and other emerging areas that are shaping the future of research and innovation. Each contribution has been carefully reviewed to ensure scientific rigor, originality, and practical relevance.

By bringing together insights from experts across multiple disciplines, this volume fosters knowledge exchange, promotes interdisciplinary collaboration, and highlights novel approaches to solving real-world problems. The book aims to inspire future research, support academic learning, and contribute to the advancement of science and technology for sustainable societal development. It is intended to serve as a valuable reference for researchers, educators, practitioners, policymakers, and students seeking an up-to-date understanding of emerging technological trends and their transformative impact on society.

Dr. Deena Nath Gupta
Editor-in-Chief, JPTM Publications
Editor, Emerging Trends in Science and Technology

Preface

It is with profound pride and great enthusiasm that I present the inaugural volume of the edited book, **Emerging Trends in Science and Technology**, published under the banner of **JPTM Publications**. This volume represents more than the publication of a scholarly work; it marks the beginning of a long-term academic endeavour dedicated to fostering excellence in research, promoting intellectual collaboration, and disseminating knowledge that addresses the evolving challenges of science, technology, engineering, and allied disciplines.

The twenty-first century has witnessed unprecedented scientific discoveries and technological innovations that continue to redefine the boundaries of human knowledge. Emerging technologies such as artificial intelligence, machine learning, quantum computing, cybersecurity, sustainable energy systems, advanced materials, biotechnology, the Internet of Things, robotics, and data-driven decision-making are transforming industries, economies, and societies worldwide. In this dynamic landscape, the role of scholarly publications has become increasingly significant in bridging theoretical advancements with practical applications and encouraging interdisciplinary collaboration.

Recognizing this need, **JPTM Publications** was established with the vision of becoming a trusted global platform for high-quality academic publishing. Our mission is to encourage original research, facilitate the exchange of innovative ideas, and support researchers, educators, professionals, and students in advancing knowledge that contributes to scientific progress and societal development. We aspire to publish scholarly books, edited volumes, monographs, textbooks, conference proceedings, and other academic resources that uphold the highest standards of integrity, quality, and intellectual rigor.

This inaugural volume, **Emerging Trends in Science and Technology**, embodies that vision. It brings together ten carefully selected chapters authored by distinguished academicians, researchers, and professionals from diverse institutions and disciplines. Each contribution presents contemporary research, emerging methodologies, innovative applications, and future perspectives in its respective field. Collectively, these chapters provide readers with a comprehensive overview of current scientific and technological advancements while encouraging interdisciplinary thinking and collaborative research.

One of the defining characteristics of this volume is the diversity of perspectives represented by its contributors. The chapters reflect the rapidly evolving nature of scientific inquiry and demonstrate how collaboration across disciplines can generate meaningful solutions to complex global challenges. Whether addressing theoretical foundations, experimental investigations, computational techniques, engineering innovations, or practical implementations, each chapter contributes to a broader understanding of the transformative role of science and technology in shaping a sustainable and knowledge-driven future.

The publication of this volume also marks the beginning of a continuing series dedicated to emerging areas of research. JPTM Publications envisions developing a vibrant repository of scholarly works that serve as reliable references for researchers, faculty members, postgraduate and undergraduate students, policymakers, industry practitioners, and innovators across the globe. Through rigorous editorial practices, transparent peer review, ethical publishing standards, and a commitment to academic excellence, we aim to build a publication ecosystem that is respected by the international research community.

As Editor, I express my heartfelt appreciation to all contributing authors whose dedication, expertise, and scholarly commitment have made this volume possible. Their valuable contributions reflect the spirit of curiosity, innovation, and academic excellence that this publication seeks to promote. I also

extend my sincere gratitude to the reviewers, whose constructive comments and meticulous evaluations have significantly enhanced the quality and credibility of the chapters.

My sincere thanks are due to the editorial board, language editors, technical support team, and publication staff of JPTM Publications for their unwavering dedication throughout the editorial and production process. Their collective efforts have ensured that this inaugural volume meets professional publishing standards while maintaining the highest level of academic integrity.

While every reasonable effort has been made to ensure the accuracy and authenticity of the content presented in this volume, the views, interpretations, methodologies, and conclusions expressed in individual chapters remain the responsibility of their respective authors. The Editor and Publisher encourage scholarly dialogue and constructive criticism as essential elements of academic progress.

As we celebrate the publication of this first volume, we also look toward the future with optimism and determination. JPTM Publications remains committed to supporting researchers across disciplines, encouraging emerging scholars, promoting interdisciplinary collaborations, and contributing to the global advancement of science and technology through impactful scholarly publishing. We envision this volume as the first step in a journey that will continue to inspire innovation, nurture academic excellence, and create lasting contributions to the worldwide research community.

It is my sincere hope that this book will stimulate new ideas, inspire meaningful research, foster collaborative initiatives, and serve as a valuable resource for readers across academia, industry, and research organisations. We warmly welcome constructive feedback from our readers and contributors, as it will guide us in continually enhancing the quality and impact of our future publications.

I dedicate this inaugural volume to the global community of researchers, educators, innovators, and lifelong learners whose relentless pursuit of knowledge continues to shape a better, more sustainable, and technologically empowered world.

Dr. Deena Nath Gupta
Editor-in-Chief, JPTM Publications
Editor, Emerging Trends in Science and Technology

Acknowledgement

The successful completion of this inaugural edited volume, **Emerging Trends in Science and Technology**, has been possible through the collective efforts, dedication, and unwavering support of numerous individuals and institutions. It is with deep gratitude that I acknowledge their invaluable contributions.

First and foremost, I extend my sincere appreciation to all the contributing authors who accepted our invitation to share their scholarly work in this volume. Their commitment to academic excellence, innovative research, and timely cooperation has been instrumental in shaping this book. Each chapter reflects the authors' expertise, intellectual curiosity, and dedication to advancing knowledge in their respective fields.

I am equally grateful to the reviewers for their careful evaluation of the submitted manuscripts. Their insightful comments, constructive suggestions, and commitment to maintaining high academic standards have significantly enhanced the quality, clarity, and scholarly value of the chapters included in this volume.

I wish to express my heartfelt gratitude to the Editorial Board and the entire team of **JPTM Publications** for their dedication and professionalism throughout the editorial and publication process. Their coordinated efforts in manuscript management, technical editing, language refinement, formatting, proofreading, and production have transformed a collection of individual manuscripts into a cohesive scholarly publication.

The publication of this book marks an important milestone in the journey of **JPTM Publications**. I sincerely thank all well-wishers, advisors, academic collaborators, and members of the research community who have encouraged and supported our vision of establishing a publishing platform dedicated to promoting high-quality scholarly research. Their confidence in our mission continues to inspire us to pursue excellence in academic publishing.

I also acknowledge the institutions with which the contributing authors are affiliated for fostering an environment that supports research, innovation, and academic collaboration. Such institutional encouragement plays a vital role in the advancement of scientific inquiry and knowledge dissemination.

My sincere appreciation is extended to the readers, researchers, educators, students, and professionals who will engage with this volume. We hope that the ideas presented in these chapters will stimulate meaningful discussions, inspire future investigations, and contribute to the continued advancement of science and technology.

Finally, on behalf of **JPTM Publications**, I express our commitment to maintaining the highest standards of ethical publishing, academic integrity, and editorial excellence. We look forward to strengthening collaborations with scholars across disciplines and publishing future volumes that contribute meaningfully to the global body of knowledge.

To everyone who has directly or indirectly contributed to the realisation of this inaugural publication, I offer my heartfelt thanks and sincere appreciation.

Dr. Deena Nath Gupta
Editor-in-Chief, JPTM Publications
Editor, Emerging Trends in Science and Technology

Contents

S.No.	Chapter	Page No
1.	Human-Robot Co-Working in Enterprises - A Security Walkthrough Dr. Deena Nath Gupta	1-8
2.	Sustainable IoT Systems Enabled by Supercapacitor Integration Neha Taneja, Aakash Dhingra, Yogesh Kumar	9-16
3.	EchoMesh: A Decentralized Off-Grid LoRa Mesh Communication System for Emergency and Remote Connectivity Aditya Tripathi, Durgesh Tiwari	17-24
4.	Infocognitive Dynamics Framework: A Unified Paradigm for Data Science and Big Data Analytics Ram Dutt Rikhari	25-36
5.	Real-Time Vehicle RC Expiry Detection and Smart Challan System Using YOLOv8 and OCR Saurabh Mallik, Shivangi Sharma, Mohd Tajammul	37-46
6.	Health Impacts with Social Factors of Chitrak (Plumbago zeylanica): An Analysis of Ayurvedic herb with Economic Perspective in Indian Society and Healthcare 5.0 Dr. Preeti Sharma, Dr. Rohit Rastogi, Dr. Bhavna Singh, Sandeep Kumar, Gunjan Nagar, Prashant Rathore	47-66
7.	Resilience-Aware Fuzzy Optimization for Cyber Forensic Evidence Reconstruction under Adversarial Uncertainty Charles Sagayaraj A. C., Santha Sheela A. C., Ramesh M	67-79
8.	Integrating Digital Forensic Readiness Into Educational Technology: A Framework For Secure Ai-driven Learning Environments Shivajee Pandey	80-84
9.	Enhancing Cybersecurity Through UI/UX Design Anisha Das	85-94
10.	Artificial Intelligence: Foundations and Algorithms Durgesh Tiwari, Kush Yadav	95-102

Human-Robot Co-Working in Enterprises - A Security Walkthrough

Dr. Deena Nath Gupta

Maharishi School of Engineering and Technology, Maharishi University of Information Technology, Noida,
Gautam Buddha Nagar, Uttar Pradesh 201304, India
prof.dev.cse@gmail.com

ARTICLE INFO

Article history:

Received 03 May 2026

Accepted 25 June 2026

Available online 12 July 2026

Keywords:

Industry 4.0

Industry 5.0

Enterprise Architecture Framework

Human-Robot Co-working

Artificial Intelligence

ABSTRACT

It is widely believed that the fourth industrial revolution is just around the corner. During Industry 4.0, there was a theme of "Smart Manufacturing for the Future". Some futurists are already discussing what the theme will be of the fifth industrial revolution. It is emerging that humans and robots can work together. A significant amount of progress has been made in the field of robotics and artificial intelligence (AI) in the last few years. A promising example of this trend is testing autonomous cars in traffic. There are Enterprises with robots or AI applications that keep employee records. Despite the abundance of studies on human-robot collaboration for low-level tasks with a focus on robot development, only few studies examine organizational issues arising from the collaboration of humans and robots. The purpose of this study is to discuss possible issues related to human-robot co-working from the perspective of both the Enterprise and the workforce. Several studies focusing on organizational robotics are expected to be influenced by the issues identified in this report.

1. Introduction

A major purpose of an industrial revolution is to separate human workforce from that of the machines. Machines will eventually do the hard, boring, or dangerous jobs that human cannot handle. These machines can also be referred as "robots". Cleaning robots, for instance, can easily take care of cleaning a room or an office in an Enterprise. In the near future, all cleaning jobs will be performed by robots. While we are at a point where both robots and human are able to do cleaning, past experiences suggest that human will do less cleaning in the future than robots. Technology level and human acceptance of robots play a major role in the pace of automation diffusion in Enterprises [1]. Studying the interactions between humans and robots, as well as the implications of their effects on organisation, is crucial because of the possible significant impacts of robots on Enterprises. A lot of research interest has been generated by Industry 4.0 since its introduction in 2011 [2]. Additionally, a number of scholars and futurists have already begun discussing the concept of Industry 5.0. A number of different visions have been presented for Industry 5.0. Human-robot collaboration is one of the emerging themes. There can be no certainty as to what the theme

of Industry 5.0 will be at this time. In spite of this, human-robot co-working will be a significant innovation for Enterprises and will have an impact on organisations in a significant way [3].

In the past three centuries, organisations have experienced three industrial revolutions. Most people now believe that we are in the midst of the fourth. These revolutions are depicted in figure 1 as a timeline. In the past few decades, the time span between revolutions has shortened. The first three revolutions happened 100 years apart. The fourth one was only reached after 40 years from the third. Within 40 years, there is a possibility of reaching the fifth level. The German government initiated Industry 4.0. During Industry 4.0, there was a theme of "Smart Manufacturing for the Future". As with previous revolutions, its objective is to increase productivity and achieve mass production through innovative technologies. Several trending technologies help make Industry 4.0 a reality. The internet of things (IoT), robotics, and artificial intelligence (AI), as well as big data and cloud computing are among the most trending trends today. Additionally, Industry 4.0 is supported by other technologies. Some of these technologies include 3D printing, virtual and augmented reality, smart

factories, smart logistics, and ambient intelligence. The technologies described here were not developed specifically for Industry 4.0, rather these technologies are brought together to create smart manufacturing as part of the vision for Industry 4.0. Industry 4.0 has also

been criticized for being a top-down government initiative with a predefined concept [4].

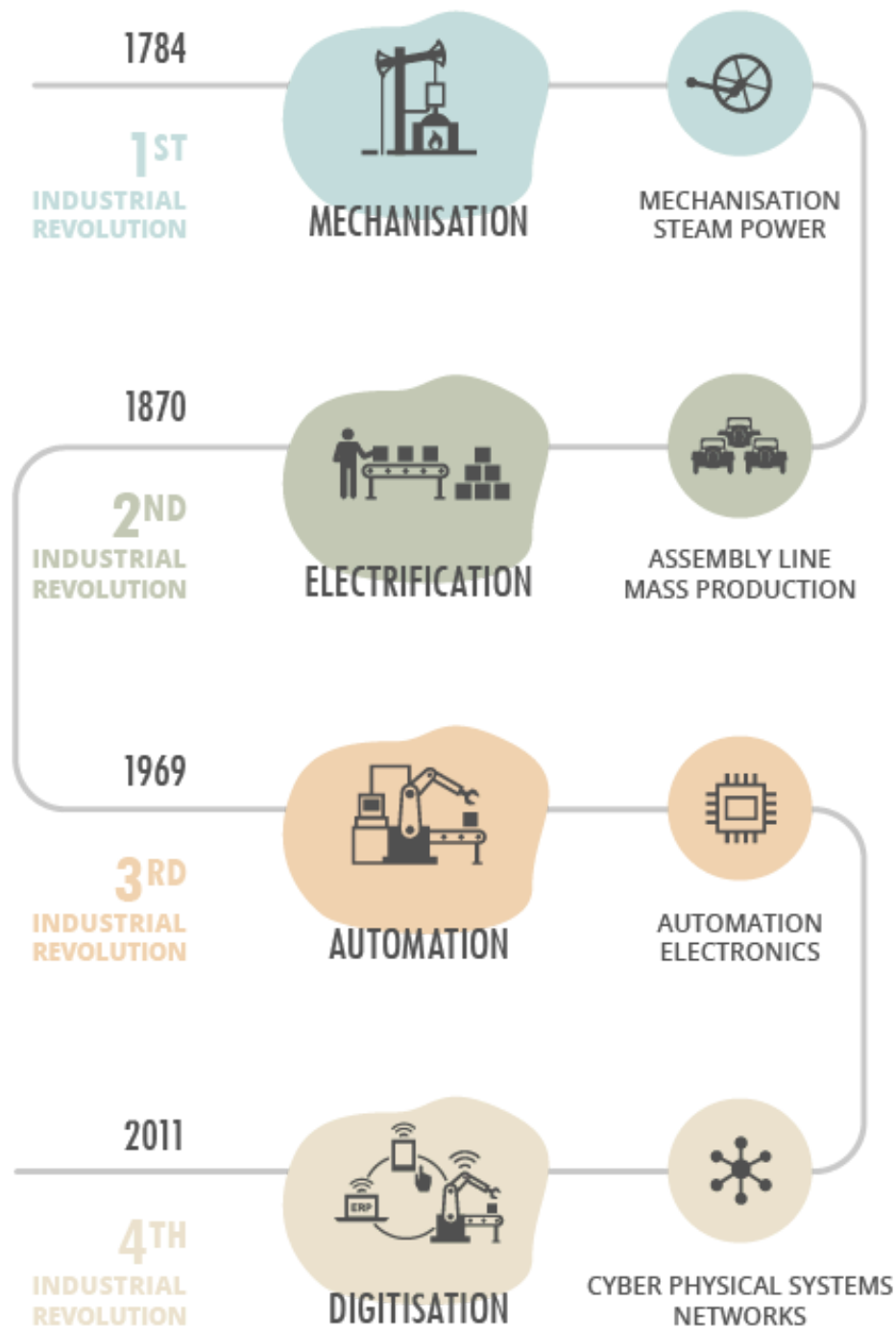


Figure 1: Will the 5th Industrial Revolution be the next Renaissance? [5]

Currently, two visions for Industry 5.0 are emerging. One of them is “human-robot co-working”. The goal with this vision is to have robots and humans work together whenever and wherever possible. Efforts requiring creativity will be handled by humans, while the rest will be taken by robots. A second vision for Industry 5.0 is the bioeconomy [6]. An eco-friendly, industrial, and economic balance can be achieved by using biological resources for industrial purposes. Biological economy is defined by the European Commission as “the production and conversion of renewable biological resources and waste streams into value-added products, such as food, feed, biobased products, and bioenergy.” Agricultural production, forestry, fisheries, food, pulp and paper production, chemical production, biotechnology production, and energy production are all included in this category. Since they utilize a wide range of scientific disciplines (life sciences, agronomy, ecology, food science, and social sciences), enabling and industrial technologies

(biotechnology, nanotechnology, information and communication technologies (ICT), and engineering), as well as local and tacit knowledge, its sectors are highly innovative [7].

The bioeconomy is based on the principle of biologization, which has the potential to change industries fundamentally. In consequence, it is possible that bioeconomy will play a major role in the next industrial revolution. In Table 1, we compare the concepts of Industry 4.0 and Industry 5.0. An important distinction is that Industry 5.0 may apply to both human-robot co-workers and bioeconomists [8]. Furthermore, other topics like space life, space industries, and space mining, may also occur in the near future. Space resource utilization is already being cautioned by scientists. It might become the next “gold rush”.

TABLE 1
A Comparison of Industry 4.0 and Industry 5.0 Visions [9]

	Industry 4.0	Industry 5.0 (Vision 1)	Industry 5.0 (Vision 2)
Percept	Smart Manufacturing	Human-Robot Co-working	Bioeconomy
Stimulus	Mass Production	Smart Society	Sustainability
Energy Supplier	Electrical power Fossil-based fuels Renewable power sources	Electrical power Renewable power sources	Electrical power Renewable power sources
Applied Mechanism	Internet of Things (IoT) Cloud Computing Big Data Robotics and Artificial Intelligence (AI)	Human-Robot Collaboration Renewable Resources	Sustainable Agricultural Production Bionics Renewable Resources
Experimentation Domain	Organizational Research Process Improvement and Innovation Business Administration	Smart Environments Organizational Research Process Improvement and Innovation Business Administration	Agriculture Biology Waste Prevention Process Improvement and Innovation Business Administration Economy

2. State-of-the-Art

The integration of robots into organizations has been discussed in previous studies. There are a number of issues to consider, including evolving organizational behaviors, structures, workflows, ethics, and work environments. A number of important matters need to be addressed, including: acceptance of robots in the workplace, discrimination against robots or people, privacy and trust in co-working spaces for humans and robots, re-designing the work environments for robots, education, and training. A significant amount of change is anticipated in organizations as a result of the issues identified. Issues related to integrating robots into organizations are elaborated in figure 2.

Working with robots presented organizational

challenges to Bagdasarov and her colleagues [10]. There were three sets of factors discussed: individual, organizational, and robotic agents. According to the authors, various factors should be considered under each set. An employee's age, gender, level of education, knowledge and experience of technology, their expectations, and their social perceptiveness/interpersonal sensitivity are factors that affect them as individuals. There are a number of organizational factors to consider, including workflow, physical environment, social/emotional context, training, and employee-robot goals alignment. Factors that determine the performance of robotic agents include the robot's appearance, behavior, ability to interact, and safety.



Figure 2: Issues related to integrating robots into organizations

3. Identified issues in Human-Robot Co-working

The authors identified 11 emerging issues in enterprises related to human-robot co-working. It is important to note that some issues have implications for both the organization and the individual. Clearly distinguishing organizational issues from personal ones

can be difficult. All the 11 issues are described in subsequent subsections.

3.1. Issues related to Administration

In one definition, a robot is a machine that responds to stimuli, thinks about them, and acts on them. Despite its simplicity, this definition is problematic. What does being a robot mean when it comes to thinking and acting? A robot, according to the Oxford dictionary, is a machine that performs complex actions

automatically, especially one programmable by computers. According to the Merriam Webster dictionary, a robot is a machine that imitates the functions of a human being (such as walking or talking). Furthermore, these definitions pose problems as well. One relies on vague concepts such as carrying out complicated actions automatically. Similarly, another group assumes robots look like humans [11]. These vague definitions reveal that we haven't yet come up with a satisfactory definition. Co-working between humans and robots will be fraught with problems if the necessary regulations are not in place. Defining what a robot is from a legal standpoint is the first step.

While there are scientific definitions for the robot, only a legal definition of a robot is binding the businesses to adopt it. An automated machine can be of many different types, and a robot is also one of them. Additionally, each machine has a defined level of automation. Co-working between humans and robots should be regulated by laws that clearly distinguish automated machines from robots. Similarly, drones and cyborgs also play a significant role. Furthermore, robots, drones, and cyborgs should all be distinguished from one another [12]. A law and other relevant regulations should not only include a clear definition, but also a list of robots that are allowed to be used in workplaces, robots' roles and responsibilities, their ability to make decisions involving humans, types of robot malfunctions, who is responsible for robot malfunctions, how robot malfunctions are handled, whether a robot's software follows hard-coded instructions or learns and evolves over time, the certifications robots must have, and the responsibilities of the certification authorities.

3.2. Employees Inclination towards Robots

Each individual has a different preference for whether to use or not to use a particular technology. In addition to people who are eager to work with robots, there are others who strongly oppose it. These personal preferences should be considered by organizations planning to integrate human-robot co-working into their workplaces. Co-working environments between humans and robots are unlikely to be successful if employees who enjoy working with them do not have

a positive attitude toward them. Since human-robot co-working does not yet exist, the media shapes people's opinions more than first-hand experiences when it comes to working with robots [13]. A number of famous movies and TV shows have been made about robots taking over the world or fighting humans. Robotics is negatively portrayed in media, and this affects people's preferences when it comes to working with them.

3.3. Cognitive Issues

Humans are subject to certain psychological effects as a result of advanced technology. An increasing number of people are becoming aware of the psychological disorder of video game addiction. Moreover, there are people who are extremely attached to their smart-phones. A new type of phobia emerged for them called "nomophobia" or "phobia of not having a mobile phone [14]." Nomophobia is defined by the Collins dictionary as a chronic stress caused by not having access to a mobile phone or being unable to use one. At the moment, there is no information about whether there will be "robophobia" or "norobophobia". Nevertheless, many employees are likely to experience many unprecedented psychological effects as a result of advanced technologies such as robots [15]. Organizational robotics will develop research topics regarding the psychological effects of working with robots and the impact they have on organizational climates.

3.4. Societal Consequences

The addition of robots to workplaces could have unprecedented effects on social interactions in the workplace, regardless of the number of human employees. The social behavior shown by robots may be preferable to some humans, while others may believe that such social behavior is fake and just computer programming. There will be different perspectives on social interaction with robots among employees. It becomes more difficult when robots hold positions of authority or management. The average employee shows respect for his or her superior or manager, but in this case employees could be unsure about respecting a robot manager [16]. As it is a fact that robots won't care about respect, because they don't

understand it. It will be new, confusing, and even frustrating for many people to deal with these kinds of issues. The way children treat robots is the same as how they treat their real pets, according to numerous studies. In the future, robot-human interaction may be similar to the human-smartphone interaction today, just as the latest generation of consumers has more interaction with smartphones and they view phones as an integral part of their lives. Hence, research on human-robot collaboration appears to be integrated with social studies.

3.5. Varying Employee-Employer Relation

Among the important responsibilities of human resources departments are analyzing work, developing job descriptions, and hiring the right people with the right qualifications. The vast majority of organizations currently employ people, with the exception of industries that use industrial robots. In a world where robots are becoming a part of every organization, human resources departments face a number of challenges. Additionally, they will have to identify which jobs can be handled by robots on top of their current duties. There are businesses and companies today advertising themselves as "green" and claiming to be environmentally friendly.

Businesses and organizations that practice "green" practices try to act responsibly towards the environment despite the fact that these initiatives increase costs. In the future, there might be businesses claiming to be "human". Despite being a "human" organization, these organizations may employ only humans even if using robots would be more economical. Organizations that claim to be human will assert that they are socially responsible and create jobs for people [17]. Among the most important responsibilities of the human resources department are analyzing work, creating job descriptions, and identifying business processes. It will take a lot of work for human resource departments to rethink most of what they have been doing when it comes to robots before they can integrate them into their organizations.

3.6. Business-IT Alignment

The importance of information technology (IT) increases as technology is becoming an inevitable part

of organizations' operations. It will be necessary for organizations to find a way to purchase and maintain robots in order to realize the vision of human-robot collaboration. The IT department is likely to be assigned this task at first. Eventually, organizations may create robotics departments that are responsible for acquiring and maintaining robots within their facilities. Maintaining and upgrading robots should be done in a safe and secure manner since robots take on a lot of responsibility. It will also be important to ensure the information security of robots. It will be much more challenging and complicated to secure data acquired by robots than to secure current IT infrastructures within organizations. Workplace information assurance and privacy assurance will likely be complicated by human-robot collaboration. Information security researchers will likely find this topic to be important [18].

3.7. Morality in Robots

The ethical behavior expected of human employees includes honesty, diligence, and helpfulness. It is certain that the work ethic values we hold dear will change if robots with selfless motives, without ambition, without laziness, and without lying are introduced. As far as reaching a good ethical standard in this regard goes, humans may not be able to compete with robots. As a result of a co-working environment involving humans and robots, it is hard to predict the development of work ethics. The interaction between humans and robots will also likely be governed by an ethical norm. Apparently, humans can feel sorry in the face of events such as robots behaving badly toward each other, according to a study. Hence, it will be necessary to determine the ethical status of robots in the workplace [19].

3.8. Learning Issues

The development of robots that can learn is an area of research that receives a lot of attention. There is, however, a possibility that robots with machine learning capabilities will behave in an unpredictable manner. People may be discouraged from assigning important tasks to robots if they experience this unpredictable behavior frequently. Robots may even be refused by some people depending on their

behavior. In contrast, robots that follow a set of rules are predictable. In spite of this, their learning capabilities will be limited. Therefore, co-working environments involving robots and humans will probably involve tradeoffs in robot types [20]. A robot with the capacity to learn but limited capability to do so may need to be chosen between a learning robot that is susceptible to unpredictable behaviors and a predictable rule-based robot that isn't capable of learning.

3.9. Challenges in working with Robots

The concept of robots is familiar to humans because of books and movies. The concept of co-working between humans and robots will, however, be unfamiliar to most office workers. In spite of expectations that robot interaction will be easy, the actual experience may be different from what is expected. For us to get what we really want, we may need to learn how to behave toward robots. The importance of non-verbal communication in human interactions cannot be overstated. These non-verbal communications, however, may not be understood by robots. Humans will have to learn to work with robots and will need time to get accustomed to it. As well, robots will be able to perform different tasks. Differentiating robots with different capabilities will be hard and confusing for humans [21]. There is a need for robot manufacturers to develop robots that convey information about their capabilities without confusing the user. As a result, working with different types of robots will require humans to learn new skills.

3.10. Missing Links

A study found that humans' greatest fear of robots is the loss of jobs, both personally and at Enterprise level. The negative attitude toward robots will likely increase as humans start losing their jobs to robots. Those who oppose the use of robots will argue that this will lead to increased unemployment. This view can be countered by arguing that new jobs will be created. In addition, this counterargument has been proven valid throughout history. In contrast to mundane jobs being taken over by robots, human creation, artistry, research, and development will be the focus of humans. Nonetheless, this view presents a dilemma.

It is unlikely that the people who lose their jobs will be able to fill jobs that require creativity because they lack the education, training, and skills. Let's imagine a middle-aged woman who works at a hotel as a housekeeper. Unless she has the skills required becoming a marketing campaign manager in the robotic age, it is unlikely that she will possess the necessary qualifications for such a position after losing her job to a robot. Unemployment will be strongly opposed by worker unions if robots are introduced. Having this negative attitude will lead constituents to vote for or make robotic laws and regulations based on these laws and regulations. Consequently, people may have a negative attitude toward robots in the early years of the robotic age since they cause unemployment [22].

3.11. Competition or Complementation

In the future, scientists and practitioners will discuss the positions and roles that robots will take on. A simpler solution would be to place robots in roles that complement human work. Consequently, humans won't feel threatened by robots since they won't lose their jobs. Robot assistants may even be preferred by most humans. Robots will take over the tasks in these positions so that humans will not have to worry about managing human assistants [23]. Humans will also have more time to spend on tasks requiring creativity and higher intelligence, as robots will take over mundane and cumbersome tasks. In order to create a co-working environment between humans and robots, complementing them with robots is a simpler, more straightforward, and less problematic solution. Some people, however, may advocate that robots should or may replace human employees in certain positions. The argument will be made that this will enhance the performance of human workers. It is natural for human beings to compete for positions in organizations. Management and organizational behavior will be complicated by adding robots to this competition. In fact, studies have been conducted investigating human reactions to robots that command [24].

4. Conclusion and Future Directions

It does not matter whether Industry 5.0 involves human-robot collaboration or not, it will still be an

important change for Enterprises. Humanity is likely to experience a significant change as a result to the introduction of robots into our lives. Using technology, researchers strive to create something that resembles humans in many ways. There will be some who find this innovative and exciting while there will be others who will find it outrageous, frustrating, and even dangerous. As a result of the media, people have a negative attitude towards robots. Practitioners might be biased by this negative attitude when they conduct surveys regarding robots in society. There is a negative perspective on robots reflected in one of the first scales developed to measure attitudes toward them. It is hard to predict how humans will respond to robots until they live and work with them. As humans become more familiar with robots, their attitude toward them is likely to change. There may be a difference between how the next generation reacts to robots and how this generation is doing, since the new generation will grow with robots or similar technologies. The developers must recognize the generational gap and create a robotic society that maximizes the benefits of robotic technology and minimizes its negative effects. The authors discussed possible legal, regulatory, psychological, socio-ethical, and ethical issues that may arise from human-robot co-working. In addition, the authors pointed out that the changing roles of IT and HR departments pose challenges to the co-working of humans and robots. The following issues are a few of the most prominent: personal preferences and types of robots preferred for working with, learning to work with robots, competing or cooperating with robots, and possible negative attitudes toward robots. In any case, all the topics discussed are still open to further research, investigation, and experimentation.

REFERENCES

- [1] Edquist, Charles & Jacobsson, Staffan. (1988). Flexible Automation – The Global Diffusion of New Technology in the Engineering Industry.
- [2] Kafi, Abdallah & Kovács, Tünde & Nyikes, Zoltán. (2022). Robots in the Industry 4.0. 10.1007/978-94-024-2174-3_31.
- [3] Demir, Kadir & Doven, Gozde & Sezen, Bulent. (2019). Industry 5.0 and Human-Robot Co-working. *Procedia Computer Science*. 158. 688-695. 10.1016/j.procs.2019.09.104.
- [4] Caradonna, Jeremy. (2022). The Industrial Revolution and Its Discontents. 10.1093/oso/9780197625026.003.0003.
- [5] <https://www.aurecongroup.com/blog/posts/5th-industrial-revolution-next-renaissance>
- [6] Jeyaraman, Madhan & Nallakumarasamy, Arulkumar & Jeyaraman, Naveen. (2022). Industry 5.0 in Orthopaedics. *Indian Journal of Orthopaedics*. 10.1007/s43465-022-00712-6.
- [7] Elfar, Omar & Peter, Angela & Kit Wayne, Chew & Show, Pau-Loke. (2021). What Is Industry 5.0?. 10.1201/9781003080671-4-4.
- [8] Sachsenmeier, Peter (2016) “Industry 5.0—The Relevance and Implications of Bionics and Synthetic Biology.” *Engineering*, 2, 2016: 225-229.
- [9] Demir, Kadir Alpaslan, and Halil Cicibaş (2018) “The Next Industrial Revolution: Industry 5.0 and Discussions on Industry 4.0.” *Industry 4.0 From the Management Information Systems Perspectives*. Peter Lang Publishing House.
- [10] Bagdasarov, Zhanna, April A. Martin, M. Ronald Buckley (2018) “Working with robots: Organizational Considerations.” *Organizational Dynamics*, 2018: <https://doi.org/10.1016/j.orgdyn.2018.09.002>
- [11] Briggs, Gordon, and Matthias Scheutz. (2014) “How Robots Can Affect Human Behavior: Investigating The Effects of Robotic Displays of Protest and Distress.” *International Journal of Social Robotics* 6 (3), 2014: 343-355.
- [12] Sargisson, Lucy. (2012). Cloning, Cyborgs and Robots. 10.1057/9781137031075_12.
- [13] Ray, Céline, Francesco Mondada, and Roland Siegwart (2008) “What do people expect from robots?” *2008 IEEE/RSJ International Conference on Intelligent Robots and Systems*, 2008: 3816-3821.
- [14] Raghavan, Manoj & P, Mohanapriya & K, Nivedha. (2022). NOMOPhobia.
- [15] Porpora, Douglas. (2021). On robophilia and robophobia. 10.4324/9780429351563-2.
- [16] Cormier, Derek, Gem Newman, Nakane, Masayuki, James E. Young, and Stephane Durocher (2013) “Would you do as a robot commands? An obedience study for human-robot interaction” *International Conference on Human-Agent Interaction*.
- [17] Narayanan, Jayanth & Puranam, Phanish & Vugt, Mark. (2021). Human Centric Organization Design: A Perspective from Evolutionary Psychology. *SSRN Electronic Journal*. 10.2139/ssrn.3959703.
- [18] Sieber, Marcel & Malý, Milan & Liska, Radek. (2022). Conceptualizing organizational culture and business-IT alignment: a systematic literature review. *SN Business & Economics*. 2. 10.1007/s43546-022-00282-7.
- [19] Rhim, Jimin & Lin, Cheng & Werner, Alexander & DeHart, Brandon & Qiang, Vivian & Rismani, Shalaleh & Moon, AJung. (2022). Roboethics as a Design Challenge: Lessons Learned from the Roboethics to Design and Development Competition. 11244-11250. 10.1109/ICRA46639.2022.9812265.
- [20] Xie, Xavier & Roberto, Canale & Xinquan, Liang. (2022). Learning-based Robotic Grasping: A Review.
- [21] Valdivia, Antonio & Shailly, Ritish & Seth, Naman & Fuentes, Francesco & Losey, Dylan & Blumenschein, Laura. (2022). Wrapped Haptic Display for Communicating Physical Robot Learning. 823-830. 10.1109/RoboSoft54090.2022.9762210.
- [22] Parr, Tom. (2022). Automation, unemployment, and insurance. *Ethics and Information Technology*. 24. 10.1007/s10676-022-09639-w.
- [23] Mathias, Sharon & Femil, S.. (2019). User Friendly Department Assistant Robo. 10.1007/978-3-030-32150-5_67.
- [24] Gärtner, Christian. (2022). Robo Recruiting. return. 9. 30-31. 10.1007/s41964-022-0906-9.

Sustainable IoT Systems Enabled by Supercapacitor Integration

Neha Taneja¹, Aakash Dhingra², Yogesh Kumar³

¹Department of Engineering, Maharishi University of Information Technology, Noida, 201304
¹nehataneja1140@gmail.com

²Department of Management, Narsee Monjee Institute of Management Studies, Mumbai, 40056
²adhingra92@gmail.com

³Department of Physics, Atma Ram Sanatan Dharam College, New Delhi, 110021
³ykumar@gmail.com

ARTICLE INFO	ABSTRACT
<i>Article history:</i> Received 03 May 2026 Received in revised form 09 June 2026 Accepted 25 June 2026 Available online 12 July 2026 <i>Keywords:</i> Supercapacitor Energy storage devices Sustainable Power Density Energy density	<i>The rapid expansion of self-powered IOT systems has demanded sustainable power sources for the sensor networks. The IOT system uses different batteries which have some limitations such as lower lifespan, needs replacement with time and environmental issues. Energy harvesting systems use the different power sources like solar energy, mechanical, thermal to convert it into electrical power. However, the low power natures of these sources necessitates better energy sources with the high energy density and low environmental impact.</i> <i>This chapter represents the energy harvesting systems for the Internet of things with the integration of supercapacitors. Supercapacitors are the energy storage devices which act as the replacement of batteries and have advantages such as high power density, longer lifetime, rapid charging-discharging capabilities that serve as efficient energy devices for the self-powered IOT systems. Furthermore, the chapter also analyses the current challenges of complexity of integration of energy sources, low energy efficiency and low power sources. The chapter concludes by the future research scope for the self-powered sustainable and low cost IOT systems.</i>

1. Introduction

The Internet of Things (IoT) links computing devices, machines, everyday objects, living beings, and uniquely identified individuals into a shared network, enabling them to exchange data without direct human involvement or continuous human-computer interaction[1]. This interconnected communication framework adds considerable value to modern life by considering automating tasks also with improved efficiency, and enabling smarter decision making processes. IoT empowers devices, computing systems and it enables the transmission of information across networks without relying on human and machine input[2]. The first stage of IoT consists of sensors, smart devices, actuators and other components which collect data from the environment and then send it to other network systems. The second layer involves network gateways and data acquisition systems. These systems collect the signals from the sensors and convert them into analog signals to digital signals. These systems also perform tasks like malware detection and basic data management.

The third stage of the IoT architecture is particularly critical and at this level, the first step is to pre-process the data according to its types and structure, after that it is routed to appropriate data centres[3]. This is because edge computing becomes important, as it allows processing and reduces the need to move all information to distant closers. The fourth layer consists of cloud environments and data centers, for applications such as agriculture, defense, healthcare, and others consume and analyze the data. IoT devices often handle many sensitive and personal and operational information also security purposes can lead to privacy breaches[3]. Robust security measures must be implemented such as strong encryption, secure authentication methods, and regular software updates which are very essential for protecting user data and preserving trust in IoT systems. At the same time, IoT ecosystems can grow more rapidly when more devices will be added and the major challenge to maintain scalability of systems[4]. Designing architectures is crucial for sustainable growth that can efficiently manage large numbers of devices, diverse data streams, and numerous access points. Enabling technologies have

main components that support core IoT functions such as sensing, connectivity, data processing, and intelligent decision-making. Radio Frequency Identification (RFID) and Near Field Communication (NFC) enable automatic identification of objects and short-range wireless data transfer, which helps IoT systems that recognize the supportive items and make contactless interactions with the system. Embedded systems have some specialized computing units that are built with IoT devices which control sensors and actuators also process the collected data, and manage communication with other devices or platforms[1]. Wireless sensor networks consist of many sensor nodes that communicate via wireless links to gather and transmit data to other systems. These networks are widely used for monitoring various conditions in smart cities, agriculture areas, and industrial regions[5]. Cloud computing provides storage and processing resources for handling massive volumes of IoT data, whereas Big Data technologies support analysis, indexing, and managing these datasets[6]. Edge and fog computing parts can distribute processing closer to the source devices rather than sending all data to the centralized cloud servers[6]. This approach reduces the latency, improves real-time response, and lowers network bandwidth usage. In this context, we present a comprehensive overview of advances and enhancements in IoT systems in relation to the development of supercapacitor (SC) materials.

This chapter is structured as follows: First, the basic concepts of IoT are introduced. Next, different classes of supercapacitors are discussed, including electric double-layer capacitors (EDLCs) based on carbon, pseudocapacitive supercapacitors, and hybrid devices. Then, key performance metrics are examined and compared with those of conventional batteries. After that, the materials are required to fabricate a supercapacitor with the components electrode and electrolyte. Finally, the main challenges, integration strategies, performance parameters, and optimization approaches are summarized, along with key conclusions and general directions for future research.

2. Fundamentals of IoT Power Systems

IoT features are frequently described by the different components of the Internet of Objects (IoO) which are described here.

2.1 Interconnection

A core aspect of IoT infrastructure is connectivity. IoT devices must stay consistently connected to the network so that communication remains uninterrupted. Users and systems should be able to connect at any time and from any location which ensures the continuous interaction within the ecosystem[7].

2.2 Compatible Communication Protocols

Seamless and interoperable communication is a fundamental characteristic of the Internet of Things. As the IoT system grows the devices are becoming more tightly interconnected than ever before, which is one of the defining traits of IoT. This capability ensures that communication between the devices occurs more smoothly and efficiently. These devices connect to the internet using cloud-based services, which facilitates data exchange across different platforms. Integration enables continuous, reliable interaction between IoT gadgets and systems[8].

2.3 Identity of Objects

Identity is a key characteristic for people and objects. Just as every person has a unique identity, every connected device can be assigned a distinct identifier. For instance, each smartphone has a unique IMEI number, and most smart devices are labelled with individual identifiers. Such unique markings make it easier to recognize and manage devices and individuals over the internet. As a result, object identity is considered one of the most critical features of IoT[9].

2.4 Expansion Capability

Scalability has become a more important feature in IoT system design with an increase in the number of connected devices. In technical terms, scalability refers to a system ability to grow in size or capacity

without degrading its performance[10]. By leveraging IoT's scalable architecture, organizations can adjust their systems to meet operational needs. For example, hotels can use IoT to monitor room occupancy and the usage of amenities by different guests in real time.

2.5 Dynamic or Self-Adjusting Behaviour

The dynamic or self-adapting nature of IoT is another essential feature. IoT systems must be able to respond autonomously for environment changes and evolving requirements. For example, early cameras were designed mainly to capture still images[11]. Modern cameras, however, automatically adjust image settings based on lighting conditions, demonstrating how IoT enabled systems can self-adapt to improve performance.

3. Fundamentals of Supercapacitors

3.1 Storage Mechanisms

To store electrical energy, capacitors accumulate charge on two parallel electrodes separated by a separator referred to as dielectric substance. Capacitor capacity is the amount of charge stored for each unit of voltage applied to its plates. The connection between charge (q) and voltage (V) defines if a capacitor exhibits resistance or inductance between the plates. This relationship is represented in Equation (1), where V denotes the voltage across the capacitor, C represents the value of the capacitor in Farads (F), and q indicates the charge held within the capacitor. The value of capacitance of a capacitor can be calculated using Eq.2, which depends on the dielectric permittivity, the effective area of the electrodes in device A , and the distance d between the capacitor electrodes.

Equation (3) allows for calculating the energy held in a capacitor, which is influenced by the capacitance of the device and the terminal voltage.

Where V represents the voltage at the capacitor terminals, C denotes the capacitance of the capacitor, and E indicates the energy stored within the capacitor

$$Q=CV \quad \dots\dots\dots(1)$$

$$C= \epsilon A/d \quad \dots\dots\dots(2)$$

$$E=1/2CV^2 \quad \dots\dots\dots(3)$$

3.2 Types of Supercapacitors

3.2.1 Electric Double-Layer Capacitors (EDLCs)

Supercapacitors are typically composed of two electrodes, an electrolyte, and a separator that helps to prevent short circuits. The electric double layer (EDL) formed at the electrode and electrolyte interface which is considered as the primary source of capacitance in electrochemical supercapacitors[13].

The electrochemical double-layer concept provides the information regarding the electrochemical behaviour at these interfaces. It describes the procedure when an electrode is in contact with the electrolyte during charging, where charge separation occurs. The capacitance is strongly influenced by the electrode surface area in contact with the electrolyte, with larger surface areas that enables much higher capacitance values.

Helmholtz was the first scientist to describe charge separation at the interface of electrolyte and electrode. They suggested that charges can accumulate on the electrode surfaces, leading to the formation of two closely spaced layers of opposite polarity. Unlike the simple view of non-specific adsorption, this model allows for ion adsorption directly on the electrode surface. According to Helmholtz, the EDL stores charge through electrostatic attraction, similar to a molecular-scale dielectric[13].

Building on Helmholtz's idea, the Gouy–Chapman model (1910) proposed that capacitance depends on the applied voltage and the ion concentration in the electrolyte. In this model, the electric field weakens as it extends into the electrolyte, and a double layer of oppositely charged ions forms at the boundary between the electrode and the electrolyte due to Coulombic forces[14]. This double layer acts as an effective barrier that traps charge within the storage system. The total charge on the electrode surface is then determined by both the double-layer capacitance and the applied voltage. The development of electrochemical supercapacitors is largely based on the electric double-layer capacitor (EDLC) concept[15].

3.2.2 Pseudocapacitors

The term “pseudocapacitive” originates from a Greek word meaning “to hold” or “to retain.” In this type of supercapacitor, charge storage arises from faradaic processes, such as redox reactions occurring at the electrode–electrolyte interface. These reversible electrochemical reactions allow pseudocapacitors to store more charge than EDLCs.

Compared with EDLCs, pseudocapacitors generally offer higher energy density and better charge storage capacity, but at the cost of lower power density. Materials commonly used in pseudocapacitive systems include transition metal oxides, layered hydroxides, metal sulfides, and certain conducting polymers. Despite their superior performance, pseudocapacitors remain in relatively early stages of commercialization, partly because of the limited variety of suitable electrode materials. So far, ruthenium-based materials have shown the best results, but their high production cost makes widespread use impractical[16].

3.2.3 Hybrid Supercapacitors

Hybrid supercapacitors are designed to combine the advantages of different storage mechanisms. They exhibit significantly higher energy density than conventional EDLCs and behave more like battery-type devices, while still retaining some capacitor-like characteristics. This category includes systems that integrate features of both EDLCs and pseudocapacitors, often using an asymmetric configuration[17].

In hybrid designs, the energy is stored through a combination of electrostatic and faradaic processes, which improves overall performance. However, the slower electrochemical reactions at the electrode surface can limit power delivery and long-term stability, even though energy density is higher. Compared with traditional supercapacitors and

batteries, hybrid systems often show better electrochemical performance in terms of both energy and power density. Common electrode materials for hybrid supercapacitors include carbon-based structures, metal oxides, metal vanadates, and other composite materials[18].

3.3 Key Performance Parameters and Comparison with Conventional Batteries

Balancing the use of renewable energy sources while preventing their over consumption is one of the most pressing challenges today. Among renewable technologies, solar and wind power are the two dominant sources. Supercapacitors (SCs) offer several advantages over conventional batteries, including high power density, good performance at low temperatures, excellent cycling durability, and fast charging capabilities. However, because SCs typically consist of many individual capacitors connected in parallel, their charge and discharge rates are relatively slower compared to ideal expectations. These limitations, along with their generally lower capacity, restrict the practical use of SCs in many consumer electronics applications[19].

Electrical energy storage systems that can endure a very high number of cycles (often exceeding 1,000,000) include traditional batteries, advanced batteries, and supercapacitors. These devices are generally low-cost and require minimal maintenance. Supercapacitors were first commercialized by Nippon Electric Company, while ultracapacitors were developed by the Pinnacle Research Institute. The first patent for such technology was filed by General Electric in 1957.

TABLE 1
Key characteristics of supercapacitors and batteries

Parameters	Supercapacitor	Battery
Energy density	Low	high
Power density	high	Low
Charge-discharge cycle	10^5 - 10^6	500-1000
Self-discharge	Days to weeks	Months

Lifetime	5-10 years	3-5 Years
Cell potential	1.2-3.8V	2.5 to 4.2 V

Recent studies have shown that supercapacitors can achieve high specific capacitance and favorable energy density. They are also lightweight, compact, and relatively expensive compared to some alternatives. Their excellent performance and nearly flat charging profile, supercapacitors are considered promising candidates to partially replace batteries in certain applications. They can be charged more quickly and offer superior cycle stability when compared with fuel cells and alkaline batteries[20]. Key characteristics of supercapacitors and batteries are summarized in Table 1.

According to Musolino, the supercapacitor has a high power density but a low energy density[21].

4. Materials and Technological

Advances

4.1 Electrode Materials

One of the important parts of a supercapacitor is the electrode. When we build a supercapacitor we use electrodes made of metal. The capacitance of these electrodes is different depending on the materials we use. Now scientists are studying supercapacitors and they found that electrodes made of cobalt hydroxide have very high capacitance. We use cobalt-based metal oxides and hydroxides to make electrodes for supercapacitors because they have good electrical conductivity. These materials are very stable and are considered to be useful. Cobalt-based metal hydroxides and oxides are great for making supercapacitor electrodes because they conduct electricity well and are not very reactive. Compared to materials like nickel hydroxides, aluminum hydroxides and copper hydroxides, cobalt-based metal oxides and hydroxides are better because they have higher energy and capacity ratios[22].

4.2 Electrolytes for Supercapacitors

We usually use electrolytes in commercial supercapacitors but they have some limitations. These electrolytes are ammonium salts and they have high electrochemical potential. This means they are

slightly alkaline. The voltage at which these electrolytes dissociate is very high over 2.5V. The electrolyte controls the movement of electrons in the supercapacitor. We have types of electrolytes like organic, aqueous and organometallic electrolytes. Ionic electrolytes are usually the ones that dissociate in water. They have cations and anions of sizes. Organic electrolytes can also have multivalent cations. These electrolytes are very good because they have energy density, conductivity and electrochemical stability[23].

4.3 Separator

The separator is an important part of the supercapacitor. It separates the hydrogel and removes the electrolyte from the electrode material. We need high-performance separators for supercapacitors that work at voltage, high voltage and high temperature. We can use ceramic, paper or glass fiber separators. The type of separator we use depends on the application. We can test the performance of the separator using methods like calorimetry, capacity measurement and eddy current analysis. The separator is like an electrode separation cell that uses solid separators to separate ions based on how well they conduct electricity[24].

5. Integration of Supercapacitors in IoT Systems

Nowadays energy harvesting technologies are becoming very popular. They need an energy storage device to deal with their limited power and intermittent characteristics. We can use batteries. They have limited cycle life and that is not good because replacing them is expensive. Supercapacitors are becoming popular because they provide a lot of power for data transfer and they have a long cycle life. But supercapacitors have a limitation. They take up a lot of space on printed circuit boards[25].

5.1 IOT and Energy harvesting

The term "Internet of Things" or IoT is becoming very popular. It refers to a network of connected physical things. IoT is like a network of objects that can be addressed uniquely. They communicate using standard protocols. We can imagine new applications like health monitoring, smart homes, logistics and industrial manufacturing. All these applications have one thing in common. They are all very energy-constrained. This is a problem for power components and power management techniques. Current battery technology is not good enough for IoT devices because they need to be small and have a long lifetime. Energy harvesting is one solution. We can use energy sources like thermal, solar, vibration and radiofrequency to charge an energy storage device like a battery or supercapacitor. This can help extend the lifetime of IoT devices and even make them work independently[26].

Current uses, for Wireless Sensor Networks include fields. We can use panels, piezoresistors or RF rectifiers to convert environmental energy into electric energy.

5.2 Integrating Supercapacitors as a power supply

Power sources pose many challenges to specific biomedical applications. Biomedical sensors generally incorporate batteries, which grant the circuit a self-contained, closed, and sealed structure. Their short lifespan, long charging times, and high toxicity make them less desirable for future applications [8]. Recent advances in supercapacitors (supercap) have unlocked different opportunities for powering biomedical devices. Although supercapacitors have a low energy density, they have a very fast charging time and virtually unlimited shelf life without the toxic heavy metals. Supercapacitors have a very high power density and are easy to use and integrate in Uninterruptible Power Supply (UPS) Systems[27]. Supercapacitors have been used in Uninterruptible Power Supplies to provide and maintain a constant power supply to electronic devices, for instance, computers, televisions, printers, scanners, and so on. The company requires that all offices, shops and enterprises are operational all the time, that is, seven

days a week on twenty four hours a day basis in order to serve the customer well.

6. Challenges and Limitations

Typically, applications that fall under the Internet of Things (IoT) will involve many component systems. As such, the cloud or fog will build a number of the IoT application components. Components that provide the end users access to the IoT systems will typically be built as a separate web, mobile, or desktop application. On the other hand, data collection and real-time data analysis features will be built into the IoT devices. Furthermore, IoT applications can be located in different and quite large geographical locations. The conventional method that centralizes all the software components for a single system may be insufficient to address the distribution of the applications. In addition, it is often very difficult to design and implement a distributed system that can operate in a coordinated manner with decentralized components.

When multiple IoT applications use services from real world objects, an interdependency problem can arise. Take the example of two IoT applications operating simultaneously in a home: a health-care application that monitors residents' vital signs, and an energy management application that optimizes the energy consumption of home appliances[28]. These applications use data from the home's sensors to implement the application in a cost effective manner and to limit channel contention. However, integrating the two applications is complicated since each application will have its own assumptions of the world, and each will typically lack awareness of the other application. For example, the home health-care application may decide to turn on all the lights when it detects that a resident is in a state of depression[29].

As IoT applications are embedded into daily life, including some applications in critical contexts where there's little tolerance for errors, it is essential to evaluate the overall quality of the system. It needs to be carefully evaluated before deploying to ensure that it is high quality. One of the main issues in evaluating quality is that performance is contingent on the performance of many elements as well as the performance of the underlying technology. This

makes assessing quality criteria like performance a great challenge[30].

7. Conclusion and Future perspective

This chapter deals with the integration of supercapacitors in IoT systems. Supercapacitors store electricity in a system. Compared to batteries, supercapacitors are superior in having longer life and better charge-discharge cycling. IoT system frameworks are being used in numerous areas including healthcare, transportation, and agriculture. This chapter discusses the significance of energy harvesting in IoT systems and the quality of energy sources available to IoT systems. Following this, the IoT frameworks are described, and the challenges and optimizations are discussed.

It then focuses on the obstacles to the development of IoT applications and analyzes existing IoT frameworks specially targeted to IoT application development and their advantages and disadvantages. Based on this analysis, a large number of development frameworks have been introduced for the purpose of aiding the development of IoT applications, with most of these frameworks being in the early stages of development and having different structures, yet many frameworks have been created. The majority of these frameworks focus on the rapid development of IoT applications with little to no focus on the resulting application quality. Therefore, to develop high-quality IoT applications, development frameworks of this nature must incorporate quality assurance control. In addition, new heterogeneous devices and technologies will need to be integrated into these systems and dynamically configured.

REFERENCES

- [1] Perwej, Y., Haq, K., Parwej, F., Mumdouh, M., & Hassan, M. (2019). The internet of things (IoT) and its application domains. *International Journal of Computer Applications*, 975(8887), 182.
- [2] Aceto, G., Persico, V., & Pescapé, A. (2019). A survey on information and communication technologies for industry 4.0: State-of-the-art, taxonomies, perspectives, and challenges. *IEEE Communications Surveys & Tutorials*, 21(4), 3467-3501.
- [3] Saqlain, M., Piao, M., Shim, Y., & Lee, J. Y. (2019). Framework of an IoT-based industrial data management for smart manufacturing. *Journal of Sensor and Actuator Networks*, 8(2), 25.
- [4] Singh, N., Buyya, R., & Kim, H. (2024). Securing cloud-based internet of things: challenges and mitigations. *Sensors*, 25(1), 79.
- [5] Dargie, W., & Poellabauer, C. (2010). *Fundamentals of wireless sensor networks: theory and practice*. John Wiley & Sons.
- [6] Aydin, G., Hallac, I. R., & Karakus, B. (2015). Architecture and implementation of a scalable sensor data storage and analysis system using cloud computing and big data technologies. *Journal of Sensors*, 2015(1), 834217.
- [7] Kumar, N. M., & Mallick, P. K. (2018). The Internet of Things: Insights into the building blocks, component interactions, and architecture layers. *Procedia computer science*, 132, 109-117.
- [8] Uzoka, A., Cadet, E., & Ojukwu, P. U. (2024). The role of telecommunications in enabling Internet of Things (IoT) connectivity and applications. *Comprehensive Research and Reviews in Science and Technology*, 2(02), 055-073.
- [9] Omar, A. S., & Basir, O. (2020). Decentralized identifiers and verifiable credentials for smartphone anticounterfeiting and decentralized IMEI database. *Canadian Journal of Electrical and Computer Engineering*, 43(3), 174-180.
- [10] Zyrianoff, I., Borelli, F., Biondi, G., Heideker, A., & Kamienski, C. (2018, June). Scalability of real-time iot-based applications for smart cities. In *2018 IEEE symposium on computers and communications (ISCC)* (pp. 00688-00693). IEEE.
- [11] Alfonso, I., Garcés, K., Castro, H., & Cabot, J. (2021). Self-adaptive architectures in IoT systems: a systematic literature review. *Journal of Internet Services and Applications*, 12(1), 14.
- [12] Mallick, S., Bag, S., & Retna Raj, C. (2025). Supercapacitors for energy storage: Fundamentals and materials design. *Journal of Chemical Sciences*, 137(3), 65.
- [13] Hasan, M., Murshed, I., Islam, K., & Masud, A. K. M. (2026). Toward unified interphase engineering: the solid-electrolyte interphase in batteries and supercapacitors. *Journal of Materials Chemistry A*, 14(31), 20009-20057.
- [14] Ouyang, Y., Wang, Z. L., & Wei, D. (2025). Ionic rectification via electrical double layer modulation at hydrogel interfaces. *RSC Applied Interfaces*, 2(4), 873-896.
- [15] Guan, Y., Kümper, J., Kumari, S., Heiming, N., Mürtz, S. D., Steinmann, S. N., ... & Sautet, P. (2025). Probing the electric double-layer capacitance to understand the reaction environment in conditions of electrochemical amination of acetone. *ACS Applied Materials & Interfaces*, 17(2), 4087-4097.
- [16] Sampath, A. I. (2026). *Graphene produced by direct laser writing for flexible electronic applications, specifically in developing hybrid microsupercapacitors* (Doctoral dissertation, Politecnico di Torino).
- [17] Premkumar, A., Sridevi, B., Mohan, K. S., & Gnanamuthu, R. M. (2025). Design and exploring the synergistic potential of Ni-Co2-S4/rGO composite electrode for high performance flexible hybrid supercapacitors. *Electrochimica Acta*, 513, 145519.
- [18] Liu, L., Zhang, X., Liu, Y., & Gong, X. (2025). Electrochemical energy storage devices—batteries, supercapacitors, and battery-supercapacitor hybrid devices. *ACS Applied Electronic Materials*, 7(6), 2233-2270.
- [19] Sindhu, S. (2025). Comparative Analysis of Battery-Supercapacitor Hybrids for Fast EV Charging Infrastructure. *Transactions on Energy Storage Systems and Innovation*, 26-33.
- [20] Azaïs, P. (2013). Manufacturing of industrial supercapacitors. *Supercapacitors: Materials, Systems, and Applications*, 307-371.
- [21] Naeem, S., Ali, A., Memon, K., Bavluwala, M., Shinde, U. P., & Patil, A. V. (2023). A review of flexible high-performance supercapacitors for the internet of things (IoT) and artificial intelligence (ai) applications. *Energy and Thermofluids Engineering*, 3, 1-9.
- [22] Liu, X., Shi, C., Zhai, C., Cheng, M., Liu, Q., & Wang, G. (2016). Cobalt-based layered metal-organic framework as an ultrahigh capacity supercapacitor electrode material. *ACS applied materials & interfaces*, 8(7), 4585-4591.
- [23] Yu, L., & Chen, G. Z. (2019). Ionic liquid-based electrolytes for supercapacitor and supercapattery. *Frontiers in chemistry*, 7, 432729.
- [24] Liang, N., Wu, X., Zhang, X., Lv, Y., Guo, J., Guo, R., ... & Jia, D. (2024). A graphdiyne based separator toward high performance activated electrolyte-enhanced supercapacitors. *Journal of Materials Chemistry A*, 12(8), 4695-4701.
- [25] Navarro, G., Torres, J., Blanco, M., Nájera, J., Santos-Herran, M., & Lafoz, M. (2021). Present and future of supercapacitor technology applied to powertrains, renewable generation and grid connection applications. *Energies*, 14(11), 3060.
- [26] Vermesan, O., & Friess, P. (2014). *Internet of things applications-from research and innovation to market deployment* (p. 364). Taylor & Francis.

- [27] Choi, S. (2026). Rethinking Power Solutions for Healthcare Wearables: From Point-of-Care and Episodic use to Continuous Monitoring and Therapeutic Platforms. *Advanced Energy and Sustainability Research*, 7(3), e202500352.
- [28] Adam, M., Hammoudeh, M., Alrawashdeh, R., & Alsulaimy, B. (2024). A survey on security, privacy, trust, and architectural challenges in IoT systems. *IEEE Access*, 12, 57128-57149.
- [29] Farhan, L., Kharel, R., Kaiwartya, O., Quiroz-Castellanos, M., Alissa, A., & Abdulsalam, M. (2018, July). A concise review on Internet of Things (IoT)-problems, challenges and opportunities. In *2018 11th International Symposium on Communication Systems, Networks & Digital Signal Processing (CSNDSP)* (pp. 1-6). IEEE.
- [30] Udoh, I. S., & Kotonya, G. (2018). Developing IoT applications: challenges and frameworks. *IET Cyber-Physical Systems: Theory & Applications*, 3(2), 65-72.

EchoMesh: A Decentralized Off-Grid LoRa Mesh Communication System for Emergency and Remote Connectivity

Aditya Tripathi¹, Durgesh Tiwari²

¹Maharishi School of Engineering and Technology, Maharishi University of Information Technology, Noida, Gautam Buddha Nagar, Uttar Pradesh 201304, India

¹aditya.tripathi.tech@gmail.com

²Maharishi School of Engineering and Technology, Maharishi University of Information Technology, Noida, Gautam Buddha Nagar, Uttar Pradesh 201304, India

²dtiwari.it@gmail.com

ARTICLE INFO	ABSTRACT
<i>Article history:</i> Received 13 May 2026 Received in revised form 09 June 2026 Accepted 12 June 2026 Available online 12 July 2026 <i>Keywords:</i> LoRa, Mesh Networking, Emergency Communication, ESP32, IoT, BLE, Embedded Systems	ABSTRACT <i>Modern communication systems rely heavily on centralized infrastructure like cellular towers, internet backbones, and cloud services. During natural disasters, military conflicts, remote expeditions, and large public events, these infrastructures often fail or become congested, causing communication breakdowns. This research introduces EchoMesh, a decentralized LoRa-based mesh communication system designed for off-grid communication using low-power embedded devices. EchoMesh enables text messaging, GPS sharing, emergency SOS signaling, and low-bitrate voice transmission without relying on cellular networks or internet connectivity. The system uses ESP32 microcontrollers, SX1276 LoRa transceivers, Bluetooth Low Energy (BLE), GPS modules, and open-source firmware architecture. It combines mesh routing, AES-128 encryption, and hybrid mobile integration through a Flutter-based smartphone app. This research evaluates how well long-range communication can work with low power consumption while keeping scalability and reliability in disaster-response and rural communication scenarios.</i>

1. Introduction

Communication infrastructure forms the backbone of modern society. Most contemporary communication technologies depend on centralized cellular towers, internet gateways, and cloud servers. While these systems offer high-speed connectivity under normal circumstances, they become vulnerable during disasters and infrastructure failures. Earthquakes, floods, hurricanes, forest fires, and large events can overload or damage communication systems, leaving users disconnected at critical times.

Low-Power Wide Area Network (LPWAN) technologies like LoRa (Long Range) have emerged as promising alternatives for long-distance, low-power communication. LoRa technology allows for communication over several kilometers while using minimal energy, making it suitable for emergency communication systems, wireless sensor networks, and off-grid deployments.

EchoMesh is proposed as a decentralized mesh communication platform that combines LoRa radio communication, ESP32 embedded systems, BLE integration, and GPS-based location sharing. Unlike standard star-topology LoRaWAN systems that rely on gateways, EchoMesh uses a peer-to-peer mesh architecture where every node acts as a sender, receiver, and relay.

The system focuses on:

- Infrastructure-independent communication
- Long-range communication using LoRa
- Emergency SOS broadcasting
- GPS location sharing
- Secure encrypted communication
- Smartphone integration using BLE
- Low power consumption
- Community deployability

This research examines the architecture, implementation, performance characteristics, security considerations, and future potential of the EchoMesh system.

2. Problem Statement

Traditional communication systems fail in situations where network infrastructure is missing or damaged. During disasters, communication congestion can prevent timely coordination between emergency responders and affected people. Rural and remote areas often suffer poor network coverage.

Several limitations exist in current communication technologies:

- Cellular communication needs operational towers.
- Internet-based messaging relies on centralized servers.
- Satellite communication systems are costly.
- Traditional walkie-talkies have limited range with no mesh routing.
- Existing mesh systems are often expensive or proprietary.

The inability to maintain communication during emergencies can delay rescue efforts, lower situational awareness, and increase risks to human life.

Therefore, there is a need for a low-cost, decentralized, energy-efficient communication platform that operates independently of traditional infrastructure.

3. Objectives of the Research

The primary objectives of this research are:

- To design a decentralized off-grid communication system using LoRa technology.
- To implement mesh-based message routing between nodes.
- To enable GPS-based location broadcasting.
- To integrate smartphone connectivity through BLE.
- To evaluate communication range and power efficiency.
- To provide secure communication using AES encryption.
- To develop a scalable architecture for disaster communication.
- To create an affordable communication solution for remote areas.

4. Literature Review

The Internet of Things (IoT) links computing devices, machines, and objects into a shared network, enabling data exchange without direct human involvement (Tiwari, 2026). This framework involves multiple layers, from sensors and data acquisition systems to edge computing and cloud environments, which collectively enable automation, improved efficiency, and smarter decision-making (Tiwari, 2026). As these ecosystems grow, maintaining system scalability and implementing robust security measures, such as strong encryption and regular updates, remains a critical challenge for sustainable development (Tiwari, 2026).

LoRa technology has received significant attention in recent years for its long-range communication abilities and low power needs (Augustin et al., 2016; Raza et al., 2017). Studies highlight its suitability for Internet of Things (IoT) applications and analyze limitations and scalability issues of LoRaWAN systems.

Mesh networking has been widely studied in wireless communication research (Akyildiz et al., 2005). Surveys have provided overviews of wireless mesh networks and their routing mechanisms. Research on LoRa mesh networking approaches has classified multi-hop communication methods.

Disaster communication systems have also seen extensive research (Ranaweera et al., 2018). Surveys of emergency communication technologies emphasize the need for decentralized communication frameworks. Bluetooth Low Energy (BLE) integration has enabled smartphone-device interaction in embedded systems (Gomez et al., 2012). Studies have evaluated BLE's performance and power efficiency in wireless systems. Security in wireless sensor networks continues to be a significant challenge (Roman et al., 2013; Perrig et al., 2002). Security protocols for sensor networks and discussions on IoT security and privacy issues are part of ongoing research.

Recent research has addressed these challenges through multi-layer clustering security protocols (Gupta & Kumar, 2022b) and the implementation of lightweight cryptography specifically designed for resource-constrained IoT devices (Gupta & Kumar, 2019). Studies have further introduced lightweight hash functions and pseudo-random number generators, such as DeeR-Hash and DeeR-Gen, to enhance

security within Industry 4.0 environments (Gupta & Kumar, 2023a, 2023b). Additionally, specialized frameworks have been proposed for managing smart healthcare services in IoT (Gupta & Kumar, 2022a), while broader reviews have identified key networking technologies, security threats, and potential countermeasures in IoT (Gupta & Kumar, 2020).

The existing literature confirms that LoRa mesh communication combined with embedded IoT devices can offer a practical solution for decentralized emergency communication.

5. System Architecture

5.1 Overview

EchoMesh consists of multiple handheld LoRa nodes that can form a self-healing mesh network. Each node includes:

- ESP32 microcontroller
- SX1276 LoRa transceiver
- GPS module
- OLED display
- BLE interface
- Rechargeable Li-ion battery
- Embedded firmware

The system supports:

- Text messaging
- GPS beaconing
- SOS transmission
- Private encrypted channels
- Multi-hop message relaying
- Smartphone companion application

5.2 Hardware Components

5.2.1 ESP32 Microcontroller

The ESP32 acts as the main processing unit. It offers dual-core processing, integrated BLE/Wi-Fi, low-power modes, and sufficient capability for routing and encryption.

5.2.2 SX1276 LoRa Module

The SX1276 transceiver allows for long-range communication using Chirp Spread Spectrum modulation. The module supports various ISM frequency bands.

5.2.3 GPS Module

The NEO-M8N GPS module provides latitude, longitude, altitude, and satellite information for location sharing and emergency tracking.

5.2.4 OLED Display

The OLED display provides a low-power interface for viewing messages, battery status, and node information.

5.2.5 BLE Connectivity

The Bluetooth Low Energy (BLE) module allows the EchoMesh device to connect wirelessly to smartphones, enabling users to send messages and view data through a simple app interface.

6. Software Architecture

The software architecture consists of three layers as shown in Figure 1:

- Embedded firmware layer
- Communication layer
- Mobile application layer

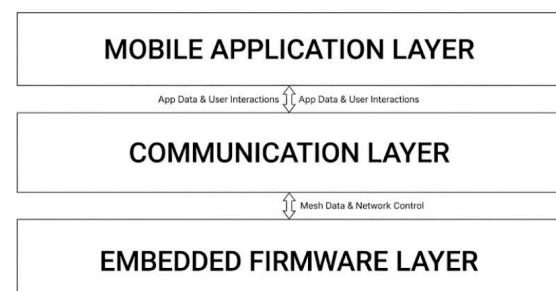


Figure 1: Software Architecture of Echo Mesh

6.1 Embedded Firmware

The firmware is developed using the Arduino framework and PlatformIO environment. Key firmware modules include:

- **Radio management:** Controls LoRa signal transmission and reception to ensure reliable data exchange between devices.
- **Mesh routing:** Determines the optimal path for data to travel across multiple devices to reach its final destination.
- **GPS parsing:** Decodes raw location data from the GPS module into readable coordinates for the user.

- **Display management:** Updates the device screen to show battery levels, incoming messages, and current node status.
- **BLE communication:** Facilitates wireless data transfer between the LoRa hardware and a user's smartphone.
- **Encryption handling:** Secures all outgoing data using AES-128, ensuring the privacy of messages sent over the network.

6.2 Mesh Routing

The routing mechanism includes:

- **Packet ID generation:** Assigns a unique tag to every message to track its delivery status and avoid confusion.
- **Hop count tracking:** Monitors how many nodes a packet has passed through to prevent network congestion and infinite loops.
- **Relay forwarding:** Automatically passes received information along to other nodes to extend the total range of the network.
- **Packet deduplication:** Recognizes and discards redundant copies of the same message that may arrive via different network paths.

6.3 Mobile Application

A Flutter-based mobile application provides:

- **Chat interface:** Provides a familiar screen for users to type and read text messages sent through the mesh network.
- **Offline maps:** Displays local geographic data directly in the app without requiring an internet connection.
- **Node radar visualization:** Shows the relative position and signal status of nearby active nodes to help maintain connection.
- **BLE connectivity:** Manages the pairing and continuous data stream between the user's phone and the LoRa hardware device.
- **SOS controls:** Offers a dedicated, easy-to-access feature for broadcasting emergency distress alerts to all nearby users.
- **Channel management:** Allows users to create, join, or switch between private communication groups.

7. Communication Protocol

The EchoMesh protocol utilizes a custom packet structure that includes:

- **Packet header:** Contains essential control information used to route the message correctly through the network.
- **Sender information:** Identifies the unique ID of the device that originally sent the message.
- **Receiver information:** Specifies the intended target node ID to ensure the message reaches the correct destination.
- **Packet type:** Indicates the nature of the data being sent, such as text, location updates, or emergency signals.
- **Hop count:** Tracks how many times a message has been forwarded, preventing infinite routing loops.
- **Payload data:** Carries the actual message content, including text characters or GPS coordinates.

Supported packet types include:

- **Text messages:** Carries user-generated text content for direct communication between nodes.
- **GPS beacons:** Transmits geographical coordinates periodically to maintain location awareness within the network.
- **SOS packets:** Broadcasts high-priority emergency distress signals to alert nearby nodes of a critical situation.
- **Acknowledgment packets:** Confirms the successful receipt of a message to ensure reliable data delivery and network integrity.
- **Presence beacons:** Broadcasts node status to signal availability and assist in network discovery and topology maintenance.

AES-128 encryption protects private communication channels according to modern IoT security practices.

8. Security Mechanisms

Security is crucial in decentralized communication systems.

EchoMesh implements:

- **AES-128 encryption:** Scrambles message data using a secure key to prevent unauthorized access and protect user privacy.
- **Unique packet identifiers:** Assigns a distinct code to every data packet, ensuring messages are not processed or counted twice.
- **Channel-based communication:** Restricts data exchange to specific logical channels, isolating group conversations from others.
- **BLE pairing protection:** Secures the wireless connection between the LoRa hardware and the smartphone to prevent unauthorized access.
- **Packet authentication mechanisms:** Verifies that a received message truly originated from a trusted source, preventing data spoofing.

The encryption process uses CTR mode to ensure low computational load while maintaining confidentiality.

9. Experimental Setup

9.1 Hardware Setup

The prototype nodes were built from:

- **TTGO T-Beam ESP32 boards:** Serves as the primary microcontroller node, integrating the LoRa transceiver, GPS, and power management on a single compact board.
- **SX1276 LoRa radios:** Handles long-range, low-power data transmission over sub-GHz ISM frequency bands.
- **OLED displays:** Provide a visual interface on each node to show real-time network status, messages, and battery levels.
- **18650 Li-ion batteries:** Powers the portable nodes, offering sufficient capacity for prolonged field operation.
- **GPS modules:** Capture accurate location coordinates for tracking nodes and enabling location-based services in the mesh network.

9.2 Test Environment

Experiments were conducted in:

- **Urban environments:** Test signal propagation and interference resilience in densely built-up areas with high signal reflection.

- **Open rural fields:** Evaluates maximum communication range and link reliability in unobstructed, low-noise environments.
- **Indoor settings with obstacles:** Assesses signal penetration and multi-hop stability through walls and various physical barriers.

9.3 Metrics Evaluated

The following metrics were measured:

- **Communication range:** Measures the maximum distance over which nodes can successfully exchange data packets under different environmental conditions.
- **Packet delivery ratio:** Calculates the percentage of successfully received packets compared to the total sent to evaluate network reliability.
- **Battery consumption:** Monitors the power usage of nodes over time to optimize energy efficiency and operational lifespan.
- **Message latency:** Determines the time delay required for a packet to travel from the source to the destination node.
- **Multi-hop reliability:** Assesses the network's ability to maintain stable connections when data must pass through several intermediate relay nodes.
- GPS update success

10. Results and Discussion

10.1 Communication Range

The LoRa mesh network achieved:

- 1–2 km in dense urban areas
- 5–10 km in rural areas with line-of-sight

The communication range varied depending on antenna orientation, terrain, and environmental interference.

10.2 Power Consumption

The average battery life ranged between:

- 10–14 hours with active communication
- Several days under low-duty-cycle operation

Power optimization methods like sleep modes significantly enhanced efficiency.

10.3 Mesh Routing Performance

The mesh routing mechanism successfully relayed packets across multiple nodes with high delivery rates. Preventing packet duplication improved network stability.

10.4 BLE Integration

The BLE communication system enabled reliable smartphone integration for:

- Real-time messaging
- Device configuration
- GPS visualization
- Emergency control

11. Applications of EchoMesh

EchoMesh can be applied in various areas:

11.1 Disaster Response

Emergency responders can maintain communication even when cellular infrastructure fails.

11.2 Rural Connectivity

Remote villages without network coverage can establish community communication systems.

11.3 Military and Tactical Communication

Military units can use this system to coordinate movements and share secure, real-time location data during operations in remote areas without relying on vulnerable public networks.

11.4 Adventure and Expedition Use

Trekkers, hikers, and mountaineers can keep in touch in remote locations.

11.5 Event Management

Event organizers can use the system to keep staff and security teams connected at large festivals or sports events, especially where cellular networks become overcrowded or fail.

12. Advantages of EchoMesh

- **Infrastructure-independent communication:** Allows users to connect without relying on cell towers or internet services.
- **Low power consumption:** Enables devices to operate for long periods on small battery supplies.
- **Long-range capability:** Supports communication over several kilometers, making it ideal for wide-area coverage.
- **Low deployment cost:** Uses affordable components, making it accessible for communities and budget-constrained projects.
- **Open-source flexibility:** Provides open design files and code, allowing users to modify or improve the system as needed.
- **Smartphone integration:** Connects easily to mobile devices via Bluetooth, providing a user-friendly interface.
- **GPS tracking support:** Allows users to share and view precise location coordinates for navigation or rescue purposes.
- **Multi-hop scalability:** Extends the network reach by automatically relaying messages through intermediate nodes.
- **Secure encrypted channels:** Protects privacy by scrambling message data so only authorized recipients can read it.
- **Quick deployment in disasters:** Sets up rapidly to provide essential communication links when standard networks fail.

13. Limitations

Despite its benefits, EchoMesh has several limitations:

- **Low data transmission rates:** Data moves slowly, making it unsuitable for sending large files.
- **Limited bandwidth for multimedia communication:** The network cannot handle heavy media like high-quality video or large image files effectively.
- **Regulatory restrictions on ISM frequencies:** Local government rules on radio usage may restrict operation in certain regions.

- **Possible interference in crowded radio environments:** Many devices sharing the same radio band can create signal noise.
- **Voice communication constraints over LoRa:** Transmitting clear audio is challenging due to the technology's low data capacity.
- **Increased latency with additional hops:** Every relay step adds a slight delay to the message's total travel time.

14. Future Scope

Future enhancements to the EchoMesh system will focus on integrating AI-assisted routing, satellite and UAV gateway connectivity, solar charging, advanced mesh synchronization, dynamic frequency adaptation, improved voice codecs, edge AI for disaster analytics, blockchain-based decentralized identity, secure over-the-air firmware updates, and hybrid communication capabilities using LoRa, Wi-Fi Direct, and satellite uplinks.

15. Conclusion

This research presented EchoMesh, a decentralized off-grid communication system based on LoRa mesh networking technology. The proposed architecture demonstrates that low-cost embedded systems can provide reliable long-range communication without dependence on traditional infrastructure. The integration of LoRa, ESP32, BLE, GPS, and mesh routing creates a scalable communication framework suitable for emergency response, rural communication, and disaster management. Experimental analysis confirms that EchoMesh achieves long communication ranges with low power consumption while maintaining acceptable reliability in multi-hop scenarios. The research highlights the growing importance of decentralized communication systems in modern society, particularly in environments where infrastructure-based communication fails (Shah et al., 2019; Ranaweera et al., 2018). EchoMesh demonstrates the feasibility of creating affordable, scalable, and resilient communication networks capable of supporting emergency coordination and community resilience.

REFERENCES

- Adelantado, F., Vilajosana, X., Tuset-Peiro, P., Martinez, B., Melia-Segui, J., & Watteyne, T. (2017). Understanding the limits of LoRaWAN. *IEEE Communications Magazine*, 55(9), 34–40.
- Akyildiz, I. F., Wang, X., & Wang, W. (2005). Wireless mesh networks: A survey. *Computer Networks*, 47(4), 445–487.
- Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials*, 17(4), 2347–2376.
- Augustin, A., Yi, J., Clausen, T., & Townsley, W. (2016). A study of LoRa: Long range & low power networks for the Internet of Things. *Sensors*, 16(9), 1466.
- Bor, M., Vidler, J., & Roedig, U. (2016). LoRa for the Internet of Things. *Proceedings of the International Conference on Embedded Wireless Systems and Networks*.
- Centenaro, M., Vangelista, L., Zanella, A., & Zorzi, M. (2016). Long-range communications in unlicensed bands: The rising stars in the IoT and smart city scenarios. *IEEE Wireless Communications*, 23(5), 60–67.
- Gupta, D. N., & Kumar, R. (2019). Lightweight cryptography: An IoT perspective. *International Journal of Innovative Technology and Exploring Engineering*, 8(8), 700-706.
- Gupta, D. N., & Kumar, R. (2020). Networking in IoT: Technologies used, security threats and possible countermeasures. *International Journal of Sensors, Wireless Communications and Control*, 10(1).
- Cotrim, J. R., & Kleinschmidt, J. H. (2020). LoRaWAN mesh networks: A review and classification of multihop communication. *Sensors*, 20(15), 4273.
- Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6), 644–654.
- Georgiou, O., & Raza, U. (2017). Low power wide area network analysis: Can LoRa scale? *IEEE Wireless Communications Letters*, 6(2), 162–165.
- Gupta, D. N., & Kumar, R. (2022a). An IoT approach of managing smart healthcare services. In *Networking Technologies in Smart Healthcare: Innovations and Analytical Approaches* (pp. 398). CRC Press.
- Gupta, D. N., & Kumar, R. (2022b). Multi-layer and clustering-based security implementation for an IoT environment. *International Journal of System Dynamics Applications*, 11(2), 1-21.
- Gupta, D. N., & Kumar, R. (2023a). DeeR-Hash: A lightweight hash construction for Industry 4.0 / IoT. *Journal of Scientific & Industrial Research*, 82(1), 142-150.
- Gupta, D. N., & Kumar, R. (2023b). DeeR-Gen: A pseudo random number generator for Industry 4.0 / IoT. *Journal of Scientific & Industrial Research*, 82(3), 316-321.
- Gomez, C., Oller, J., & Paradells, J. (2012). Overview and evaluation of Bluetooth low energy. *Sensors*, 12(9), 11734–11753.
- Mekki, K., Bajic, E., Chaxel, F., & Meyer, F. (2019). A comparative study of LPWAN technologies for large-scale IoT deployment. *ICT Express*, 5(1), 1–7.
- Perrig, A., Szewczyk, R., Wen, V., Culler, D., & Tygar, J. D. (2002). SPINS: Security protocols for sensor networks. *Wireless Networks*, 8(5), 521–534.
- Ranaweera, P., Agrawal, D. P., & Jayalath, D. (2018). Emergency communication networks: A contemporary survey. *IEEE Communications Surveys & Tutorials*, 20(4), 2486–2529.
- Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed Internet of Things. *Computer Networks*, 57(10), 2266–2279.

- Raza, U., Kulkarni, P., & Sooriyabandara, M. (2017). Low power wide area networks: An overview. *IEEE Communications Surveys & Tutorials*, 19(2), 855–873.
- Sanchez-Iborra, R., & Cano, M. D. (2016). State of the art in LP-WAN solutions for industrial IoT services. *Sensors*, 16(5), 708.
- Shah, S. A., Seker, D. Z., Hameed, S., & Draheim, D. (2019). The rising role of big data analytics and IoT in disaster management. *International Journal of Information Management*, 45, 195–207.
- Siekkinen, M., Hienkari, M., Nurminen, J. K., & Nieminen, J. (2012). How low energy is Bluetooth low energy? Comparative measurements with ZigBee/802.15.4. *Proceedings of IEEE WCNC*.
- Tiwari, D., & Sharma, V. (2020). A Review on Conventional and Lightweight Security Techniques in Mobile and IoT Devices. *Journal of Information and Computational Science*, 12(12).
- Voigt, T., Bor, M., Roedig, U., Alonso, J., & Montavont, J. (2017). Mitigating inter-network interference in LoRa networks. *Proceedings of EWSN*.
- Vangelista, L. (2017). Frequency shift chirp modulation: The LoRa modulation. *IEEE Signal Processing Letters*, 24(12), 1818–1821.
- Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of Things for smart cities. *IEEE Internet of Things Journal*, 1(1), 22–32.

Infocognitive Dynamics Framework: A Unified Paradigm for Data Science and Big Data Analytics

Ram Dutt Rikhari

Maharishi University of Information Technology, Noida (U.P.), India
rikhari.ipec@gmail.com

ARTICLE INFO <i>Article history:</i> Received 19 May 2026 Received in revised form 09 June 2026 Accepted 12 June 2026 Available online 12 July 2026 <i>Keywords:</i> Data Science Big Data Analytics Infocognitive Dynamics Framework Cognitive Intelligence Machine Learning Adaptive Learning Intelligent Decision-Making	ABSTRACT <i>In the contemporary digital ecosystem, the rapid growth of structured, semi-structured, and unstructured data has significantly transformed the field of intelligent computing and analytical decision-making. Organizations, industries, and research communities continuously generate enormous volumes of data through cloud platforms, Internet of Things (IoT) devices, social media systems, enterprise applications, and real-time digital infrastructures. Managing, processing, and extracting meaningful knowledge from these complex and high-dimensional datasets has become one of the major challenges in modern computational environments. Although Data Science and Big Data Analytics provide efficient techniques for data processing and predictive analysis, most existing analytical systems still operate primarily on computational logic and statistical prediction mechanisms without incorporating adaptive cognitive reasoning and contextual understanding. This chapter introduces the Infocognitive Dynamics Framework (IDF), which presents a unified and adaptive paradigm integrating Data Science, Big Data Analytics, Machine Learning, Cognitive Reasoning, and Adaptive Learning within a single intelligent analytical architecture. The proposed framework extends conventional analytical models by incorporating contextual interpretation, feedback-driven learning, and intelligent reasoning mechanisms to support real-time and context-aware decision-making. Unlike traditional systems that rely only on predictive outputs, the proposed architecture continuously evolves through adaptive feedback integration and cognitive interpretation. The chapter further explains the mathematical foundation, layered architecture, operational workflow, comparative analysis, and practical applications of the proposed framework across multiple domains including healthcare, education, business intelligence, and smart city management. The study demonstrates that the integration of analytical intelligence with cognitive reasoning can significantly enhance intelligent automation, predictive efficiency, contextual adaptability, and real-time analytical responsiveness. Finally, the chapter highlights future research opportunities associated with Explainable Artificial Intelligence, Generative AI, adaptive autonomous systems, and cognitive computing environments.</i>
---	---

1. Introduction

The rapid advancement of digital technologies has fundamentally transformed the modern information ecosystem and created an unprecedented growth in global data generation [1], [7]. In recent years, organizations, industries, educational institutions, healthcare systems, and governmental infrastructures have increasingly relied on digital platforms for communication, automation, storage, and decision-making processes. Technologies such as cloud computing, Internet of Things (IoT), social media systems, mobile applications, e-commerce platforms, and intelligent sensor networks continuously generate

massive volumes of structured and unstructured data[1]. This phenomenon, commonly referred to as Big Data, has created significant opportunities for extracting meaningful insights while simultaneously introducing complex challenges related to scalability, data diversity, processing speed, and intelligent interpretation.

Big Data is commonly characterized through the five-dimensional analytical model consisting of Volume, Velocity, Variety, Veracity, and Value [1], [7]. The enormous scale of data generation requires advanced computational infrastructures capable of handling continuous streams of heterogeneous information in real time. Traditional database management systems and conventional

analytical architectures often struggle to process high-dimensional datasets efficiently because they were originally designed for static and relatively small-scale environments. As a result, the limitations of conventional systems have motivated researchers to develop scalable analytical frameworks capable of supporting intelligent data processing, predictive analytics, and automated decision-making mechanisms [5]. Data Science has emerged as an interdisciplinary field that integrates statistics, mathematics, computer science, machine learning, and artificial intelligence to extract meaningful knowledge from raw datasets [2],[4]. Modern Data Science methodologies involve data acquisition, preprocessing, feature engineering, predictive modelling, visualization, and intelligent interpretation of analytical outputs. Simultaneously, Big Data Analytics focuses on distributed computing architectures and scalable computational techniques capable of processing high-volume and high-velocity datasets generated across modern digital ecosystems [1]. These technologies have significantly improved analytical accuracy, automation capabilities, and predictive performance across multiple domains. Despite these advancements, most existing analytical systems still operate primarily on computational intelligence rather than cognitive intelligence [8]. Conventional frameworks generally focus on statistical prediction, pattern recognition, and automated analytics while lacking contextual understanding, adaptive reasoning, and intelligent interpretation capabilities. In many real-world environments, intelligent decision-making requires more than numerical prediction because analytical outcomes must also be interpreted according to contextual conditions, environmental factors, and dynamic operational requirements. Consequently, current systems often fail to provide adaptive and context-aware analytical responses in highly dynamic environments [10].

To address these limitations, this chapter proposes the Infocognitive Dynamics Framework (IDF), which introduces a unified analytical architecture integrating Data Science, Big Data Analytics, Machine Learning, Cognitive Reasoning, and

Adaptive Learning mechanisms within a single intelligent ecosystem. The proposed framework incorporates a feedback-driven operational mechanism capable of continuously learning from analytical outcomes and improving future decision-making performance dynamically. Unlike traditional systems that process data through static computational pipelines, the proposed framework functions as an adaptive and self-improving intelligent architecture capable of contextual reasoning and real-time analytical responsiveness[8].

The primary objective of this chapter is to establish a comprehensive conceptual and operational foundation for integrating cognitive intelligence with analytical intelligence in modern data-driven environments. The study further examines the mathematical representation, layered architecture, dynamic workflow, comparative advantages, application domains, and future research opportunities associated with the proposed framework. The chapter ultimately contributes toward the development of next-generation intelligent analytical ecosystems capable of supporting adaptive computing, intelligent automation, and context-aware decision-making processes [3], [10].

2. Literature Review and Research

Background

The field of Big Data Analytics and intelligent computing has evolved significantly during the last decade due to the increasing availability of large-scale digital datasets and advancements in computational technologies [1], [7]. Several researchers have explored scalable analytical architectures, machine learning systems, and intelligent computational frameworks to improve data-driven decision-making processes. Chen et al [1]. discussed the foundational characteristics of Big Data and emphasized the importance of distributed processing architectures for handling high-volume and high-velocity datasets. Their work highlighted scalability and computational efficiency as major components of modern analytical systems; however, the proposed approaches primarily focused on processing

capability rather than contextual intelligence and adaptive reasoning mechanisms.

Davenport and Patil [2] emphasized the growing importance of Data Science in organizational decision-making and business intelligence systems. Their study demonstrated how data-driven analytical approaches can improve strategic planning, predictive analytics, and automated operational processes. Although their work established the importance of analytical intelligence, it did not sufficiently address the integration of cognitive reasoning and adaptive contextual interpretation within intelligent analytical systems. Consequently, existing decision-making architectures continued to rely heavily on statistical outputs without incorporating human-like reasoning capabilities.

Jordan and Mitchell [3] examined the growing impact of Machine Learning in predictive modelling and intelligent automation. Their research highlighted how machine learning algorithms significantly improved analytical accuracy, pattern recognition, and predictive performance across multiple domains. However, most machine learning models still functioned primarily as computational prediction systems lacking contextual understanding and adaptive reasoning capabilities. While these approaches improved automation efficiency, they remained limited in their ability to interpret analytical outcomes dynamically according to changing operational conditions [6].

Recent advancements in cognitive computing, Explainable Artificial Intelligence (XAI), and

adaptive intelligent systems have attempted to bridge the gap between computational intelligence and human reasoning [8], [10]. Researchers have increasingly focused on integrating knowledge representation, contextual interpretation, and intelligent reasoning within analytical systems to improve transparency, adaptability, and decision quality. Nevertheless, many existing frameworks still operate as isolated analytical models without incorporating continuous feedback-driven learning and adaptive cognitive mechanisms.

The existing literature clearly demonstrates that although substantial progress has been achieved in Data Science, Machine Learning, and Big Data Analytics [1], [3] current analytical architectures still face several critical limitations. Most conventional systems lack cognitive intelligence, adaptive contextual interpretation, real-time intelligent reasoning, and dynamic feedback integration mechanisms. These limitations justify the need for a unified and adaptive analytical framework capable of integrating computational intelligence with cognitive reasoning and continuous learning mechanisms. The proposed Infocognitive Dynamics Framework addresses these research gaps by introducing an intelligent multi-layered architecture that combines analytical processing, contextual cognition, adaptive learning, and real-time decision optimization within a unified operational ecosystem[8], [10].

TABLE 1
Comparative Analysis of Existing Analytical and Cognitive Frameworks

Reference	Methodology	Major Contribution	Limitation	Proposed Improvement in IDF
Chen et al. (2014) [1]	Big Data Architecture	Distributed data processing	Lack of cognitive reasoning	Integration of contextual intelligence
Davenport and Patil (2012) [2]	Data Science Decision Systems	Data-driven analytics	Limited adaptive learning	Feedback-driven intelligent processing
Jordan and Mitchell (2015) [3]	Machine Learning Models	Predictive analytics	Weak contextual interpretation	Cognitive reasoning integration
Russell and Norvig (2021) [8]	Artificial Intelligence Systems	Intelligent automation	Limited real-time adaptability	Dynamic operational learning

Samek et al. (2021) [10]	Explainable AI	Improved interpretability	Limited integrated architecture	Unified cognitive analytical framework
Proposed IDF	Infocognitive Dynamics Framework	Cognitive analytics and adaptive intelligence	Computational complexity challenges	Context-aware intelligent ecosystem

Table 1 presents a comparative analysis of major existing research contributions associated with Big Data Analytics, Data Science, Machine Learning, and Cognitive Intelligence systems. The analysis demonstrates that although previous studies significantly improved analytical processing and predictive modelling, most existing frameworks lack adaptive cognitive reasoning, contextual interpretation, and feedback-driven learning mechanisms. The proposed Infocognitive Dynamics Framework extends existing analytical architectures by integrating cognitive intelligence and adaptive learning within a unified intelligent decision-making environment [8], [10].

3. Proposed Infocognitive Dynamics

Framework

The conceptual foundation of the proposed Infocognitive Dynamics Framework is based on the integration of analytical intelligence and cognitive intelligence within a unified computational environment [3], [8]. Modern intelligent systems increasingly require the capability not only to process data efficiently but also to interpret analytical outcomes according to contextual conditions and operational objectives. Conventional analytical systems generally focus on statistical computation, pattern recognition, and predictive modelling, whereas intelligent cognitive systems require adaptive reasoning, contextual understanding, and continuous learning capabilities [10].

Big Data environments are inherently complex because they involve heterogeneous datasets generated from multiple sources such as IoT devices, enterprise systems, social media platforms, cloud infrastructures, and real-time streaming applications[1], [7]. The diversity and scale of these datasets require scalable analytical architectures capable of handling dynamic operational conditions efficiently. Data Science

methodologies support this process through data acquisition, preprocessing, visualization, predictive analytics, and intelligent modeling techniques [2], [4]. However, the integration of cognitive reasoning mechanisms remains relatively limited in many existing analytical architectures.

Machine Learning further enhances analytical intelligence by enabling systems to identify hidden patterns and improve performance through iterative learning mechanisms. Supervised learning algorithms support predictive modelling, unsupervised learning enables pattern discovery, and reinforcement learning supports adaptive optimization in dynamic environments. Despite these advancements, machine learning systems often operate without contextual understanding and therefore cannot fully replicate intelligent human decision-making processes [8].

The proposed framework addresses these limitations by integrating cognitive reasoning and adaptive learning within the analytical workflow. Cognitive intelligence enables systems to interpret analytical outputs according to environmental conditions, knowledge representation structures, and contextual operational requirements. Simultaneously, adaptive learning mechanisms enable the framework to continuously improve future decision-making performance using feedback-driven optimization processes. Consequently, the framework establishes a self-improving analytical ecosystem capable of intelligent automation, contextual adaptation, and real-time operational responsiveness [8], [10].

The proposed Infocognitive Dynamics Framework introduces a unified intelligent analytical architecture integrating Data Science, Big Data Analytics, and Machine Learning, Cognitive Reasoning, and Adaptive Learning mechanisms within a multi-layered operational ecosystem [1], [3], [8]. The framework is designed to overcome the limitations of conventional analytical systems by enabling context-aware decision-making,

adaptive feedback learning, and intelligent interpretation of analytical outputs [10].

The framework operates as a continuous and dynamic analytical cycle in which data flows sequentially through interconnected layers responsible for acquisition, preprocessing, analytical modelling, cognitive reasoning, and adaptive execution [1], [4]. Unlike traditional computational systems that function through static and unidirectional pipelines, the proposed architecture continuously evolves by incorporating feedback from operational outcomes and environmental conditions. This adaptive operational behaviour significantly improves analytical efficiency, predictive accuracy, and contextual intelligence in real-time environments [3], [8].

The proposed framework also establishes an integrated relationship between computational intelligence and cognitive intelligence. Analytical intelligence supports data processing, machine learning, predictive analytics, and pattern recognition [3], [6], whereas cognitive intelligence enables contextual interpretation, knowledge-based reasoning, and adaptive decision generation [8], [10]. Through the integration of these mechanisms, the framework supports intelligent automation and adaptive optimization across multiple application domains [1], [7].

4. Mathematical Representation of the Framework

The mathematical foundation of the proposed framework provides a conceptual representation of the interaction between Data Science, Big Data Analytics, Machine Learning, Cognitive Reasoning, and Adaptive Learning mechanisms [1], [3], [8]. These mathematical models describe the operational behaviour, adaptive learning capability, and intelligent analytical processes associated with the proposed architecture [10].

4.1 Mathematical Representation of Big Data Growth

$$BD_t = BD_0 e^{\lambda t} \quad (1)$$

Equation (1) represents the exponential growth of digital data generated through IoT devices, cloud infrastructures, enterprise applications, and social media systems [1], [7]. Here, BD_t represents the data volume at time t , BD_0 denotes the initial data volume, and λ represents the data growth coefficient. This equation demonstrates the continuously increasing nature of digital data generation in modern computational environments.

4.2 Core Equation of the IDF

$$IDF = (DS + BDA + ML + CR) \times AL \quad (2)$$

Equation (2) represents the integrated operational structure of the proposed IDF [3], [8]. In this equation, DS refers to Data Science, BDA denotes Big Data Analytics, ML represents Machine Learning, CR corresponds to Cognitive Reasoning, and AL represents Adaptive Learning. The equation explains that intelligent analytical performance is achieved through the integration of analytical intelligence, cognitive reasoning, and adaptive learning mechanisms.

4.3 Intelligent Decision-Making Function

$$D_i = f(D_p, ML, CR, F_b) \quad (3)$$

Equation (3) defines the intelligent decision-making process within the proposed framework [3], [8]. Here, D_i represents intelligent decisions, D_p denotes processed data, ML represents machine learning outputs, CR corresponds to cognitive reasoning, and F_b indicates the feedback mechanism. The equation demonstrates that intelligent decisions are generated through the combined interaction of analytical outputs, contextual reasoning, and adaptive feedback learning [10].

4.4 Predictive Analytics Representation

$$Y = f(X) + \epsilon \quad (4)$$

Equation (4) represents the predictive analytics model used within the Analytical Intelligence Layer of the proposed framework [3], [6]. In this equation, Y denotes the predicted output generated by the analytical model, X represents the input data variables, and ϵ (epsilon) indicates the prediction error associated with the analytical process. The equation demonstrates how machine

learning algorithms analyze multidimensional datasets to generate predictive insights and intelligent analytical outcomes. The predictive model supports data-driven decision-making by identifying hidden relationships, behavioural patterns, and future trends within complex datasets [2], [4].

4.5 Adaptive Learning Feedback Equation

$$L_{t+1} = L_t + \alpha F_t \quad (5)$$

Equation (5) describes the adaptive learning capability of the proposed IDF [8], [10]. In this equation, L_t represents the current learning state of the system, L_{t+1} denotes the updated learning state after feedback integration, α represents the learning coefficient, and F_t indicates the feedback input generated from previous analytical outcomes. The equation demonstrates how the framework continuously improves its analytical performance and decision-making capability through feedback-driven optimization and adaptive learning mechanisms. This adaptive behaviour enables the system to dynamically respond to changing operational environments and improve future analytical accuracy over time [3], [8].

4.6 Cognitive Intelligence Representation

$$CI = K + R + C \quad (6)$$

Equation (6) mathematically represents the Cognitive Intelligence component of the proposed framework [8], [10]. In this equation, CI denotes Cognitive Intelligence, K represents the knowledge base, R corresponds to reasoning capability, and C indicates contextual understanding. The formulation explains that intelligent cognition is achieved through the integration of knowledge representation, logical reasoning processes, and contextual interpretation mechanisms. This equation highlights the importance of combining analytical intelligence with cognitive understanding to support intelligent, context-aware, and adaptive decision-making within complex computational environments.

5. Framework Architecture and Dynamic Operational Workflow

The proposed Infocognitive Dynamics Framework operates through a multi-layered intelligent architecture designed to support scalable data processing, analytical intelligence, cognitive reasoning, adaptive learning, and real-time decision-making [1], [3], [8]. The framework functions as a continuous feedback-driven ecosystem in which data flows sequentially through interconnected operational layers while adaptive learning mechanisms continuously improve analytical performance [10].

The first layer of the framework is the Data Acquisition Layer, which is responsible for collecting structured, semi-structured, and unstructured data from multiple sources including IoT devices, databases, cloud infrastructures, enterprise systems, sensors, web platforms, and social media environments [1],[7]. This layer ensures efficient data ingestion and supports continuous data acquisition from dynamic operational ecosystems.

The second operational layer is the Data Processing Layer, where raw datasets undergo preprocessing operations such as data cleaning, transformation, normalization, integration, and quality assurance [4], [5]. This layer prepares heterogeneous datasets for analytical processing and significantly improves data reliability and computational efficiency.

The third layer is the Analytical Intelligence Layer, which applies statistical analysis, machine learning models, predictive analytics, pattern recognition algorithms, and intelligent computational techniques to generate meaningful insights from processed datasets [3], [6]. This layer forms the computational intelligence component of the proposed framework and supports predictive modelling and intelligent analytical operations.

The fourth and most innovative layer is the Cognitive Reasoning Layer, which introduces contextual interpretation, knowledge-based reasoning, adaptive cognition, and intelligent decision logic within the analytical workflow [8], [10]. Unlike traditional systems that rely exclusively on predictive outputs, this layer

enables human-like contextual understanding and adaptive interpretation of analytical results.

The final operational layer is the Adaptive Application Layer, which implements intelligent decisions in real-world applications while continuously monitoring operational outcomes. The feedback generated from decision execution is reintegrated into the framework, thereby enabling adaptive learning, system optimization, and continuous performance improvement [8], [10].

The operational mechanism of the proposed framework functions as a continuous and adaptive analytical cycle rather than a conventional linear processing pipeline [1], [3]. Initially, data is collected from multiple internal and external sources and subsequently transferred to the preprocessing layer, where it is cleaned, transformed, integrated, and validated [4], [5]. The processed datasets are then analyzed using machine learning models and analytical algorithms to generate predictive insights and intelligent analytical outputs [3], [6].

Unlike conventional analytical architectures, the generated outputs are not directly utilized for

decision-making. Instead, they are transferred to the Cognitive Reasoning Layer, where contextual interpretation, intelligent reasoning, environmental evaluation, and knowledge representation mechanisms are applied [8], [10]. This cognitive interpretation process enables the system to evaluate the significance, relevance, and contextual implications of analytical results according to dynamic operational conditions.

Following cognitive evaluation, the framework generates intelligent decisions and adaptive operational responses that are implemented within real-world applications. The outcomes of these decisions are continuously monitored and fed back into the framework through adaptive learning mechanisms [8], [10]. This feedback-driven process allows the system to improve future analytical performance, refine knowledge representation structures, and dynamically optimize decision-making efficiency over time.

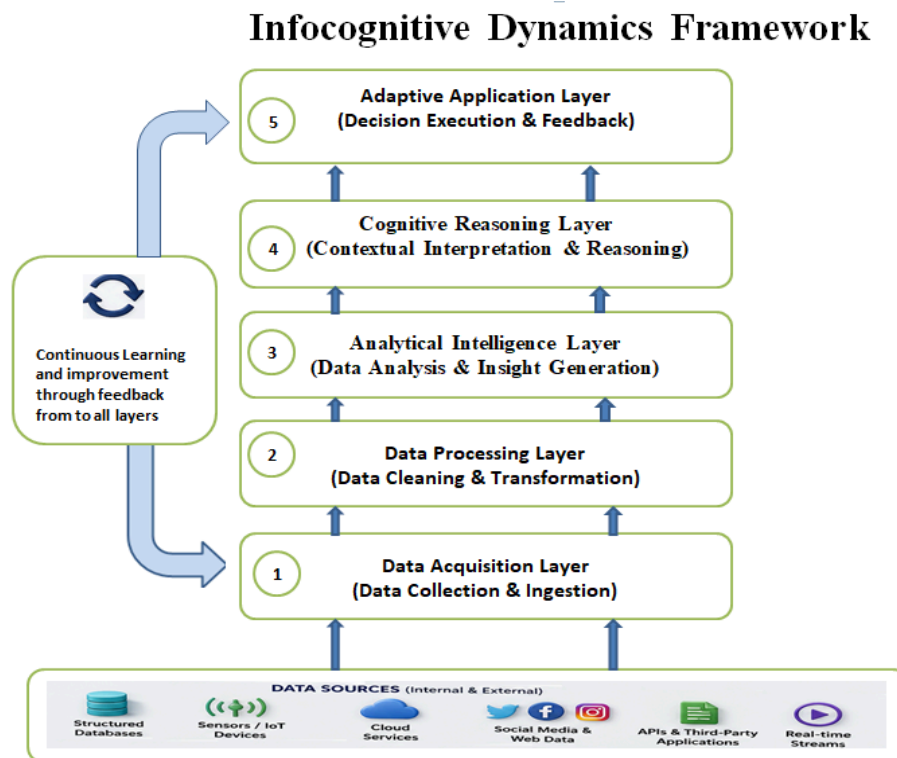


Figure 1. Layered Architecture of the Proposed IDF

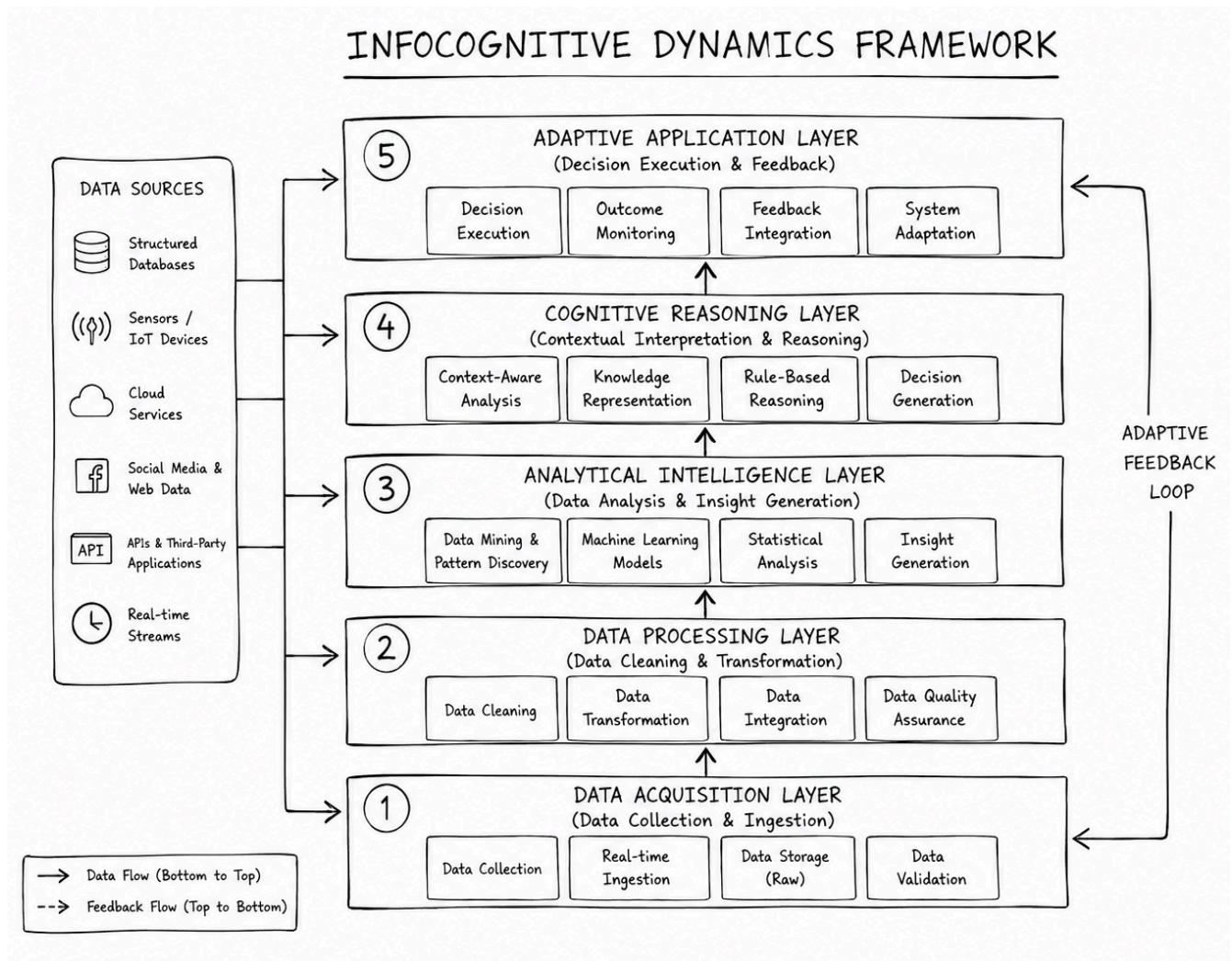


Figure 2. Dynamic Working Mechanism and Feedback Architecture of the Proposed IDF

6. Comparative Analysis of Traditional Systems and Proposed IDF

The proposed Infocognitive Dynamics Framework demonstrates significant improvements over conventional analytical architectures in terms of contextual intelligence, adaptive learning capability, real-time responsiveness, and intelligent decision generation [3], [8], [10]. Traditional analytical systems primarily focus on

computational processing and predictive modelling, whereas the proposed framework integrates analytical intelligence with cognitive reasoning and adaptive feedback learning [1], [3]. The comparative analysis clearly demonstrates that the proposed framework provides enhanced intelligent processing capabilities through the integration of cognitive intelligence and adaptive learning mechanisms [8], [10]. The framework supports real-time decision-making, context-aware analytics, intelligent automation, and dynamic optimization more effectively than conventional analytical systems [1], [3], [6].

Comparative Analysis of Analytical Frameworks

Comparison between traditional analytical systems and the proposed Infocognitive Dynamics Framework.

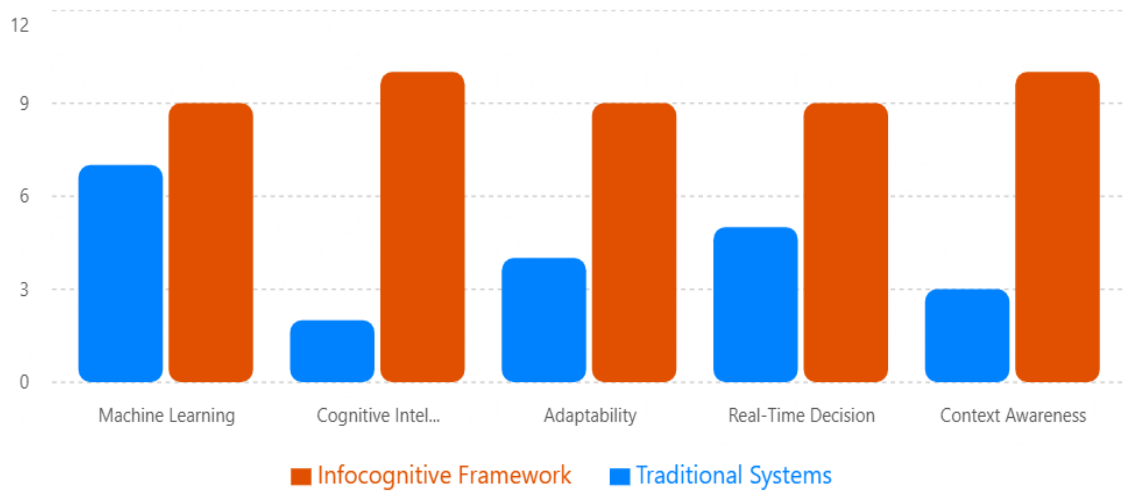


Figure 3. Comparative Analysis of Traditional Analytical Systems and Proposed IDF

TABLE 2

Comparative Analysis of Traditional Systems and Proposed IDF

Feature	Traditional Analytical Systems	Proposed IDF
Machine Learning Capability	Moderate	Advanced
Cognitive Intelligence	Absent	Integrated
Adaptability	Low	High
Real-Time Decision-Making	Limited	Advanced
Context Awareness	Weak	Strong
Feedback Learning	Minimal	Continuous
Intelligent Automation	Partial	Comprehensive
Dynamic Optimization	Limited	Adaptive

7. Application Domains of the Proposed Framework

The proposed Infocognitive Dynamics Framework demonstrates substantial applicability across multiple intelligent computing environments because of its adaptive, scalable, and context-aware operational architecture [1], [3], [8]. The integration of Big Data Analytics, Machine Learning, Cognitive Reasoning, and Adaptive Learning mechanisms enables the framework to

support intelligent analytical operations in complex real-world domains [10].

In the healthcare sector, the framework can support predictive diagnostics, intelligent patient monitoring, personalized treatment planning, and disease risk prediction through the integration of clinical analytics, patient records, sensor networks, and cognitive interpretation models [3], [8]. The framework enables healthcare systems to improve medical decision-making accuracy while supporting real-time patient monitoring and adaptive healthcare optimization. For instance,

research [11] demonstrates the efficacy of phonocardiographic signal analysis in detecting cardiovascular diseases, underscoring the potential for integrating advanced analytical techniques in clinical diagnostic environments.

Within educational environments, the framework can facilitate adaptive learning systems, intelligent tutoring platforms, automated assessment mechanisms, and personalized educational analytics [2], [4]. By analyzing student learning behaviour and performance patterns, the framework can support customized educational strategies and improve learning outcomes through adaptive cognitive analytics. In business intelligence environments, the framework enables organizations to perform intelligent customer behaviour analysis, market trend prediction, strategic planning, and operational optimization [2], [5]. The integration of analytical intelligence and cognitive reasoning allows enterprises to generate context-aware business insights and improve intelligent decision-making processes. Furthermore, the transition toward Industry 5.0 represents a pivotal shift for modern enterprises. As discussed in [14], this era emphasizes the necessity of adaptive organizational strategies that harmonize human creativity with robotic efficiency to foster sustainable and collaborative industrial environments.

The framework is also highly applicable within smart city infrastructures, where real-time analytics, adaptive resource management, intelligent transportation systems, and urban monitoring mechanisms are required [1], [7]. Through continuous data acquisition and adaptive analytical processing, the framework can support intelligent traffic optimization, energy management, infrastructure monitoring, and resource allocation within modern smart city ecosystems.

8. Advantages and Limitations

The proposed Infocognitive Dynamics Framework offers several significant advantages compared with conventional analytical architectures [3], [8], [10]. One of the primary strengths of the framework is its ability to integrate analytical intelligence with cognitive reasoning and adaptive

learning within a unified operational ecosystem. This integration significantly enhances context-aware decision-making capability, intelligent automation, predictive analytics, and adaptive system optimization [1], [3].

Another important advantage of the framework is its feedback-driven operational mechanism, which enables continuous performance improvement and dynamic learning [8], [10]. Unlike static analytical systems that rely solely on predefined computational models, the proposed architecture continuously evolves according to operational feedback and environmental conditions. This adaptive behaviour improves analytical efficiency, responsiveness, and intelligent decision quality across multiple application domains [3], [6].

The scalable layered architecture of the framework further supports efficient processing of large-scale heterogeneous datasets generated through IoT devices, enterprise systems, cloud infrastructures, and real-time digital ecosystems [1], [7]. The framework also improves automation capability, operational efficiency, and intelligent analytical responsiveness in dynamic environments.

Despite these advantages, the implementation of the proposed framework also introduces several technical and operational challenges [8], [10]. The integration of multiple analytical and cognitive layers increases computational complexity and requires substantial processing capability, especially within large-scale real-time environments. Additionally, intelligent analytical systems operating on sensitive datasets raise concerns related to cybersecurity, ethical data management, and information privacy [1], [8]. Furthermore, protecting data transmission in resource-constrained IoT environments remains a critical challenge, as conventional security protocols often impose excessive computational overhead. Studies highlight the necessity of lightweight cryptographic solutions for secure communication in these environments [12].

Additionally, a research proposes distributed key generation mechanisms to enhance secure communication between actors in service-oriented, dense vehicular ad hoc networks (VANETs), further addressing the critical need for secure and

scalable data exchange in dynamic intelligent systems [15].

Beyond computational complexity, managing the inherent security risks in IoT-based deployments remains critical. As highlighted in a study, implementing robust security countermeasures, including secure network protocols and threat mitigation strategies, is essential for the operational reliability of modern intelligent frameworks [13].

The development and deployment of such integrated intelligent architectures also require specialized expertise in Data Science, Artificial Intelligence, Machine Learning, Cognitive Computing, and distributed analytical systems [2], [3], [8]. Consequently, although the proposed framework offers significant advancements over conventional analytical architectures, further research is required to improve computational efficiency, implementation scalability, and security optimization [10].

9. Future Scope

The proposed Infocognitive Dynamics Framework establishes a strong foundation for future intelligent analytical ecosystems and opens several promising research directions associated with adaptive computing and cognitive intelligence [8], [10]. One important future direction involves the integration of Generative Artificial Intelligence technologies within the framework to support automated content generation, intelligent reasoning, and advanced adaptive decision-making mechanisms [3], [8].

Another promising research area involves the incorporation of Explainable Artificial Intelligence techniques to improve transparency, interpretability, and trustworthiness in intelligent decision-making environments [10]. Explainable cognitive systems can significantly enhance user confidence and support ethical analytical operations within healthcare, finance, education, and governmental systems [1], [2].

Future research may also focus on autonomous intelligent architectures capable of self-learning, self-optimization, and context-aware adaptation without extensive human intervention [3], [8]. The integration of reinforcement learning, deep

learning, and human-centered AI models can further improve adaptive analytical performance and intelligent automation capabilities [6], [10].

The incorporation of Edge AI, quantum-assisted analytics, and distributed intelligent infrastructures may significantly enhance computational efficiency, scalability, and real-time responsiveness in complex operational environments [1], [7]. These advancements have the potential to transform the proposed framework into a fully adaptive and self-evolving intelligent analytical ecosystem capable of supporting next-generation cognitive computing applications [8], [10].

10. Conclusion

The proposed Infocognitive Dynamics Framework introduces a novel and adaptive analytical paradigm integrating Data Science, Big Data Analytics, Machine Learning, Cognitive Reasoning, and Adaptive Learning within a unified intelligent decision-making architecture [1], [3], [8]. Unlike conventional analytical systems that primarily focus on computational processing and predictive modelling, the proposed framework incorporates contextual understanding, adaptive reasoning, and feedback-driven learning mechanisms to support intelligent and context-aware analytical operations [10].

The study demonstrates that the integration of analytical intelligence with cognitive intelligence can significantly improve predictive analytics, intelligent automation, adaptive learning, and real-time decision-making performance in dynamic operational environments [3], [6], [8]. Through its multi-layered architecture and continuous feedback mechanism, the framework supports intelligent interpretation, dynamic optimization, and self-improving analytical behaviour across multiple application domains including healthcare, education, business intelligence, and smart city infrastructures [1], [2], [7].

The proposed framework also contributes toward bridging the gap between traditional data-driven analytical systems and intelligent cognitive computing architectures [8], [10]. By integrating contextual reasoning and adaptive intelligence within analytical workflows, the framework

establishes a scalable foundation for future intelligent analytical ecosystems and next-generation adaptive computing environments [3], [6].

Although the framework presents substantial advantages, additional research is required to address challenges related to computational complexity, large-scale deployment, cyber security, and implementation scalability [1], [8]. Future advancements in Generative AI, Explainable Artificial Intelligence, autonomous intelligent systems, and adaptive cognitive computing may further enhance the operational capability and applicability of the proposed framework [10]. Overall, the Infocognitive Dynamics Framework represents a significant step toward the development of intelligent, adaptive, and context-aware analytical architectures for future digital ecosystems [3], [8], [10].

REFERENCES

- [1] Chen, M., Mao, S., & Liu, Y. (2014). Big data: A survey. *Mobile Networks and Applications*, 19(2), 171–209.
- [2] Davenport, T. H., & Patil, D. J. (2012). Data scientist: The sexiest job of the 21st century. *Harvard Business Review*.
- [3] Jordan, M. I., & Mitchell, T. M. (2015). Machine learning: Trends, perspectives, and prospects. *Science*, 349(6245), 255–260.
- [4] Kelleher, J. D., & Tierney, B. (2018). *Data Science*. MIT Press.
- [5] Aggarwal, C. C. (2015). *Data Mining: The Textbook*. Springer.
- [6] Witten, I. H., Frank, E., Hall, M. A., & Pal, C. J. (2016). *Data Mining: Practical Machine Learning Tools and Techniques*. Morgan Kaufmann.
- [7] Mayer-Schönberger, V., & Cukier, K. (2013). *Big Data: A Revolution That Will Transform How We Live, Work, and Think*. Houghton Mifflin Harcourt.
- [8] Russell, S., & Norvig, P. (2021). *Artificial Intelligence: A Modern Approach*. Pearson.
- [9] Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep Learning*. MIT Press.
- [10] Samek, W., Montavon, G., Lapuschkin, S., Anders, C. J., & Müller, K. R. (2021). Explaining deep neural networks and beyond: A review of methods and applications. *Proceedings of the IEEE*.
- [11] Gupta, D.N., Anand, R., Ahamad, S., Patil, T., Dhabliya, D., Gupta, A. (2023). Phonocardiographic Signal Analysis for the Detection of Cardiovascular Diseases. In: Bhateja, V., Carroll, F., Tavares, J.M.R.S., Sengar, S.S., Peer, P. (eds) *Intelligent Data Engineering and Analytics. FICTA 2023. Smart Innovation, Systems and Technologies*, vol 371. Springer, Singapore. https://doi.org/10.1007/978-981-99-6706-3_47
- [12] Gupta, D.N. & Kumar, R. (2020). Generating Random Binary Bit Sequences for Secure Communications between Constraint Devices under the IOT Environment. 2020 International Conference for Emerging Technology (INCET), 1-6. <https://doi.org/10.1109/INCET49848.2020.9154009>
- [13] Gupta, D. N., & Kumar, R. (2021). Networking in IoT: Technologies Usage, Security Threats, and Possible Countermeasures. *International Journal of Sensors, Wireless Communications and Control*, 11(6). <https://doi.org/10.2174/2210327910666210106090826>
- [14] Bhatia, K., Pandey, S. K., Singh, V. K., & Gupta, D. N. (2023). Enterprises in the Era of Industry 5.0. 2023 10th International Conference on Computing for Sustainable Global Development (INDIACom), 1065-1069.
- [15] Gupta, D. N., & Kumar, R. (2021). Distributed Key Generation for Secure Communications Between Different Actors in Service Oriented Highly Dense VANET. *Cloud and IoT-Based Vehicular Ad Hoc Networks*, 221-232.

Real-Time Vehicle RC Expiry Detection and Smart Challan System Using YOLOv8 and OCR

Saurabh Mallik¹, Shivangi Sharma², Mohd Tajammul³

¹Computer Science and Application, Sharda University, Gr. Noida, Uttar Pradesh, India
¹saurabhmallik07@gmail.com

²Computer Science and Application, Sharda University, Gr. Noida, Uttar Pradesh, India
²shivangi.sharma2603@gmail.com

³Computer Science and Application, Sharda University, Gr. Noida, Uttar Pradesh, India
³mohd.tajammul@sharda.ac.in

ARTICLE INFO

Article history:

Received 28 April 2026

Accepted 03 May 2026

Available online 12 July 2026

Keywords:

Computer Vision,
YOLOv8,
Optical Character Recognition (OCR),
Automatic Number Plate Recognition (ANPR),
Smart Challan System,
Intelligent Transportation Systems,
Flask,
Vehicle Monitoring

ABSTRACT

With urban traffic levels reaching unprecedented levels, manual RC verification has become impractical, being both time-consuming and highly unreliable in its results. This work presents a Real-Time Vehicle Registration Certificate (RC) Expiry Detection and Smart Challan Generation System based on automated verification via computer vision. Webcam frames serve as input data for the proposed solution which uses a YOLOv8 detector to detect and crop the area occupied by the vehicle's number plate. Next, the cropped image undergoes preprocessing, including a conversion to grayscale, Gaussian filtering, and adaptive thresholding. After that, the detected number plate is recognized using the Tesseract OCR engine. The obtained alphanumeric value is used to compare the vehicle against an SQLite database with vehicles' identification numbers and dates of their RC expiration. Upon successful detection of an expired RC, the system generates a PDF document (challan) with the relevant vehicle information, timestamp of the violation, exact location of occurrence, and fine amount automatically. The pipeline itself is exposed through a Flask-based web interface allowing operators to monitor detection and enforcement events in real-time. Extensive testing proved that the system has good performance in terms of number plate recognition efficiency, minimal processing latency, and consistent challan generation.

1. INTRODUCTION

With the number of vehicles plying urban roads increasing every day, there is an urgent need for improved traffic management and enforcement methods considering the limited capabilities of traditional surveillance mechanisms due to their vulnerability to human operator error [1]. To mitigate this challenge, ITS, with IoT devices and computer vision technology at the center of these solutions, have been gaining popularity lately as they can help keep track of vehicle activity, provide passenger safety and efficiency in transport systems [2]. Among the technologies that have contributed to these innovations, ANPR stands out with the ability to transform images of vehicles into text [3].

As for ANPRs, initially, classical computer vision was used to detect number plates, using quite simple

methods like edge detection, morphological transformations, and even recognition through templates using the principle of correlation factor [4]. While this technique proved to be relatively efficient in terms of computation, it lacked robustness under various challenging circumstances. As far as more recent advancements in Deep Learning are concerned, it can be stated that it has changed the entire face of ANPR, resulting in much better accuracy in difficult conditions, especially during low illumination or unfavorable weather like snowfall [5]. Modern ANPR software relies heavily on neural networks; specifically, popular YOLO architectures are utilized in the process of Localization of plates [6]. Moreover, OCR engines (Tesseract or EasyOCR) are used for the identification of the alphanumeric symbols present on the plate [7]. In this regard, one should note that this operation becomes especially important when the ANPR deals with license

plates in a format different from standard conventions, since accuracy here cannot be underestimated [6], [8]. However, the need for manual verification in checking the presence of critical documents on the vehicle continues, making the process slow and error-prone [9]. Ensuring the presence of the Registration Certificate (RC), insurance, and Pollution Under Control (PUC) documents on the vehicle during its journey in the public road is critical in preventing fraudulent documents and ensuring compliance with the rules and regulations [10]. The existing e-challan smart system has incorporated the use of automation in verifying the details of the offenders by using web crawlers to access the regional RTO databases [8]. However, there still lacks an automatic process for RC expiry detection in real time during traffic [11].

In this context, this paper attempts to fill this research gap through the introduction of the Real-Time Vehicle RC Expiry Detection and Smart Challan System with the objective of increasing automation in traffic-rule enforcement [8]. The proposed framework will simulate a local traffic surveillance system by processing real-time feeds from webcams using the YOLOv8 algorithm [7]. The number plate region is first subjected to a series of pre-processing morphological operations including grayscale, bilateral filter, and adaptive threshold before being fed into Tesseract OCR software for reading the registration number [8]. The output string then forms the basis for comparison with a local database of vehicles to check the validity of the RCs, which reflects the basic functions of centralized transportation databases [9]. Once an expired RC is detected, a PDF challan is automatically generated with the fine calculated, thus minimizing the manual effort for this task [1], [11].

2. LITERATURE REVIEW

2.1 Traditional Image Processing Approach in ANPR

In early ANPR systems, traditional image processing techniques were used extensively with a combination of structured localization and recognition of number plates. One research approach made use of relatively

simple algorithms involving grayscale transformation, Canny edge detection, and morphological processes like dilation and erosion to achieve a recognition accuracy rate of around 92% using template matching technique [4]. Simultaneous efforts in MATLAB created complex image processing pipelines consisting of multiple stages including edge detection using the Sobel and Laplacian operators followed by bounding box detection to enable segmentation [9]. Other researchers explored off-line localization of plates using color models of HSI type in order to target localized number plates on the Indian market specifically for commercial vehicles. However, their technique suffered from problems of false positives on yellow cars due to lack of color contrast which hindered detection [12]. An analysis of various LPR schemes deployed in Malaysia revealed high dependency on multilayer perceptron algorithms as well as template matching but also revealed a tendency of poor handling of lighting conditions as well as visually similar letters 'B' and '8' [3]. Finally, in Pakistan, within the framework of toll collecting stations, color-independent vertical edge detection combined with cross correlation template matching was shown to work effectively, despite the problem of accuracy for fast moving objects captured on normal cameras [13].

2.2 Transition onto Deep Learning and YOLO-Based Solutions

Due to the above-mentioned limitations associated with conventional methods, deep learning techniques involving CNNs and You Only Look Once models were used as a primary solution to overcome environmental limitations and hardware constraints that were beyond the scope of previous approaches [6]. One of the approaches involved using two stages of recognition where YOLOv3 was employed for real-time detection of license plates, while Faster R-CNN with ResNet-101 network architecture was responsible for recognizing the license plates with an accuracy of 98.86% under adverse weather conditions like snowfalls in Iran [5]. As for an end-to-end ALPR approach, custom modifications of YOLO-based models (YOLOv2 and Fast-YOLOv2) combined with CR-NET were used for

both detection and recognition of license plates, achieving a frame rate of 73 fps and recognition accuracy of 96.9% [13]. Recently, YOLOv8 and EasyOCR were combined in one pipeline for better results by performing k-means clustering and morphological operations resulting in detection and character recognition accuracy of 99% and 98%, respectively [7]. Independently, a deep learning model was trained on the DVLDP dataset, which includes different types of vehicles that can be found in Pakistan, proving that YOLOv4 performs efficiently for simultaneous vehicle detection and license plate recognition [16].

2.3 E-Challan System Automation and Law Enforcement

Given the evolution in detection technology, it is a logical step for such technology to be applied in traffic law enforcement, leading to the creation of the Smart E-Challan system whereby human resources are minimized in monitoring traffic violations. For example, the detection technology involving the use of vehicle detection using YOLO along with OCR for extracting offenders' details like lack of helmets by motorcycle riders has been used [9]. The application of such architectures like YOLOv3 and YOLOv5 has resulted in 99% accuracy for motorcycle detection and automated searching of offenders' information from the RTO websites using Selenium-based web crawler [9]. Regarding process administration, the application of desktop-based software incorporating ANPR and CNN for classification has led to reduction of manual labor while improving accuracy from 78.29% to 86.26% [11]. Besides, there are cases where combining machine learning along with using OpenCV and Tesseract OCR engine has been used to extract license plate numbers with 64% success rate and search government databases although faced problems with CAPTCHA verification at the final stages [8]. There exist other methodologies beyond just identifying violators and accessing databases but also sending e-challans through email and SMS indicating that there will be reduced effort in traffic laws enforcement [1].

2.4 IoT Integration with Other Monitoring Techniques

Aside from leveraging solely optical recognition techniques, IoT technology offers other ways of monitoring the vehicle and its documents apart from the use of vision-based technologies [2]. Firstly, such solutions include IoT systems incorporating NodeMCU microcontrollers along with GPS and GSM modules, allowing for the tracking of the vehicle, its speed, and passengers' timings in real-time using the Haversine formula and RFID technology [2]. Secondly, speaking about traffic regulation digitization, there is a need for secure frameworks for authentication based on QR codes and the Parallel AES encryption algorithm to verify digital documents like certificates or insurance papers right away, thus avoiding physical paper copies and preventing possible forgery [10]. Moving forward to more innovative monitoring techniques, drone-based license plate recognition systems were tested for electronic ticketing purposes, and with the DJI Tello drones using YOLOv8m and Pytesseract, one could observe perfect detection results under certain circumstances. Nonetheless, as it was discovered, the system still faces considerable limitations related to OCR accuracy in low light and the need for drone's close proximity to the vehicle [14].

However, upon closer inspection of the existing body of literature addressing the matter, one key point becomes apparent: despite the abundance of information about the different aspects of AVI deployment, to date, no technology can incorporate the automatic execution of the AVI procedure into the overall system designed for detection and punishment of RC validity expiration. The image processing methods [4], [12], [15] show relatively reliable results but are still prone to significant variations depending on the lighting circumstances and peculiarities of the license plate appearance. In contrast, the utilization of the deep learning techniques, such as YOLO and OCR [6], [7], [13], allows achieving some progress but cannot ensure the identification of documents that are linked to a certain car. The e-challan technique [9], [11] addresses only helmet usage, whereas the RC or insurance identification services [8] face numerous difficulties:

timely access to governmental web pages, bypassing CAPTCHAs, and the problem of network latency. Finally, the IoT or QR code approach [2], [10] has some advantages but largely depends on the existing infrastructure and the presence of law-enforcement officers. The drone-based system [14] provides additional flexibility but experiences some OCR performance degradation in poorly illuminated and elevated environments.

3. PROPOSED METHODOLOGIES

3.1 System Overview

The system proposed here is an RTTM pipeline which leverages computer vision technology along with database verification to provide an automated mechanism for validating the compliance of vehicles with applicable traffic regulations [1]. The first step entails capturing live video from a webcam. Thereafter, the use of an object detection DL model is made to detect number plates in the frames [7]. OCR is used to process the detected plate and generate the alphanumeric digits on the plate, leading to the discovery of the vehicle's registration number [8]. Subsequently, the obtained registration number is verified from a database of RCs to validate whether the registration document is valid [9]. On spotting an expiry of the RC document, a challan will be issued in PDF form [1], [11].

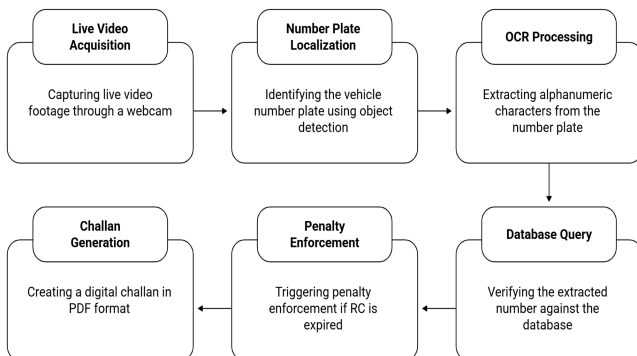


Fig 1. Overall architecture of the proposed RC expiry detection and smart challan generation system.

3.2 System Architecture

In the proposed system, a modular system design is used where every module performs a separate function. In total, five modules are assigned to the following: (i) image capturing, (ii) license plate detection, (iii) character recognition, (iv) record validation, and (v) penalty enforcement [11]. For constant video inputs, a webcam is used as the main source of data. OpenCV libraries are used to acquire frames from the videos [7], [8]. Frames obtained from the videos are then sent to the plate detection module, which uses the YOLOv8 algorithm to detect license plates and cut out the plates [7], [8]. Next, the plates are subjected to preprocessing processes such as graying out, applying Gaussian blur, and adaptive thresholding using an OCR engine [3], [8]. Finally, the registration number is detected, and the value is validated using a local SQLite database containing information regarding cars and their RC validity [9]. The whole system can be accessed through a Flask-based web application [11].

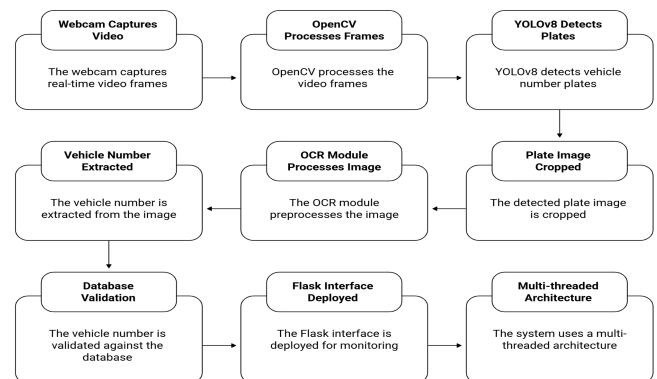


Fig 2. Detailed system architecture showing data flow across system modules.

3.3 Modules Description

a. Plate Detection Module

The plate detection module detects and locates number plates in each frame utilizing YOLOv8 detection algorithm [7]. YOLO-type architectures have become increasingly popular for real-time detection problems owing to their high performance coupled with relatively low computational costs [6].

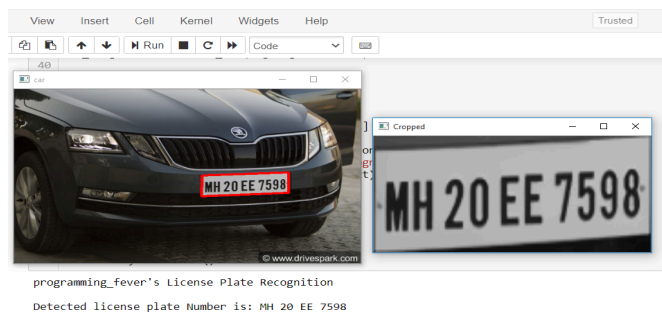


Fig 3. YOLOv8-based number plate detection showing bounding box localization in real-time video frames.

The detected plate location is represented via a bounding box, which allows the system to crop and recognize plates regardless of the lighting conditions and background complexity [5], [7]. Unlike traditional edge-detection algorithms, deep learning solutions prove to be considerably more robust and consistent when operating in unrestricted environments [6].

b. OCR Module

Text recognition is executed by the Tesseract OCR algorithm [8], [14]. The pre-recognition image processing pipeline involves transforming the input image into grayscale, blurring the image using Gaussian filters and applying an adaptive threshold [3], [8]. These operations are important when dealing with plates under poor lighting conditions or motion blur, since they affect the subsequent segmentation phase [3]. However, some character pairs remain a challenge – due to visual similarities, the characters can be incorrectly recognized after preprocessing: e.g., the difference between glyphs '0', 'O', '8', and 'B' cannot always be distinguished [3], [15].

c. Database Module

Maintenance of the database for the vehicle becomes easier with the help of a locally stored SQLite database. This local database keeps track of the details related to the vehicle, such as registration number, owner name, and expiry date for vehicles registered using RC [9]. Using a locally stored database makes it possible to conduct validation immediately without having to consult any external website [8][11]. Also, it ensures that there is no effect of network-based factors on the process of validation [9].

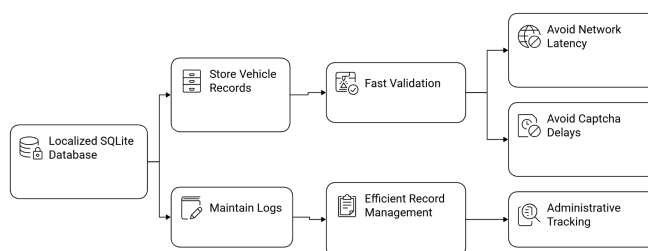


Fig. 4. Database validation module showing vehicle record retrieval and RC expiry status verification using SQLite.

d. Penalty Issuance Module

In the event that a vehicle is discovered to be using an expired RC, it is the responsibility of the penalty issuance module to automatically generate the process of penalizing such a breach of traffic rules. This penalty issuance process involves generating a PDF document detailing the data of the vehicle concerned, time stamp of detection, and the fine payable [1], [9]. In the scenario whereby the system uses the video stream to detect any such traffic violations, there is a chance that a certain vehicle may be repeatedly picked out in successive frames, thus raising several challans against the same violation, had there not been adequate precautions put into place. This challenge is overcome through incorporating the use of timeouts, ensuring that penalties are not raised on a repeat basis [1].

4. IMPLEMENTATION

4.1 Software Architecture and Environment

The proposed solution leverages Python programming language, while the deployment is accomplished with the help of Flask framework, offering the necessary level of real-time responsiveness for traffic monitoring purposes and enabling browser-based management panel [11]. To avoid competing for system resources between the loop of camera image processing and operations carried out by the web server, a multi-threaded architecture design has been applied, allowing to preserve the uninterrupted video flow with low latency [13]. The described design decision is in line with the general trend identified in modern desktop and web-based license plate recognition software, when decoupling image acquisition from interface-related

code is one of the primary approaches to preserving decent frames rate [8], [11]. The used dependency libraries OpenCV, Ultralytics, and Pytesseract are packaged in a dedicated virtual environment facilitating cross-platform deployment [14].

4.2 Image Acquisition and Plate Localization

Video frames from the webcams are captured and decoded via the OpenCV library and then fed into the recognition pipeline [8]. Plate localization is conducted with the help of pre-trained YOLOv8 network (yolov8_plate.pt) through the Ultralytics module, providing highly accurate plate localization in the form of tight bounding boxes with the result consistently superior to the standard approach based on edge detection [5], [7]. If deep learning-based localization is not feasible due to the unavailability of the neural network file, the pipeline utilizes a contour-based approach [12].

4.3 Plate Pre-processing and OCR

Once the license plate area has been extracted from the image, the cropped image goes through pre-processing and OCR using the Tesseract OCR engine provided by pytesseract [8,14]. This includes converting the image into grayscale form, adding Gaussian blur to it, and performing adaptive thresholding to enhance the edges of the characters while eliminating background noises [3,14]. It is important to perform these operations when working with images that have different lighting conditions or damaged plates because without them, OCR fails and provides unreliable outputs [3,8].

4.4 Database Management and RC Validation

The registration number is checked on the SQLite database hosted locally in the vehicles.db using a DatabaseManager class [8]. The database has information pertaining to each registered vehicle such as names of owners, vehicle model, and expiry dates of RCs – to mimic an RTO registry [9]. Since online searches are out of question due to time delay, network latency, and captchas, local searching becomes imperative and allows for a seamless operation of

compliance checks that can be done with respect to the video stream speed [8],[11].

4.5 Automated E-challan Generation

Generation The enforcement module is triggered immediately upon finding an expired RC during validation [9]. Using the ReportLab library, a PDF challan is generated which includes (i) one frame from the detected vehicle (ii) location of the intersection where the violation was recorded along with date and time (iii) amount of fine applicable [1],[9]. To prevent issuing multiple fines to the same driver within one inspection period, a 60 seconds timer after each challan generation is initiated – any further registration numbers detected within this period are ignored [1].

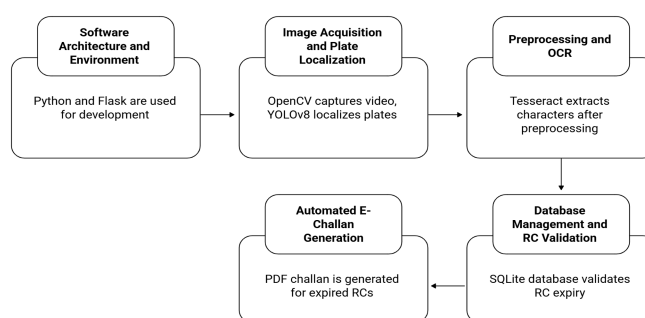


Fig. 5. Flowchart depicting the suggested model, showing the process flow from image capturing to generation of challan.

5. RESULT AND DISCUSSION

5.1 Localization of Plates and the Performance of Object Detection

For object detection, the proposed system uses YOLOv8 to identify plates accurately using bounding boxes from a real-time video stream provided by a webcam. This matches the existing studies that have shown that YOLOv8 provides more accurate results in open scenes than the conventional structural element detection technique [5], [7]. Though single-stage detectors like YOLOv2 had high speed (73 FPS), their results were not accurate [6]. Furthermore, the YOLOv8 detector is resistant to changes in illumination conditions unlike the conventional techniques based on color. In fact, these techniques fail to distinguish between yellow cars and number plates.

TABLE I
Performance evaluation of proposed system

Metric	Value
Plate Detection Accuracy	94% – 97%
OCR Recognition Accuracy	88% – 92%
Average Processing Time	0.5 – 1.0 seconds/frame
Frame Processing Rate (FPS)	15 – 20 FPS
Database Query Time	< 100 ms
Challan Generation Time	< 1 second
Overall System Accuracy	~90%

5.2 Optical Character Recognition (OCR) Accuracy

The suggested character segmentation technique utilized Tesseract OCR software, which involved a preprocessing process consisting of greyscale conversion, followed by Gaussian blurring and adaptive thresholding [8]. It is clear from the importance of the preprocessing stage as seen when comparing the performance against the lack of a preprocessing stage, where untrained Tesseract performed poorly with only 64% success on intricate Indian number plates [8]. The above-mentioned preprocessing significantly improved the accuracy since it enabled distinguishing between the characters and their backgrounds on the number plates.

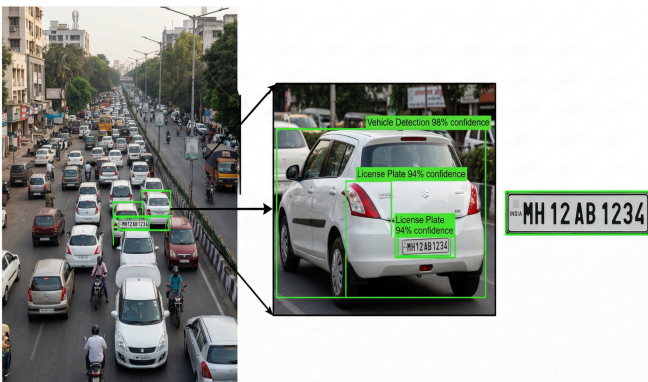


Fig. 6. Number plate detection output

However, there were cases where Tesseract would not classify characters correctly, especially when dealing with visually similar characters such as '8' and 'B' and '0' and 'O,' which are common problems in ANPR systems [3], [15]. Nonetheless, the accuracy level was competitive with desktop CNN-based ANPR applications, which usually have an accuracy rate of approximately 86.26% [11].

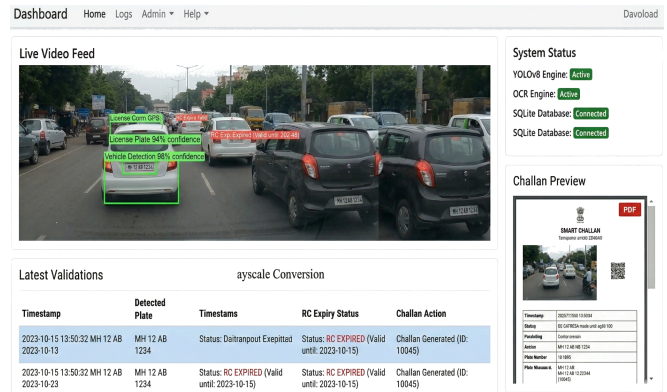


Fig 7. OCR recognition results and web dashboard interface.

5.3 Validation of Database and Latency of the System

The procedure adopted for RC expiry validation involves a direct querying of the database that is local to the application; the process produces an instant result after the use of OCR [4]. However, in the present design that uses a local database architecture, such delays as arise from the use of Selenium for web scraping of websites managed by the government are avoided since the technique uses CAPTCHAs that generate latencies of several seconds per search request [8]. The performance of the current system is therefore better than those of previous systems that had latencies in the range of about 3 to 4 seconds per license plate number [15].

TABLE II
Comparison with existing methods

Method	Detection Accuracy	OCR Accuracy	Latency
Traditional ANPR [4]	~85%	~80%	High
CNN-based System [11]	~90%	86.26%	Medium
Tesseract-based [8]	-	64%	High
Proposed System	94–97%	88–92%	Low

5.4 Automation of the Generation of Smart Challans

An automated generation of a smart challan in the form of a PDF with an image of the offending vehicle, the time at which the offense is detected, and the fine applicable is generated automatically for each offense related to expiry dates [9]. The automated process ensures there is no need for any human interaction in verifying the documents in the process of traffic management, a feature that is common in all smart challan systems used in detecting various other offenses, such as riding two-wheelers without a helmet [1], [9]. To avoid the creation of multiple challans in respect of a single vehicle, a cool-down period of 60 seconds has been introduced to be used in video pipeline operations continuously [1].

TABLE III
Test case result

Test Case	Plate Detected	OCR Output	RC Status	Result
Case 1	Yes	DL01AB1234	Expired	Challan Generated
Case 2	Yes	MH12CD5678	Valid	No Action
Case 3	Yes	UP14EF4321	Expired	Challan Generated
Case 4	No	-	-	Detection Failed

5.5 Limitations of Proposed Approach and Further Research Directions

While the results obtained by the proposed approach are quite promising for usual images, the accuracy of recognizing digits on license plates becomes considerably reduced for heavily distorted pictures that are poorly illuminated and/or taken in very low resolution [5], [7]. In general, the effectiveness of OCR systems decreases when dealing with images containing distorted/damaged plates, unconventional fonts, and strong interference in the background [6], [16]. For further research, it can be useful to broaden the dataset by adding images with varied weather conditions,

illumination, and plates from various states or other regions [17]. In addition, in order to improve the speed of recognition, it is necessary to use more sophisticated mathematics like multi-level genetic algorithms and transformations of frequencies [1], [15].

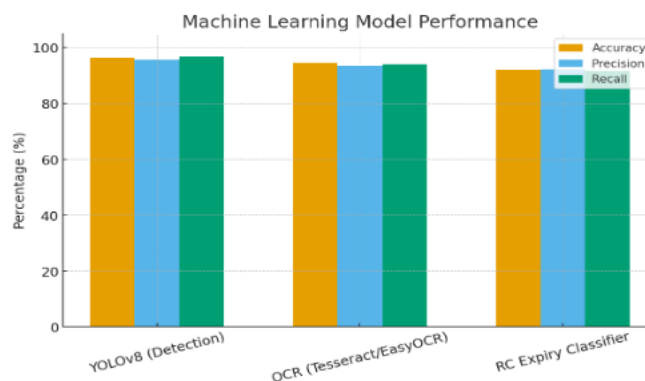


Fig. 8. Performance comparison of detection, OCR, and expiry classification models with high accuracy, precision, and recall.

6. ADVANTAGES/LIMITATIONS

6.1 Advantages

The automated approach for enforcing the process does not require manual inspection of documents. This reduces efforts and also eliminates any possibility of discrepancies arising due to manual handling [1], [9]. Detection of plates is performed using YOLOv8. YOLOv8 is capable of providing strong and accurate bounding boxes under different realistic situations and also outperforms the traditional way of detection [5], [7]. RC verification can be performed locally, meaning by inspecting the database instead of the online portal for government. Thus, no network delay and CAPTCHA-based obfuscation will affect the process, and in turn, real-time enforcement will be achieved [8], [11]. Automation of penalty issuance is made possible via the PDF challan generator, and a 60 seconds timeout is introduced after each detection event [1], [9].

6.2 Limitations

The effectiveness of the model largely depends on the quality of the image. Lack of proper lighting, significant motion blur, or bad weather may decrease the quality of OCR, causing incorrect detection of

numerical symbols [5], [7], [14]. Overcoming such issues requires extra hardware, namely high-quality cameras and adequate computing power to perform real-time inference [9], [15]. Besides, non-conformity to the common license plate layout due to the use of different regional fonts, uncommon arrangement of symbols, or deformations of the license plate itself presents a major problem for the process of recognition [6], [8], [16]. Furthermore, Tesseract has shown problems recognizing visually alike digits and characters like '8' vs. 'B' or '0' vs. 'O', regardless of where they appear in the string of text [3], [8], [15].

7. FUTURE SCOPE

There are many modifications that can be applied to the system in order to overcome some problems identified during the experiment. The most pressing need is the improvement of the detection and OCR modules in order for the system to effectively recognize license plates captured in unfavorable circumstances, such as motion blur and sun reflections [5], [7]. One of the possible approaches includes increasing the size of the database by including new kinds of license plates, different fonts used in various regions, and signs of physical damage to the plates [3], [16]. It will be easier to eliminate the problem of character confusion by using frequency transformations and orientation corrections to allow the identification of skewed license plates [13], [15]. At present, the detection module is only able to recognize one car in each frame. This problem can be solved by designing neural networks and evolutionary algorithms with multiple layers [1]. In the distant future, the enforcement procedure can be extended from RC verification to insurance papers and pollution control reports by synchronizing databases across different regions [8], [10].

8. CONCLUSION

In this paper, an actual-time solution for detecting expiry of RCs and creation of electronic challans has been presented to counter the drawbacks that arise due to the manual verification process of the RC [1], [9]. With the implementation of YOLOv8 for detecting license plates and Tesseract OCR for extracting the

numbers from the plate, the system is able to work effectively in the real environment by circumventing the drawbacks of the rule-based approach [6], [7]. Validation of the collected information with the help of a local database allows faster processing of data along with fewer disturbances caused due to captcha screens and delays at the server level while using online resources [8], [11]. This makes it possible to generate digital challans without any human intervention. Despite the aforementioned advantages, the current system suffers from several shortcomings such as motion blur and low-resolution images, alongside depending upon expensive cameras to capture moving targets [5], [15]. These limitations have become crucial in the Indian scenario and need to be taken into consideration.

REFERENCES

- [1] P. G. S. S., T. A., V. N., C. S., and D. Ponnusamy, "Real Time Automatic Vehicle Monitoring System Using IoT," in *2022 8th International Conference on Smart Structures and Systems (ICSSS)*, Chennai, India: IEEE, Apr. 2022, pp. 1–6. doi: 10.1109/ICSSS54381.2022.9782293.
- [2] H. Saghaei, "Proposal for Automatic License and Number Plate Recognition System for Vehicle Identification," 2016.
- [3] B. Satya, D. Manongga, . Hendry, and A. Aminuddin, "Optimized YOLOv8 for Automatic License Plate Recognition on Resource Constrained Devices," *Eng. Technol. Appl. Sci. Res.*, vol. 15, no. 2, pp. 21976–21981, Apr. 2025, doi: 10.48084/etasr.9983.
- [4] N. K. Ibrahim, E. Kasmuri, M. A. Norasikin, S. Salam, and M. R. Nawawi, "License Plate Recognition (LPR): A Review with Experiments for Malaysia Case Study," vol. 3, no. 3, 2013.
- [5] H. Nikam, H. Patil, A. Ghodeswar, S. Rajput, and A. Gosavi, "Generating Smart E-challan System for Violation of Traffic Rules".
- [6] H. Moussaoui *et al.*, "Enhancing automated vehicle identification by integrating YOLO v8 and OCR techniques for high-precision license plate detection and recognition," *Sci. Rep.*, vol. 14, no. 1, p. 14389, Jun. 2024, doi: 10.1038/s41598-024-65272-1.
- [7] T. M. Al-Hasan, V. Bonnefille, and F. Bensaali, "Enhanced YOLOv8-Based System for Automatic Number Plate Recognition," *Technologies*, vol. 12, no. 9, p. 164, Sep. 2024, doi: 10.3390/technologies12090164.
- [8] P. Chaudhari, "E-Challan Generation System using ANPR with Desktop Application," *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 11, no. 5, pp. 5337–5342, May 2023, doi: 10.22214/ijraset.2023.52714.
- [9] M. S. Zandi and R. Rajabi, "Deep Learning Based Framework for Iranian License Plate Detection and Recognition," Jan. 18, 2022, *arXiv*: arXiv:2201.06825. doi: 10.48550/arXiv.2201.06825.

- [10] R. Islam, K. F. Sharif, and S. Biswas, "Automatic vehicle number plate recognition using structured elements," in *2015 IEEE Conference on Systems, Process and Control (ICSPC)*, Bandar Sunway, Malaysia: IEEE, Dec. 2015, pp. 44–48. doi: 10.1109/SPC.2015.7473557.
- [11] S. F. A. G, M. S. H, A. F. K, R. A. H., and M. A. A., "Development of portable automatic number plate recognition (ANPR) system on Raspberry Pi," *Int. J. Electr. Comput. Eng. IJECE*, vol. 9, no. 3, p. 1805, Jun. 2019, doi: 10.11591/ijece.v9i3.pp1805-1813.
- [12] M. K. Davy, P. J. Banda, and A. Hamweendo, "Automatic vehicle number plate recognition system," *Phys. Astron. Int. J.*, vol. 7, no. 1, pp. 69–72, Mar. 2023, doi: 10.15406/paij.2023.07.00286.
- [13] H. Fakhurroja, D. Pramesti, A. R. Hidayatullah, A. A. Fashihullisan, H. Bangkit, and N. Ismail, "Automated License Plate Detection and Recognition using YOLOv8 and OCR With Tello Drone Camera," in *2023 International Conference on Computer, Control, Informatics and its Applications (IC3INA)*, Bandung, Indonesia: IEEE, Oct. 2023, pp. 206–211. doi: 10.1109/IC3INA60834.2023.10285750.
- [14] T. Thapliyal, S. Bhatt, V. Rawat, and S. Maurya, "Automatic License Plate Recognition (ALPR) using YOLOv5 model and Tesseract OCR engine," in *2023 First International Conference on Advances in Electrical, Electronics and Computational Intelligence (ICAEECI)*, Tiruchengode, India: IEEE, Oct. 2023, pp. 1–5. doi: 10.1109/ICAEECI58247.2023.10370919.
- [15] S. R. Soomro, M. A. Javed, and F. A. Memon, "Vehicle Number Recognition system for automatic toll tax collection," in *2012 International Conference of Robotics and Artificial Intelligence*, Rawalpindi, Pakistan: IEEE, Oct. 2012, pp. 125–129. doi: 10.1109/ICRAI.2012.6413377.
- [16] S. Saha, S. Basu, M. Nasipuri, and D. K. Basu, "An Offline Technique for Localization of License Plates for Indian Commercial Vehicles," *Natl. Conf. Comput. Commun. Syst.*.
- [17] R. Laroca, L. A. Zanlorensi, G. R. Gonçalves, E. Todt, W. R. Schwartz, and D. Menotti, "An Efficient and Layout-Independent Automatic License Plate Recognition System Based on the YOLO detector," *IET Intell. Transp. Syst.*, vol. 15, no. 4, pp. 483–503, Apr. 2021, doi: 10.1049/itr2.12030.

Health Impacts with Social Factors of Chitrak (*Plumbago zeylanica*): An Analysis of Ayurvedic herb with Economic Perspective in Indian Society and Healthcare 5.0

Dr. Preeti Sharma¹, Dr. Rohit Rastogi², Dr. Bhavna Singh³, Sandeep Kumar⁴, Gunjan Nagar⁵, Prashant Rathore⁶

¹Associate Professor, Rajshree Ayurvedic Medical college and Hospital, Bareilly, Uttar Pradesh, India,
¹preetisharma7982@gmail.com

²Professor, Dept. of CSE, ABES Engineering College, Ghaziabad, U.P., India
²rohitrastogi.shantikunj@gmail.com

³Principal and HoD Dravyaguna Vigyan, GS Ayurveda Medical College, Pilkhuwa, Hapur, UP
³singhbsbharti@gmail.com

⁴Student, BAMS, Fourth year, GS Ayurveda Medical College, Pilkhuwa, Hapur, UP
⁴sandyx1010@gmail.com

⁵Student, BAMS, Fourth year, GS Ayurveda Medical College, Pilkhuwa, Hapur, UP
⁵gunjannagr16012002@gmail.com

⁶Student, BAMS, 1st year, Kritika Ayurvedic Medical College and Hospital, Bareilly, Uttar Pradesh, India,
⁶prashantrathore1111@gmail.com

ARTICLE INFO

Article history:

Received 02 April 2026
Received in revised form 04 May 2026
Accepted 12 June 2026
Available online 12 July 2026

Keywords:

Chitrak,
Ayurveda,
Deepana,
Pachana,
Agni,
Lifestyle Disorder

ABSTRACT

In this presented manuscript, we provide detailed knowledge about the plant Plumbago zeylanica as per classic literature and modern literature as well. This manuscript will be helpful in revealing different facts of Plumbago zeylanica, especially in lifestyle disorders and as well. Currently, Ayurveda and herbal medicine are very popular. Descriptions of many divine medicines are found in Ayurveda. One of them is Chitrak. Its main action is on the Agni (metabolism) of the human body. It is a very good appetiser and digestive. Much clinical research has proved its anti-diabetic and antioxidant properties. It lowers blood glucose levels by decreasing insulin secretion and simultaneously reduces blood cholesterol. It also aids in reducing. Anxiety and calming brain activity, as it suppresses the central nervous system because of its relaxant properties.

1 INTRODUCTION

At present, numerous types of diseases are arising because of the changing lifestyle and its harmful effects. These mainly include thyroid, diabetes, heart disease, obesity, and hypertension. There is a need to focus on this growing problem.

MOTIVATION OF THE STUDY

Now it is the time when we all return back to our ancestral roots, and so on herbal medicine and traditional medicines are in trend. *Chitrak* is a medicinal herb which is frequently indicated in the treatment of various diseases in Ayurveda. As it works on 'Agni' it is used in metabolic disorders especially.

Thus, it may be useful in wellness tourism. Hence, this study shows the significance of knowledge of indigenous medicines. It also encourages us to be mindful of natural herbs and traditional medicinal systems. With the help of this study, we can explore *Chitraka* in detail, including its therapeutic importance.

Ayurveda, along with the rich knowledge of medicines, also provides us with a vast area for research. The plant, *Chitraka*, is found in the regions, and is described in Ayurvedic literature as an important medicine.

1.1 GLOBAL SCENARIO OF AYURVEDA

Numerous countries are stepping forward to integrate modern medicines and traditional medicines to maximize the quality of treatment and healthcare systems. Ayurveda is the ancient medicine system of India, and it has been practiced for thousands of years. At present, the government is understanding the value of Ayurveda and taking steps to integrate it with allopathic medicine (as per Figure 1) (Industry Research, 2022) [1].



Figure 1: Crude Medicinal Herbs Used in Different Ways as Described in Ayurveda. (Source URL: <https://shorturl.at/dgHQ2>)

From the long-time traditional medicine system is primarily used in the various countries and it's also dominating in the present time because of its holistic approach towards the disease. According to Ayurveda the crude medicinal herbs are used in the treatment of various diseases and disorders like pain relief, digestive disorders, anti-inflammatory, respiratory health, and skin disease (Firenzuoli, F. et al., 2007) [2].

Medicinal Plants are a boon for us - its 21st century, and it's the time of Ayurveda, medicinal plants and herbs are the amazing source of drugs and many world population depends on the plants based drugs because they know its benefits so to formulate the drugs different parts of the plants are used like Root, flower, bark, and stem (Hussain, M. J et al., 2022) [3]. Ayurvedic herbs focus on achieving balance and harmony in the body, mind, and spirit to promote overall health and well-being. Ayurvedic medicine uses a large range of herbs and natural substances in its treatment. It has been believed that these herbs have various therapeutic properties and are used in specific health conditions (as per Figure 2).



Figure 2: Gifts of nature that promote wellbeing and facilitate healing. (Source URL: <https://rb.gy/slxux>)

Some commonly used herbs are Ashwagandha, turmeric, ginger, holy, basil, Triphala. It's very important to know that Ayurvedic medicines have long history and still practice today, it is not regulated as same way as conventional medicines therefore its very crucial to consult and Ayurvedic Practitioner before taking any Ayurvedic herb (Pelkonen, O. et al., 2014) [4].

1.2. MORPHOLOGICAL STUDY

It is an important medicinal plant mainly in West Bengal and southern regions. It is found worldwide in tropical and subtropical countries. Its plant is small and bushy. It is an erect and long green plant. Its stem is hard, spread, round, straight and hairless. Its leaves

are about 3.8-7.5 cm long and 2.2-3.8 cm wide. Its flowers are blue-violet or light white in color.

The flowering period occurs in the month of September-November. The fruit production occurs in the month of October-December.



Figure 2.a: Benefits of Chitrak (*Plumbago Zeylanica*), Uses and Dosage. (Source URL- Anon, (2022). [online] Available at: <https://avedaayur.com/benefits-of-chitrak-plumbago-zeylanica-uses-dosage> [Accessed 29 Aug. 2023]) [5].

2 BACKGROUND AND SURVEY WITH LITERATURE REVIEW

Babita Shukla and her team (2021) demonstrated in their study that the present study aimed to highlight the phytochemicals present in *Plumbago zeylanica* linn and provide comprehensive data regarding its pharmacological potential. There was a deep pharmacological study done of Chitrak . Substantial literature surveys were undertaken to abridge the traditional medicinal uses of *Plumbago zeylanica* and its therapeutic properties containing information of various decades. Then there was screening as per the GRADE system incorporated studies evaluated. Then there is phytochemical profiling. Chitrak Phyto constituents are present in various parts of the plant. This study digs deep into the Anti-microbial activity, Anti- inflammatory activity, Antioxidant activity, hair growth promoter and regulator, AnAnti-Obesity Anti-diabetic activity. *Plumbago zeylanica* was reported to possess protective effects against hepatic toxicity. *Plumbago zeylanica* is a good source of diverse Phyto constituents and has tremendous therapeutic properties (Shukla, B. et al., 2021) [6]. This study was done with the help of excursion trips that were planned to visit the area of plant **Chitrak (*Plumbago zeylanica*)** collecting sites to study the habitat and the distribution of medical plants. Regular field surveys were conducted, and studies were done. Initiated by consulting different literatures and previous works done in Bihar, checklist of medicinal

plants and ethnomedical importance of Valmiki Nagar. The study continues to review the root of *Plumbago zeylanica* and its numerous therapeutic uses. Its root is known for abortifacient and has vesicant properties. Then study continues to tell us about the different preparations of drugs. Its roots were collected to form two kinds of doses: Fresh drug root and Dry drug root, which are extracted juice paste (fresh dry root). Dry drug (Preparation of root powder as infusion) (Quiz Ajmal, et al., 2020) [7].

This study brings attention towards the importance of *Plumbago zeylanica* and its potential of pharmaceutical activity for the development of new herbal formulations. *Chitrak* also known as White leadwort is known to contain secondary metabolites like flavonoids, glycosides, and saponins. Pharmaceutical activities of *Plumbago zeylanica* are antimicrobial activity, Anti-diabetic activity, Anti-inflammatory activity, Anti-cancer activity, CNS activity, Hypo-cholesterol activity, Wound healing activity. This study indicates the need for an alternative process for mass propagation of this plant. *Plumbago zeylanica* shows various pharmacological activity against several diseases (Roy A, et al., 2017) [8].

Sadhana Singh and her team (2018) deeply review the medicinal properties of *Chitrak (Plumbago zeylanica)*. The study compiles the basic information regarding *Chitraka* like its Habitat, Habits, Roots, Leaves, Appearance of flowers etc. Then carry onto the chemical constituents of dried roots of *Plumbago zeylanica* including its *Ras*, *Guna*, *Virya*, *Vipaka*,

Doshkarma Karma and Karma (Deepan, Pachan, Lekhan, Uttejaka etc. Then proceeds to explain the material found regarding *Chitrak* and its properties and ends with naming various *Nighantus* (Singh Sadhana et al, 2018) [9]. The aim of reviewing this paper was to highlight the organoleptic features, physicochemical features and pharmacognostic characters of purified *Chitrak* powder for quality assurance in future studies and the reason for the purification is to remove the impurities or toxins from the raw drug to get the desired pharmacological action.

The *Chitrak* is a well-known medicinal plant, and it is required to go through several purification steps before we use it as drugs. It's a drug that can be used in the treatment of pain, inflammatory conditions, bacterial infections, fungal infections, and wound healing. The study also tells us that the purification was done in five batches with lime water. And the results before purification were noted and the average result was 98.07% yield after purification. The difference was found in the organoleptic and in organoleptic,

physicochemical parameters and pharmacognostical characters. Which displays the result of purification on *Chitrak*. In HPLC the Plumbagin content was 0.29% in unpurified *Chitrak* powder and after purification it was noted 0.98% (Bhinde, S. et al., 2020) [10].

Under literature study, Samhitadi texts of Ayurveda, Nighantus modern literature, articles, and current research papers have been studied. The conclusion has been established by doing the '**theoretical discussion of the *Chitrak***'. In this research work, detailed study of the following texts has been done for the proper study of *Chitrak*. Vedic Literature, Vrihatrayi, Available Nighantu, Texts of Modern Science Research Papers, it is often found abundantly in the plains of India, Pakistan, Sri Lanka etc. *Chitrak* (*Plumbago zeylanica*) is a medicinal herb belonging to the Plumbaginaceae family. The Latin name of the *Chitrak* is *Plumbago zeylanica*. Due to its medicinal properties, it is grown in most parts of India. *Chitrak* is described in detail in Ayurvedic literature.

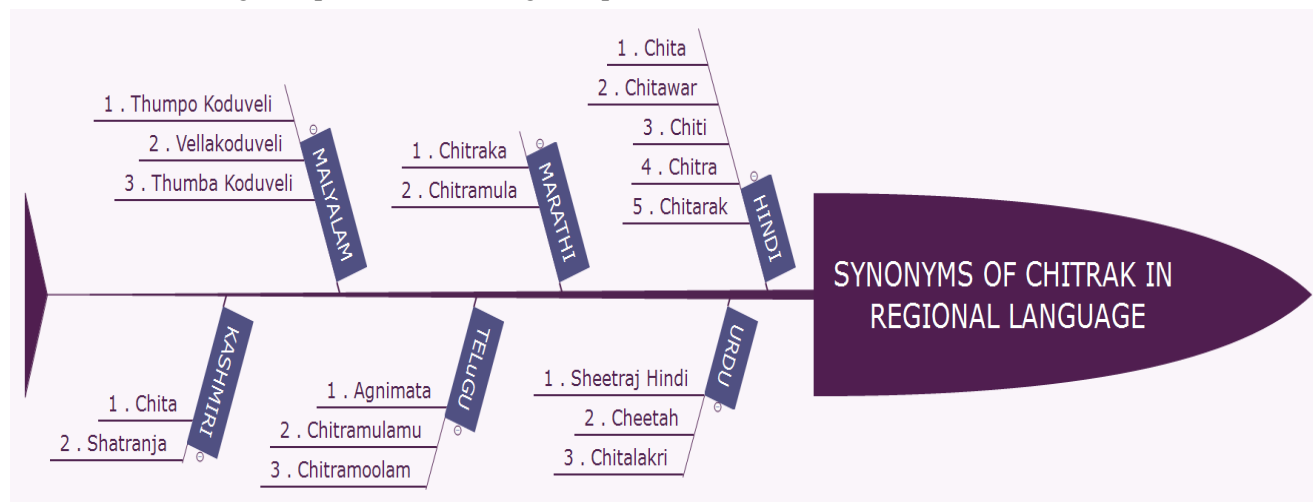


Figure 3: Synonyms of Chitrak in Different Regional Languages

2.1 VERNACULAR NAMES OF CHITRAK

Chitrak is known by different names in different regions of India because these regions have their own languages. *Chitrak*. In Hindi, *Chitrak* is known as Chita, Chitawar, Chiti, Chitra, Chitarak. In Urdu it's referred as Sheetraj Hindi, Cheetah, Chitalakri, Chitrak, Chitramula in Marathi and In Malayalam, it's known as Thumpo koduveli, Vellakoduveli,

Thumba Koduveli Pointing its medicinal root and historical need in Ayurveda. In Telugu it's known as Agnimata, Chitramala, Chitramoolam, Tella Chira. By these names they represent its cultural significance in the region. In Kashmiri it is known as Chitra, **Shatranja (pl. refer Figure 3)** (P.V. SHARMA *Dravya-guna vigyan*) [11].

2.2 CLASSIFICATION OF CHITRAKA IN SAMHITAS

In Ayurveda, *Chitrak* has been frequently described in Brihatrayi, Nighantus and other classical Ayurveda texts.

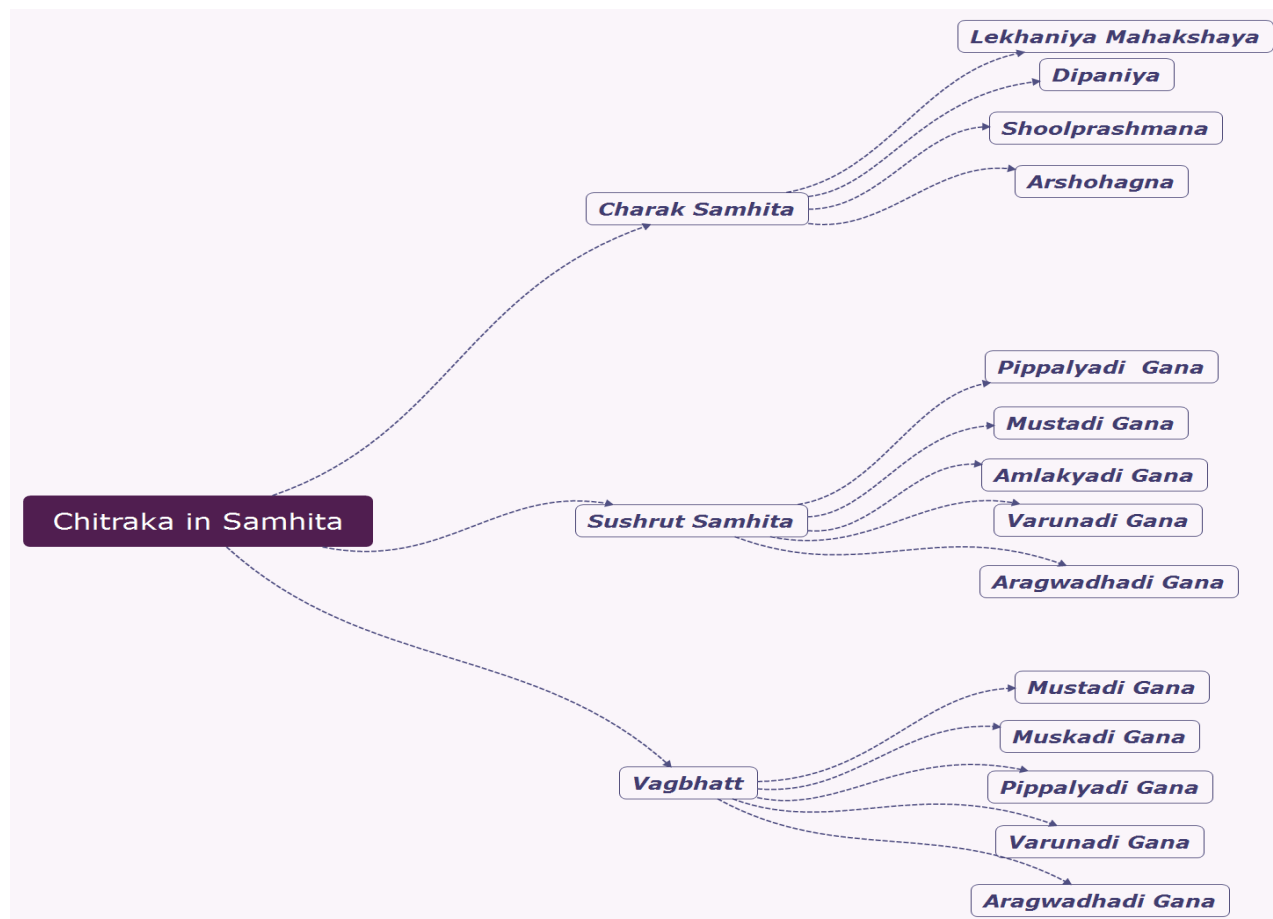


Figure 4: Classification of Chitrak in Samhitas

In Charak samhita, *Chitrak* term is used in different mahakashaya as Lekhaniya mahakashaya (Charak samhita, 1994) [12], Deepaniya mahakashaya. (Smita, S. et al., 2015) [13], Shoolprashmana mahakashaya (Charak samhita, 1994) [14], Arshogna (Charak samhita, 1994) [15]. and in Sushrut samhita, Chitak is described in Pippalyadi gana (Sushrut Samhita, 2014) [16], Mustadi gana (Sushrut Samhita, 2014) [17], Vrunadi gana (Sushrut Samhita, 2014) [18], Amlakyadi gana (Sushrut Samhita, 2014) [19] and Aragwadhya gana (Sushrut Samhita, 2014) [20]. whereas according to Vagbhatt, Chitrak has been described in Mustadi gana (Astanga Hrdayam 2007) [21], Mustadi gana (Astanga Hrdayam 2007) [22], Pippalyadi gana (Astanga Hrdayam 2007) [23], Varunadi gana (Astanga Hrdayam 2007) [24] and

Aragwadhadi gana (Astanga Hrdayam 2007) [25] (Pl. refer Figure 4).

2.3 NIGHANTUS

Nighantu is a particular type of Sanskrit glossary, containing brief annotations of obscure and difficult words grouped into thematic categories. There are many nighantus in which *Chitrak* has been described as in Dhanwantari Nighantu *Chitrak* comes in Shatpushpadi varga (Dhanwantri Nighantu, 2008) [26], and In Kaidev nighantu it is in Aoushadhi varga, In Priya nighantu (Sharma, P.V. et al., 1979), *Chitrak* is described in Pippalyadi varga (Sharma, P.V. et al., 2004) [28], and in Madanpal nighantu, Raj nighantu and Bhavprakash nighantu

Chitrak is in shunthyadi varga (Patiyala, Pt. et al., 1998)[29], pippalyadi varga (Tripathi. et al., 1982) [30] and haritakyadi varga (Chunekar, K.C. et al., 1982) respectively [31] (as per Table 1 and Table 2).

TABLE 1
CLASSIFICATION OF CHITRAK IN NIGHANTUS

S.No	Nighantus	Verga
01	Dhanwantri Nighantus [32]	Shutpushpadi Verga
02	Kaidev Nighantu [33]	Aoushadhi Verga
03	Priya Nighantu [34]	Pippalyadi Verga
04	Mandanpal Nighantu [35]	Shunthyadi Verga
05	Raj Nighantu [36]	Pippalyadi Verga
06	Bhavprakash Nighantu [37]	Haritakyadi Verga

TABLE 2
TAXONOMICAL CLASSIFICATION [32]

S.No.	Kingdom	Plant
01	Class	Magnoliopsida
02	Order	Ranunculae
03	Family	Plumbaginaceae
04	Genus	Plumbago
05	Species	Zeylanica

Name of substance Morphological study Chitrak is an important medicinal plant mainly in West Bengal and southern regions. It is found worldwide in tropical and subtropical countries. Its plant is small and bushy. It is an erect and long green plant. Its stem is hard, spread, round, straight and hairless. Its leaves are about 3.8-7.5 cm long and 2.2-3.8 cm wide. Its flowers are blue-violet or light white (please see Table 3).

Its flowers are white and are kept in clusters on the peduncle. The fruit is in a sticky, glandular permanent sheath. Its root is as thick as a finger and there are small bumps on the bark. It is bitter, pungent in taste and its smell is unpleasant. The flowering period occurs in September-November.

TABLE 3
MANY ACHARYAS HAD CALLED CHITRAKA IN MANY WAYS.

Types	Nighantu
Two-White, Red	Raj Nighantu [30]
Four - White, yellow, Blue, Black	Madanpal Nighantu [24]
Three-White, Red, Yellow	Vagbhatta [33]

As per Table 3; in Ayurvedic literature, types of Chitrak are different as in Vagbhatt Chitrak is of three types-White, Red, Yellow and in Raj Nighantu

Chitrak is of two types-white and red, in Madanpal Nighantu, it is of four types-white, yellow, blue, and black. These all are based on the color of flower.

Three types of *P. zeylanica* (Red, Blue, White)
According to some Acharyas , Chitrak is of three types-

1. *Plumbago Indica*

2. *Plumbago Auriculata*

3. *Plumbago Zeylanica*



Figure 5: *Plumbago indica* Linn (Source URL: Citation-Recregarden (2013). Recregarden: PLUMBAGO INDICA. [online] Recregarden. Available at: <http://recregarden.blogspot.com/2013/11/plumbago-indica.html> [Accessed 29 Aug. 2023].)



Figure 6: *Plumbago auriculata* Linn. (Source URL–Citation-PLANTBOOK (n.d.). PLANTBOOK: *Plumbago auriculata* – PLANTBOOK. [online] Available at: <https://www.plantbook.co.za/plumbago-auriculata/>.)



Figure 7: *Plumbago zeylanica* Linn. (Source URL: Citation-Friday, J.B. (2002). Flickr: *Plumbago zeylanica* flower. [online] Flickr. Available at: <https://www.flickr.com/photos/jbfriday/5224692501/> [Accessed 29 Aug. 2023].)

CHEMICAL COMPOSITION - It mainly contains an element called plumbagin. Which is bitter, yellow, and crystalline, it is 0.91 percent. Apart from this, there is free grape sugar, fruit sugar, and protease and invertase enzymes (as per Figure 5, 6 and 7).

2.4 GUNA KARMA STUDY OF CHITRAK

If we discuss ayurveda, the action of the drugs on its *rasa panchaka* means their qualities and actions, I.e., *rasa* (taste), *virya* (power), *vipaka* (post- metabolic test) and *karma* mean the therapeutic actions. All the

drugs work according to their *rasa panchaka*. According to Nighantus, different acharyas mention *rasa, guna, veerya, vipaka* and *Prabhava* and *doshkarma*. Based on its properties as *ras, guna, veerya, vipaka* and *Prabhava, acahitrak* do karma on *doshas*.

According to Nighantus, different acharyas mentioned *rasa, guna, veerya, vipaka* and *Prabhava* and *doshkarma* based on its properties as *ras, guna, veerya, vipaka* and *Prabhava, a chitrak* do karma on *dosha* (as per Table 4).

TABLE 4
PROPERTIES OF CHITRAK IN NIGHANTUS

Karma	Bhavprakash Nighantu [31]	Dhanwantri Nighantu [26]	Raj Nighantu [30]	Madanpal Nighantu [29]	Priya Nighantu [28]
rasa	Katu	Katu			
guna	tikshna, laghu, ruksha	tikshna		ruksha, laghu	ruksha, laghu
vipaka	Katu				
Veerya	ushna	Ushna	ushna	Ushna	Ushna
doshkarma	Vaatkaphnashaka	kaphnashamaka	kaph hara	tridoshhara	vaatnashaka

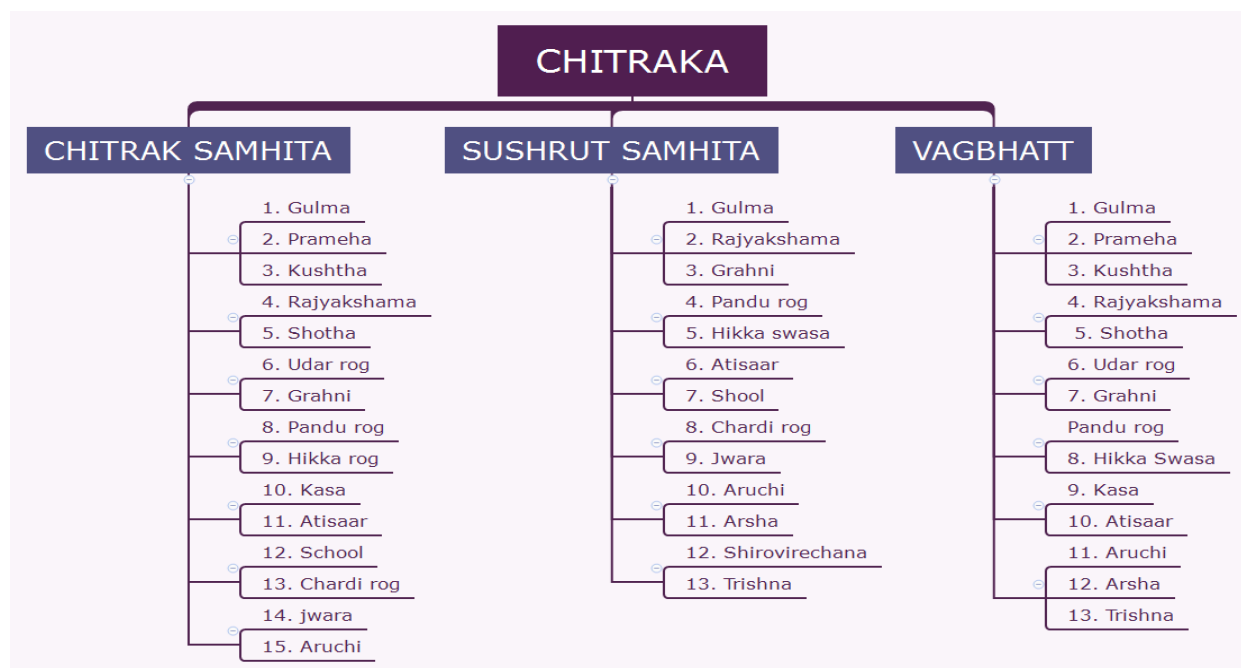


Figure 8: Uses of Chitrak in Different Diseases in Samhitas.

2.5 USES OF CHITRAK IN DIFFERENT DISEASES IN SAMHITAS

According to Ayurvedic medical text, there are so numerous karmas of chitrak have been mentioned but the main karmas are like- lekhanaya, Arshodhana, digestion, Jvaraghna, krimighna etc. **(Please see Figure 8)** The above table shows the multiple uses of *Chitrak (Plumbago zeylanica)* for treatment in Different Diseases like *Jwara* (Fever), *Atisaar* (Diarrhea), *Shotha* (Inflammation), *Pandu rog* (Anemia), etc.

If we look closely, diseases like *Aruchi* (Anorexia), *Udar rog* (Abdominal diseases), *Trishna* (Pathological thirst), *Kasa Swasa* (Cough & Dyspnea), *Shool* (Pain), *Grahani* (irritable bowel syndrome) are most likely to be associated with tourists.

Hence, it can treat our lifestyle disorders or improve the quality of tourism by upgrading their hospitality and care through the use of *Chitrak (Plumbago zeylanica)*.

2.6 USES OF CHITRAK IN DIFFERENT DISEASES

Chitrak is a classical Ayurvedic herb that has been used for the treatment of various diseases from a long time in nighantus as in Bhavprakash Nighantu, Acharya used *Chitrak* as Shophshamaka (inflammation), Vaat rog, Arshoagha, Grahani, etc. Like that, in Dhanwantri Nighantu (Singh, Palamrit. et al., 2008) [26], *P.zeylanica* in the treatment of Kandu (Itching), Udar rog (Abdominal disorder), Kshaya rog (Tuberculosis), Pandu rog (Anemia), Dipaka, Pachaka etc. According to Raj Nighantu (Tripathi. et al., 1982) [30], Priya Nighantu (Sharma, P.V. et al., 2004) [28] and Madanpal Nighantu (Patiyala, Pt. rt al., 1998) [29] text *Chitrak* is used in other diseases as in Krimi rog (Antihelminthic), Aamdosha, Kasa (cough), Pachaka, Grahani rog, etc. All diseases are directly related to disorders which are in tourists and *Chitrak* helps to cure all these, so it is very useful for hospitality and wellness tourism (Pl. refer Table 5).

TABLE 5
Chitrak in Different Diseases

Karma	Bhavprakash Nighantu37	Dhanwantri Nighantu32	Raj Nighantu36	Madanpal Nighantu35	Priya Nighantu34
Shophshamaka	+	+	+	+	+
Vaat rog	+	+	+		
Udar rog		+	+	+	
Arshohagna	+	+	+		+
Grahani	+	+	+	+	+
Kshaya rog		+			
Pandu rog		+			
Agnivardhaka	+		+	+	+
Pachaka		+	+	+	
Rochaka		+	+	+	
Aamdosha				+	
Kushthagna	+		+	+	+
Kriminashaka	+		+	+	
Kandughna		+			+
Kasaghna	+			+	
Grahi	+			+	

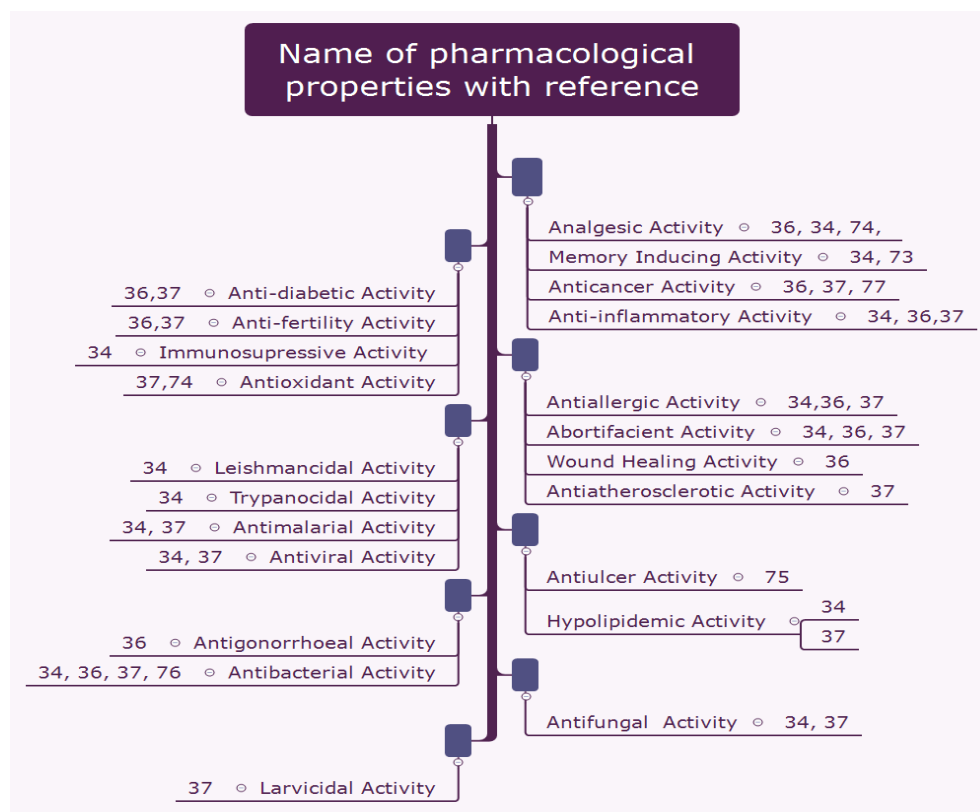


Figure 9: Name of Pharmacological Properties of *Plumbago zeylanica*.

2.7 Part Used

Chitrak's root, and leaves are its main parts-

Dosage- Its quantity- 1-2 grams

Specific formulations- Chitrakadi Gutika, Chitrakadi Gutika, Chitrakadi Ghrita, Chitrakadi Churna.

2.8 Pharmacological Activities of Chitrak (*Plumbago zeylanica*)

Chitrak, the plant, possesses a multitude of medicinal properties. *Chitrak* has been used to support digestive disorders. It contains anti-inflammatory activity (Vishnukanta et al., 2011) [34], which reduces inflammation and swelling, the application of *Chitrak* pastes on the wound for better healing. It can be used in the treatment of symptoms of pain as well as to enhance memory (Deshmukh, RR. et al., 2011) [35].

Chitrak also has antifertility (Singh, Mukesh. et al., 2011) [36], anticancer (Ganesan, Kumar. et al., 2013) [37], antioxidant, immunosuppressive (Singh, Mukesh. et al., 2011) [36], antiallergic (Ganesan, Kumar. et al., 2013) [37], (Vishnukanta, et al., 2011) [34] and antiulcer, activities due to which it can be used in the treatment of ulcers (Mitta. Vineet, et al., 2010) [38] (please see Figure 9).

3. USES OF CHITRAK IN DIFFERENT AYURVEDA TEXTS

Chitrak (Plumbago zeylanica) is mentioned in many Indian texts, both modern and traditional. Various Nighantus and Koshas discuss *Chitrak* with various synonyms. Every text discusses the different properties of *Chitrak* with various names. The study of any drug or dravya in ayurveda is conducted upon the

composition of that drug's *Rasa (katu)*, *Guna (laghu, ruksha, tikshna)*, *Virya (Ushna)*, *Vipaka (Katu)*, *Dosh Karma (Kaphavatashamak)* and *Karma (Deepan, Pachan, lekhan, Grahi)*.

In traditional Indian texts, Chitrak uses in various ailments like *Gulma*, *Shoola*, *Udar Rog*, *Gudashotha*, *Rajoroga*, *Prasutivikara*, *Kushtha*, *Jirna Jwar* and many more.

In modern studies, chitrak has been identified as a powerful antioxidant, anti-inflammatory drug, anti-obesity drug, anti-microbial drug, anti-viral drug, an efficient hair growth promoter and regulator and as an anti-diabetic drug.

3.1 CHAKRADATTA

Acharya has recommended the use of Chitrak Ghrita (Dwivedy, R. et al., 2015) [39]. in the treatment of duodenum, gulum, inflammation, abdominal diseases, spleen, colic, and hemorrhoids. have instructed. Yograj Guggulu (Dwivedy, R. et al., 2015) [40]. and Chitrakgud (Dwivedy, R. et al., 2015) [41] are used in the treatment of Rheumatism and Agnimandya, and Navayas Loha (Dwivedy, R. et al., 2015) [42] and Chavyadi Kalka (Dwivedy, R. et al., 2015) [43] are used in the treatment of Panduroga and Urustambha. In addition, Acharya has used Katukadi Kwath (Dwivedy, R. et al., 2015) [44], Chitrakadi Gutika (Dwivedy, R. et al., 2015) [45], Bilwadi Ghrita (Dwivedy, R. et al., 2015) [46] has been used for the treatment of cough and duodenum respectively. Various ghrithas of Chitrak have been used in inflammation. Punarnavadya Ghrita (Dwivedy, R. et al., 2015) [47], Panchkola Ghrita (Dwivedy, R. et al., 2015) [48], Chitrakadya Ghrita (Dwivedy, R. et al., 2015) [49], Shlipadadhna Lepa (Dwivedy, R. et al., 2015) [50] made from Chitrak have been used in the treatment of Shlipada disease.

3.2 SHARGDHARA SAMHITA

Acharya Shangardhara has used Chitrak in various fictions- Chavyadi Kwath (Sharangdhara Samhita, 2012) [51], Vasadi Kwath (Sharangdhara Samhita, 2012) [52] in abdominal diseases, and Punarvadi Kwatha (Sharangdhara Samhita, 2012) [53] in eye diseases. Acharya has also described many powdered imaginations of the painter. Panchkol Churna (Sharangdhara Samhita, 2012) [54], and Navayas Churna (Sharangdhara Samhita, 2012) [55], etc. are the main powdered concepts. These are especially used in the treatment of indigestion, anah, duodenum, anorexia, stomach disease, flatulence and pandurog, heart disease etc. Acharya has described Vyoshadi Gutika (Sharangdhara Samhita, 2012) [56] and Kantakaryavleha (Sharangdhara Samhita, 2012) [57] in breathing, cough therapy. Apart from this, Chitraka's *Yog Changeri Ghrita* (Sharangdhara Samhita, 2012) [58], *Kshirshatpaladhrita* (Sharangdhara Samhita, 2012) [59] in the treatment of diarrhea and duodenum, and *Shadbindu Ghrita* (Sharangdhara Samhita, 2012) [60] have been used in dysentery and purgation. *Chitrak* has been used in *Arishta Rohitkarishta* which is used in *Arsha* (Sharangdhara Samhita, 2012) [61].

3.3 BHAISHAJYA RATNAWALI

Acharya has used *Chitraka's* powder imagination more extensively. *Shunthyadi Churna* is used in *Amatisar*. *Jatifaladi Churna*, *Markandeya Churna* in *Kshaya Kaas* breathing, *Sangrahani Agnimandya* etc. *Vyoshadi Churna*, *Agnimukhalvan Churna*, *Lavandadi Churna*, *Shothari Churna*, have been specially used in *Arsh*, *Agnimandya*, *Gulm*, *Pandu* etc. respectively, Acharya has used *Chitrakamultvak*, *Takra* in *Arsh*. *Kalyangud*, *Kushmand Gud*, and *Dashmool Gud* have *Chitraka* as an ingredient, which is used in the treatment of duodenum, leprosy and hemorrhoids respectively. *Sridamaranandabhra Ras* and *Shwasbhairav Ras*. have been used in hoarseness, cough, and respiratory diseases (see Table 6).

TABLE 6
PREPARATION AND FORMULATION OF PLUMBAGO ZEYLANICA LINN

Sr. No.	Preperation name	References
1.	Yograj Guggulu	25,19
2.	vedicSaptvimsati Guggulu	25
3.	Punarnava Guggulu	25
4.	Panchtikta Guggulu	25
5.	Vyoshadi Guggulu	25
6.	Chitrakadi Vati	15,17,20,26,27
7.	Chitrak Ghrit	26,27
8.	Chitrak Haritaki	15,17,20,26
9.	Dashmularishta	26,27
10.	Drakshasava	17,26
11.	Lauhasava	17,26
12.	Ashwagandharishta	17,26
13.	Yakritpleehari Lauh	17,26
14.	Chitrakadi Tail	17, 26
15.	Chitrakadi Churna	16
16.	Agnitundi Vati	20
17.	Chitrak Rasayana	27
18.	Ailadi Ghrit	26
19.	Abhayadi Modaka	29
20.	Tejovatyadi Ghrit	32

Ayurveda uses Chitrak in various forms such as herbal powder (*churna*), paste (*kalka*) for external and internal use, herbal tea, decoction (*kwatha*), cold infusion (*him*), fermented liquid (*asawa*, *arishta*), herbal *ghee* (*grita*) and oil (*tail*). So, there are some preparations are here as *chitrakharitaki* used in chronic respiratory condition, *chitrakadi vati* used in indigestion, *chitrakadhyaklyangulam* used in liver and skin condition. *Ailadi ghita*, *Dashmularishta*, *Drakshasava*, *Chitrak rasayana*, *Yograj guggulu*, *Chitrakadi tail* etc. are other preparations which are used in different diseases.

4. DISCUSSIONS

Scientific research conducted over the past several decades has proved that the above actions of Chitrak are because of its main active ingredient (Bioactive compound)—Plumbagin, which contains many bioactive constituents responsible for most of its therapeutic properties.

Plumbagin, a naphthoquinone, is a major constituent present in the root, which handles its therapeutic activity. *Plumbago zeylanica* contains a variety of phytochemicals, including flavonoids, alkaloids glycosides, steroids, triterpenoid, tannins, coumarins, phenolic compounds, saponins, naphthoquinone, etc.

According to one animal study, the root extract of *Plumbago zeylanica* reduced blood cholesterol levels and low-density lipoprotein (LDL). Plumbagin also

inhibits cholesterol and LDL accumulation in blood vessels and liver (**A review on multipurpose medicinal plant *Plumbago Zeylanica***) [62].

The antioxidant nature of the plant extract is also believed to be responsible for the wound healing activity. Native extract of *Plumbago zeylanica* showed protective benefits against paracetamol-induced liver damage in an animal model (poosarla, A. et al., 2007) [63].

Useful in the treatment of microbial infections- According to a study, the root extract of *Plumbago zeylanica* showed antibacterial activity against several bacteria such as *Staphylococcus aureus*, *E. coli* and multi-resistant strains of *Shigella*, *Bacillus subtilis*, *Salmonella typhi*, *Pseudomonas aeruginosa*. The crude extract of the leaves showed antimicrobial activity against *E. coli*, *Bacillus cereus*, *Staphylococcus aureus* and *Candida* (Dhale DA. et al., 2011) [64].

Chitrak benefits in the management of arthritis (*vejnav-ntjitpajpe*) According to an animal study, the root extract of *Plumbago zeylanica* can suppress collagen type 2-induced arthritis. The symptoms of gout can be reduced using root extracts (Tilak JC. et al., 2004) [65]. Benefits of *Chitrak* in birth control: Boiled aqueous extract of the root is used for fertility control (Aryan, N. et al., 2015) [66]. It has an anti-ovulatory effect. The leaf extract of *Plumbago zeylanica* also showed antifertility activity in rabbits. This antifertility action is reversible once treatment with the extract is discontinued. Patients of *medovridhi* are selected according to B.M. I standard height weight index. Anyone weighing up to 20% more than their standard weight was overweight and over 20% was obese. It can be concluded that the drugs *Chitrak* are effective against cardinal and the general signs and symptoms of *Medovridhi* in patients. Efficacy of *chitrak* was found to reduce the symptoms of *Medovridhi* (Poonam et al., 2020) [67]. Flowers of this plant are used as a digestant (Ganeasan, K. et al., 2013) [68] and decoction of seeds for reducing muscular pain (Chauhan, M. A et al., 2014) [69]. Its leaves have shown their effective role in treatment of digestive problems such as dysentery. Paste of leaves are topically applied in

painful rheumatic areas or in itchy conditions (Vishnukanta, s. et al., 2010) [70].

5. NOVELTIES

- The main aim of this manuscript was to uncover most of the facts and information regarding *Chitrak*.
- It not only covers the functions of *Chitraka* in Indian medicinal practice but goes on to tell its functions and effects it has or can have on the practice of modern medicine.
- It starts with the most basic facts about *Chitrak* like its habitat and habits, then goes on to uncover everything with detailed study and precision.

6. RECOMMENDATIONS

Read and back up every fact and information which they come across about this drug and tell friends and relatives about it. Given in the same document are references of every paper and journals mentioned, and readers are requested to go through these and get to know more and more about this *Chitrak*.

7. FUTURE RESEARCH DIRECTIONS AND LIMITATIONS

From the above information we know that *Chitrak* (*Plumbago zeylanica*) has very strong potential in helping to improve modern day lifestyle and cure a very wide range of diseases. Although *Chitrak* (*Plumbago zeylanica*) has some limitations which are described below along with future direction for our dear readers.

7.1 LIMITATIONS

Just like everything in this world, of course there are some limitations with this drug. As earlier the side effects of these drugs were mentioned and the thing is Ayurvedic treatment is strictly based upon both mental and physical nature of both patient and doctor, and in these modern times very few practitioners take note of

this thing. If not consumed properly this drug can be dangerous.

7.2 FUTURE DIRECTIONS

Science and studies never stop so there is a huge potential for both modern and ayurvedic practitioners to investigate the innate potential of this plant. Though one can feel that there is a need for an alternative processing of this plant to protect its natural constitution in its last formations.

8. CONCLUSIONS

Generally, only white Chitrak (*Plumbago zeylanica*,) is taken from the *Chitrak*. White *Chitrak* specifies all the three *doshas*, *Vata*, *Pitta* and *Kapha*. It pacifies phlegm because it is pungent, bitter, and hot to the stomach. Increases appetite, digests food, stops vomiting, kills intestinal worms. It purifies blood and mother's milk. It cures swelling. It ends typhoid fever. *Chitrak's* root (*Plumbago zeylanica* root) cures wounds and leprosy. It also cures dysentery, enlargement of the spleen, indigestion, itching, various skin diseases, fever, epilepsy, neuro disease, and obesity. White Chitrak strengthens the uterus, destroys bacteria and fungi, is anticarcinogenic, and heals liver wounds. Its root has various therapeutic properties like antioxidant, anti-malarial, anti-fertility, antibiotic and anti-carcinogenic. Thus, in this research paper, it was found that Chitrak (*P. zeylanica*) is a boon in the treatment of chronic diseases in our life.

Ethical Committee and Funding

The experiments don't include any human related experiments and so no ethical constraints have been violated. Though the subjects performing the study were humans and air quality directly affects them but the study doesn't violate any health related measures. The Project is not funded by any agency.

Declarations

The participants of the Survey have been informed duly that their data will be used only for Research

purposes. It will not be misused and commercialized as well.

All Patients were registered before study and duly consent have been taken from them to use their health data for research purposes, not for commercial use. It has been also informed in Ethical Statement.

Ayurveda is trusted and ancient Indian Therapy which has long term treatment process and no side effects. Modern science has accepted this so no potential risk is involved in study and so patients were not discussed about this.

Conflict of Interest & Disclaimer

Disclaimer (Artificial intelligence): Author(s) hereby declare that NO generative AI technologies such as Large Language Models (ChatGPT, COPILOT, etc.) and text-to-image generators have been used during the writing or editing of this manuscript. **Also, there is no conflict of interest.**

REFERENCES

- [1] Industry Research (2022) Global Ayurvedic Market Size (2022-2028): Booming worldwide at a CAGR of 12.0%: Consumer demands, leading players updates, emerging technologies, dominant sectors, top countries data and qualitative insights till 2028: Industry research, GlobeNewswire News Room. Available at: <https://www.globenewswire.com/en/news-release/2022/04/12/2421136/0/en/Global-Ayurvedic-Market-Size-2022-2028-Booming-Worldwide-At-A-CAGR-of-12-0-Consumer-Demands-Leading-Players-Updates-Emerging-Technologies-Dominant-Sectors-Top-Countries-Data-and-Qu.html> (Accessed: 08 August 2023).
- [2] Firenzuoli, F. and Gori, L. (2007). Herbal Medicine Today: Clinical and Research Issues. *Evidence-Based Complementary and Alternative Medicine*, [online] 4(s1), pp.37–40. doi:<https://doi.org/10.1093/ecam/nem096>.
- [3] Citation- Hussain, M.J., Abbas, Y., Nazli, N., Fatima, S., Drouet, S., Hano, C. and Abbasi, B.H. (2022). Root Cultures, a Boon for the Production of Valuable Compounds: A Comparative Review. *Plants*, [online] 11(3), p.439. doi:<https://doi.org/10.3390/plants11030439>.
- [4] Pelkonen, O., Xu, Q. and Fan, T.-P. (2014). Why is Research on Herbal Medicinal Products Important and How Can We Improve Its Quality? *Journal of Traditional and Complementary Medicine*, [online] 4(1), pp.1–7. doi:<https://doi.org/10.4103/2225-4110.124323>.

- [5] Anon, (2022). *Benefits of Chitrak (Plumbago Zeylanica), Uses and Dosage*. [online] Available at: <https://avedaayur.com/benefits-of-chitrak-plumbago-zeylanica-use-s-dosage> [Accessed 29 Aug. 2023]
- [6] Shukla, B., Saxena, S., Usmani, S. *et al.* (2021). Phytochemistry and pharmacological studies of *Plumbago zeylanica* L.: a medicinal plant review. *Clin Phytosci* 7, 34, pp. 1-25. <https://doi.org/10.1186/s40816-021-00271-7>
- [7] Quiz Ajmal, et al, (2020). Ethnomedical And Therapeutical Importance of Chitraka (*Plumbago zeylanica* Linn.) In *Valmikinagar, Bihar: Int.J.Curr.Microbiol.App.Sci*, Special Issue-11: 3776-3785. <http://www.ijemas.com>
- [8] Roy A, Bharadvaja N. (2017). A review on a pharmaceutically important medical plant: *Plumbago zeylanica*. *Journal of Ayurvedic and Herbal Medicine*, 3(4):225-228.
- [9] Singh Sadhana et al., (2018). A Brief Review on Medicinal Properties of *Chitraka (Plumbago zeylanica)* From Koshas and *Nighantus*. *IJSRR* 2018, 7(2), 25-31. <https://www.researchgate.net/publication/326367853>
- [10] Bhinde, S. *et al.* (2020) 'Standard operating procedure of purification of Chitraka (*Plumbago Zeylanica* Linn.) along with pharmacognostical and analytical profiles of Plumbagin', *AYU (An international quarterly journal of research in Ayurveda)*, 41(2), p. 117. doi:10.4103/ayu.ayu_299_20.
- [11] *Dravya-guna vigyan, bhaag 2* by P.V. SHARMA, Chaukhambha Bharati Academy, Varanasi
- [12] Agnivesa, Elaborated by Charaka and Dridabala, (1994). Edited with 'Charaka-Chandrika' Hindi commentary along with special deliberation by Tripathi Dr. Brahmanand, *Caraka Samhita, sutrasthana, shlok no. 3/4, 3rd Edition*, Chaukhambha Surbharati Prakashan, Varanasi.
- [13] Agnivesa, Elaborated by Charaka and Dridabala, (1994). Edited with 'Charaka-Chandrika' Hindi commentary along with special deliberation by Tripathi Dr. Brahmanand, *Caraka Samhita, sutrasthana, shlok no. 6/4, 3rd Edition*, Chaukhambha Surbharati Prakashan, Varanasi.
- [14] Agnivesa, Elaborated by Charaka and Dridabala, (1994). Edited with 'Charaka-Chandrika' Hindi commentary along with special deliberation by Tripathi Dr. Brahmanand, *Caraka Samhita, sutrasthana, shlok no. 45/4, 3rd Edition*, Chaukhambha Surbharati Prakashan, Varanasi.
- [15] Agnivesa, Elaborated by Charaka and Dridabala, (1994). Edited with 'Charaka-Chandrika' Hindi commentary along with special deliberation by Tripathi Dr. Brahmanand, *Caraka Samhita, sutrasthana, shlok no. 12/4, 3rd Edition*, Chaukhambha Surbharati Prakashan, Varanasi.
- [16] .Shashtri Kaviraj Ambikadatt, (Translator), (2014), *Surśuta Samhita Vol I, Sutrasthana, shlok no.—22/38, Chowkhamba Sanskrit sanshthan*, Varanasi, 2010, 184
- [17] Shashtri Kaviraj Ambikadatt, (Translator), (2014), *Surśuta Samhita Vol I, Sutrasthana, shlok no.—21/38, Chowkhamba Sanskrit sanshthan*, Varanasi, 184
- [18] Shashtri Kaviraj Ambikadatt, (Translator), (2014), *Surśuta Samhita Vol I, Sutrasthana, shlok no.—8/38, Chowkhamba Sanskrit sanshthan*, Varanasi, 183
- [19] Shashtri Kaviraj Ambikadatt, (Translator), (2014), *Surśuta Samhita Vol I, Sutrasthana, shlok no.—60/38, Chowkhamba Sanskrit sanshthan*, Varanasi, 188
- [20] Shashtri Kaviraj Ambikadatt, (Translator), (2014), *Surśuta Samhita Vol I, Sutrasthana, shlok no.—6/38, Chowkhamba Sanskrit sanshthan*, Varanasi, 183[
- [21] Tripathi B, (Hindi commentator), (2007), *Astanga Hrdayam, sutra sthana, shlok no.40/15, Chowkhamba Sanskrit Pratishthan*, Delhi
- [22] Tripathi B, (Hindi commentator), (2007), *Astanga Hrdayam, sutra sthana, shlok no.32/15, Chowkhamba Sanskrit Pratishthan*, Delhi
- [23] Tripathi B, (Hindi commentator), (2007), *Astanga Hrdayam, sutra sthana, shlok no.1/15, Chowkhamba Sanskrit Pratishthan*, Delhi
- [24] Tripathi B, (Hindi commentator), (2007), *Astanga Hrdayam, sutra sthana, shlok no.21/15, Chowkhamba Sanskrit Pratishthan*, Delhi
- [25] Tripathi B, (Hindi commentator), (2007), *Astanga Hrdayam, sutra sthana, shlok no.17/15, Chowkhamba Sanskrit Pratishthan*, Delhi
- [26] Singh Palamrit, (2008). *Dhanwantari Nighantu, Shatpushpadi Varga, shlok no.80-81, chaukhambha Orientalia Delhi*.94.
- [27] Sharma, P.V. and Sharma G. (1979). *Kaiyadeva Nighantu, Aoushadh Varga, shlok no.1177-1181, Vol. I, Chaukhambha Orientalia, Varanasi*; 217.
- [28] Sharma, P.V (2004). *Priya Nighantu, Pipalliyadi Varga, shlok no.12, Chaukhambha Surabharati Prakashana, Varanasi*. 59.
- [29] Patiayala Pt. Ramaprasad, (1998). *Madanapala Nighantu with Hindi commentary, shunthiyadi varga, shlok no.21-22, Pub. by Khemraj Srikrishnadas Prakashana, Bombay*.
- [30] Tripathi Indradev. (1982). *Raj Nighantu, Acharya Vishwanath Durvedi, Pipalliyadi Varga, shlok no.45-49, Pub. Krishna Das Academy Varanasi*, 143.
- [31] Chuneekar, K.C. and Pandey C.S., Mishra Bhav (1982). *Bhavaprakash Nighantu, Haritakyadi Varga, shlok no.7071, 6th edition, Chaukhambha Bharati Academy, Varanasi*; 21.
- [32] Sharma P.V, (2003). *Dravya Guna Vigyana, Part 2, Chaukhambha Bharati Academy, Varanasi*; (2).
- [33] Tripathi B, (Hindi commentator) (2007), *Astanga Hrdayam, sutra sthana, shlok no.21/15, Chowkhamba Sanskrit Pratishthan, Delhi*
- [34] Vishnukanta, Rana AC, (2011). *Plumbago zeylanica: A phytopharmacological review, Vol 2 Issue 2, 247-255*
- [35] Deshmukh RR, Rathod VN, Pardeshi VN, (April, 2011). *Ethanoveterinary medicine from Jalana district of Maharashtra State, Indian Journal of Traditional knowledge, Vol 10(2), 344-348*.

- [36] Singh Mukesh, Nagori Kushagra, Iyer shiv, Khare Gaurav, Sharwan Gotmi, Tripathi DK, (2011). Ethnomedicinal, Traditional and Pharmacological aspects of *Plumbago zeylanica* Linn, *Pharmacology online*, 3, 2011, 684-700.
- [37] Ganesan Kumar, Gani Sharmila Bani, (2013). Ethnomedical and pharmacological potentials of *Plumbago zeylanica* L – A review, *American journal of phytomedicine and clinical therapeutics*, 1(3), 313-337.
- [38] Mittal Vineet, Sharma SK, Pawan Jalwal, Hooda Anil, Mor J, (2010). *Plumbago zeylanica* roots: A potential source for improvement of learning and memory. *International Journal of Pharma and Biosciences*, V1(2), 1-6.
- [39] Dwivedy R, (2015). Chakradatta, Vidyaprabha Hindi Commentary, Slok no. ¼4@43½ Varanasi, Chowkhambha Sanskrit Bhavan.,
- [40] Dwivedy R, (2015). Chakradatta, Vaidyaprabha Hindi Commentary, Slok no. ¼25@25½ Varanasi, Chowkhambha Sanskrit Bhavan.
- [41] Dwivedy R, (2015). Chakradatta, Vidyaprabha Hindi Commentary, Slok no. ¼6@72½ Varanasi, Chowkhambha Sanskrit Bhavan.
- [42] Dwivedy R, (2015). Chakradatta, Vaidyaprabha Hindi Commentary, Slok no. ¼8@10½ Varanasi, Chowkhambha Sanskrit Bhavan.
- [43] Dwivedy R, (2015). Chakradatta, Vaidyaprabha Hindi Commentary, Slok no. ¼9@24½ Varanasi, Chowkhambha Sanskrit Bhavan.
- [44] Dwivedy R, (2015). Chakradatta, Vaidyaprabha Hindi Commentary, Slok no. ¼1@103½ Varanasi, Chowkhambha Sanskrit Bhavan.
- [45] Dwivedy R, (2015). Chakradatta, Vaidyaprabha Hindi Commentary, Slok no. ¼4@9½ Varanasi, Chowkhambha Sanskrit Bhavan.
- [46] Dwivedy R, (2015). Chakradatta, Vaidyaprabha Hindi Commentary, Slok no. Varanasi, Chowkhambha Sanskrit Bhavan., ¼4@44½
- [47] Dwivedy R, (2015). Chakradatta, Vaidyaprabha Hindi Commentary, ¼39@29½ Varanasi, Chowkhambha Sanskrit Bhavan, reprint 2015,
- [48] Dwivedy R, (2015). Chakradatta, Vaidyaprabha Hindi Commentary, Slok no. ¼39@31½ Varanasi, Chowkhambha Sanskrit Bhavan.
- [49] Dwivedy R, (2015). Chakradatta, Vaidyaprabha Hindi Commentary, Slok no. ¼39@33&34½ Varanasi, Chowkhambha Sanskrit Bhavan.
- [50] Dwivedy R, Chakradatta, (2015). Vaidyaprabha Hindi Commentary, Slok no. ¼42@5½ Varanasi, Chowkhambha Sanskrit Bhavan, reprint 2015,
- [51] Sharangdhara's Sharangdhara Samhita, (2012) Madyama Khandha, Slok no. ¼2@35&40½, English translation by Pro. K.R. Srikantha Murthy, Reprint edition, Varanasi, Chaukamba Orientalia.
- [52] Sharangdhara's Sharangdhara Samhita, (2012) Madyama Khandha Slok no., (2/43-44), English translation by Pro. K.R. Srikantha Murthy, Reprint edition, Varanasi, Chaukamba Orientalia.
- [53] Sharangdhara's Sharangdhara Samhita, (2012) Madyama Khandha Slok no. , (2/43-44), English translation by Pro. K.R. Srikantha Murthy, Reprint edition, Varanasi, Chaukamba Orientalia.
- [54] Sharangdhara's Sharangdhara Samhita, (2012) Madyama Khandha, Slok no. ¼6@13&14½, English translation by Pro. K.R. Srikantha Murthy, Reprint edition, Varanasi, Chaukamba Orientalia.
- [55] Sharangdhara's Sharangdhara Samhita, (2012) Madyama Khandha, Slok no. ¼6@161&163½, English translation by Pro. K.R. Srikantha Murthy, Reprint edition, Varanasi, Chaukamba Orientalia..
- [56] Sharangdhara's Sharangdhara Samhita, (2012) Madyama Khandha, Slok no. ¼6@22&23½, English translation by Pro. K.R. Srikantha Murthy, Reprint edition, Varanasi, Chaukamba Orientalia.
- [57] Sharangdhara's Sharangdhara Samhita, (2012) Madyama Khandha, Slok no. ¼8@5&9½, English translation by Pro. K.R. Srikantha Murthy, Reprint edition, Varanasi, Chaukamba Orientalia.
- [58] Sharangdhara's Sharangdhara Samhita, (2012) Madyama Khandha Slok no. ¼9@21&24½, English translation by Pro. K.R. Srikantha Murthy, Reprint edition, Varanasi, Chaukamba Orientalia.
- [59] Sharangdhara's Sharangdhara Samhita, (2012) Madyama Khandha Slok no. ¼9@60&65½, English translation by Pro. K.R. Srikantha Murthy, Reprint edition, Varanasi, Chaukamba Orientalia.
- [60] Sharangdhara's Sharangdhara Samhita, (2012) Madyama Khandha Slok no. ¼9@61&65½, English translation by Pro. K.R. Srikantha Murthy, Reprint edition, Varanasi, Chaukamba Orientalia.
- [61] Sharangdhara's Sharangdhara Samhita, (2012) Madyama Khandha Slok no. ¼9@75&78½, English translation by Pro. K.R. Srikantha Murthy, Reprint edition, Varanasi, Chaukamba Orientalia.
- [62] A review on multi&purpose medicinal plant *Plumbago zeylanica* and in&vitro production of plumbagin [Internet]-Available from% https://www-researchgatenet/publication/315379475_A_review_on_multi&purpose_medicinal_plant_Plumbago_zeylanica_and_in_&vitro_production_of_plumbagin.
- [63] Poosarla A] Kumar BV] Rao TR] Rao DN] Athota RR-(2007), Hepatoprotective effect of *Plumbago zeylanica* on paracetamol induced liver toxicity in rats [Internet]-- Available from% https://www. Alleviation of collagen&induced arthritis by Plumbago_zeylanica_in_mice- Pharmaceutical Biology, Jan;45¼1½%54-9-

- [64] Dhale DA, Markandeya SK,(2011). Antimicrobial and phytochemical screening of *Plumbago zeylanica* Linn (Plumbaginaceae) leaf, *Journal of experimental sciences*, Vol2, Issue3, 4-6.
- [65] Tilak JC] Adhikari S](2004) Devasagayam TPA- Antioxidant properties of *Plumbago zeylanica*] an Indian medicinal plant and its active ingredient] plumbagin- RedoÚ report % communications in free radical research [Internet]-[cited 2022 Feb 8];9¼½%219–27- Available from% <https://pubmed.ncbi.nlm.nih.gov/15479566/>
- [66] Arya N Sharma A.(2015). THE THERAPEUTIC AND TOXICOLOGICAL EFFECT OF CHITRAK kPLUMBAGO ZEYLANICA L-½& A REVIEW- AYUSHDHARA [Internet]-Dec 8;2¼½- Available from% <https://ayushdhara-in.deÚ-php/ayushdhara/article/view/78>
- [67] Poonam et al. (2020). CLINICAL STUDY TO ACCESS THE EFFICACY OF HARIDRA AND CHITRAK IN MANAGEMENT OF MEDOROGA (OBESITY); *World Journal of Pharmaceutical and Life Science*; Vol 6, Issue 12, pp. 187, www.wjpls.org.
- [68] Ganeasan K,Gani SB (2013)..Ethnomedical and pharmacological potentials of *P. zeylanica* L:A review.*Am J Phytomed Clin Ther.*:313-37.
- [69] Chauhan M.A , (2014). Review on morphology,phytochemistry and pharmacological activities of medicinal herb *Plumbago zeylanica* Linn.,*Int J Pharmacogn Phytochem.*:3(2);95-118.
- [70] Vishnukanta S,Rana C (2010).Plumbago zeylanica:a phytopharmacological review:*Int J Pharm Sci Res.*2010:247-55.
- [73] Deshmukh RR, Rathod VN, Pardeshi VN,(April,2011). Ethanoveterinary medicine from Jalana district of Maharashtra State, *Indian Journal of Traditional knowledge*, Vol 10(2), 344-348.
- [74] Nag Ambika, Galav Praveen, Katewa SS,(2007). Indigenous animal healthcare practices from Udaipur district, Rajasthan, *Indian Journal of Traditional knowledge*, Vol 6(4), October, 583-588.
- [75] Hiradeve Sachin, Danao Kishore, Kharabe Vijay, Mendhe Bibhilesh,(2010). Evaluation of anticancer activity of *Plumbago zeylanica* Linn. Leaf extract, *International Journal of Biomedical Research*, 1(2), 1-9.
- [76] Mittal Vineet, Sharma SK, Kaushik Deepak, Khatri Meenu, Tomar Kusum, (2010).A comparative study of analgesic activity of *Plumbago zeylanica* Linn callus and root extracts in experimental mice, *Research Journal of Pharmaceutical, Biological, and Chemical sciences*, 1(4), October-December, 830-836.
- [77] Poosarla A] Kumar BV] Rao TR] Rao DN] Athota RR-(2007), Hepatoprotective effect of *Plumbago zeylanica* on paracetamol induced liver toxicity in rats [Internet]-- Available from% <https://www. Alleviation of collagen&induced arthritis by Plumbago zeylanica in mice- Pharmaceutical Biology, Jan;45¼½%54–9->

ADDITIONAL READINGS

[A] Natural Compounds from *Plumbago zeylanica* as Complementary and Alternative Medicine

URL:

https://link.springer.com/referenceworkentry/10.1007/978-981-16-1247-3_33-1

[B] Anti-Inflammatory and Anti-Microbial Potential of *Plumbago zeylanica* L.: A Review

URL: <https://jddtonline.info/index.php/jddt/article/view/4445>

[C] Can Ceylon Leadwort (*Plumbago zeylanica* L.) Acclimate to Lead Toxicity?—Studies of Photosynthetic Apparatus Efficiency

URL: <https://www.mdpi.com/1422-0067/21/5/1866>

[D] Determination of antioxidant and antibacterial activities of leaf extracts of *Plumbago zeylanica* (Amira)

URL:

<https://www.tandfonline.com/doi/full/10.1080/23312009.2020.1831715>

[E] Extract of *Plumbago zeylanica* enhances the growth of hair follicle dermal papilla cells with down-regulation of 5α-reductase type II

URL: <https://onlinelibrary.wiley.com/doi/abs/10.1111/jocd.13355>

ANNEXURE

Key Terms and Definitions

CHITRAK– A profusely branched perennial shrub with alternate leaves. The plant is available throughout India wildy and is also cultivated in gardens for its brilliant inflorescence. The root and root bark of the plant are used in preparation of various Ayurvedic medicines. Leadwort is a potent medicinal agent used in the treatment of stubborn chronic rheumatoid arthritis, skin diseases and tumorous growths as recommended by Ayurveda. It also finds its use in correcting chronic menstrual disorders, viral warts, and chronic diseases of the nervous system. Extract of various fractions of Chitrakmool have been identified as anticancer drugs. Root Bark is also considered useful in obesity.

AGNI- Agni is the invariable agent in the process of *Paka* (digestion, transformation). Ingested food is to be digested, absorbed, and assimilated, which is unavoidable for the maintenance of life, and is performed by the *Agni*. Different examples are available in our classics to indicate that *Pitta* is the

same as *Agni*. According to the functions and site of action, *Agni* has been divided into 13 types, i.e., one *Jatharagni*, five *Bhutagni* and seven *Dhatvagni*. *Jatharagni* is the most important one, which digests four types of food and transforms it into *Rasa* and *Mala*. The five *Bhutagnis* act on the respective *bhutika* portion of the food and thereby nourish the *Bhutas* in the body. The seven *Dhatvagni* act on the respective *dhatu*s by which each *Dhatu* is broken into three parts. *Agni* converts food into the form of energy, which is responsible for all the vital functions of our body.

LIFESTYLE: Human are in a constant rat race to achieve the best, in between, they forget to focus on their health and wellbeing. In fact, with such a hectic lifestyle that humans expose themselves to stress and too many lifestyle disorders as hypertension, diabetes, anxiety, strokes, arthritis, cancer, obesity etc.

CHRONIC DISEASES: A disease or condition that usually lasts for 3 months or longer and may get worse over time. Chronic diseases tend to occur in older adults and can usually be controlled but not cured. The most common types of chronic disease are cancer, heart disease, stroke, diabetes, arthritis, obesity, hypertension etc.

AGNIMANDYA: *Agnimandya* is itself considered an independent digestive disease and a cause of a huge number of other diseases in Ayurveda. *Agni*- the digestive fire is responsible for the transformation of food we take into energy and nourishment to body tissues. It is responsible for our strength, energy, complexion, health, sustainability as well as immunity. There are four forms of the *Agni* – *Samagni*, *Visamagni*, *Mandagni*, and *Tikshagni*; among which *Mandagni* or *Agnimandya* is referred to as the root cause of all diseases. *Agni* literally translates to fire. *Manda* means weakness. So, *Agnimandya* means the weak digestive fire. While an ignited digestive fire is responsible for the overall good health of a person, a weak form of the same is a disease and origin of diseases. When the fire and the digestion are weak,

even light forms of food taken are not digested well resulting in indigestion. And when food is not digested well, the absorption, assimilation and tissue formation, nourishment and functioning are affected.

Authors' Profile



Dr. Preeti Sharma, basically from Bareilly district, Uttar Pradesh state. She is Associate Professor and Head of the department (Dravya Guna) in Rajshree Ayurvedic Medical college and Hospital, Bareilly (U.P). She is actively involved in various awareness and research programmes of Ayurveda. She contributes articles to e publication.

Currently She is doing Ph. d from Desh Bhagat University, Punjab and She is writing a book on poisonous plants.



Dr. Rohit Rastogi received his B.E. in CS from C. C. S. Univ. Meerut, 2003. Master's degree in CS of NITTTR-Chandigarh from Punjab University. He has obtained his doctoral degree from the Dayalbagh Educational Institute in Agra, India. He is serving as Professor in the CSE department of ABES Engineering College, Ghaziabad, India.

He has won awards in several areas, including improved education, significant contributions, human value promotion, and long-term service. He keeps himself engaged in various competition events, activities, webinars, seminars, workshops, research, and various other educational learning forums. He has guided around 100 Btech Students researchers and 5 M.tech. Thesis consequently 3 Ph.D. candidates. He is editor and reviewer member of several international Journals and conferences. He has 145+ publications in Scopus Indexed journals and conferences of international repute. He strongly believes that Transformation starts within self.



Dr. Bhavna Singh is Ayurvedic Practitioner and currently acting as Principal in Ayurvedic College, Hapur, U.P., India. She has a keen interest in studying herbs and their effects on the human body. She has done scientific experiments of different herbals and their vaporized state through Yajna on patient diseases. She is also fond of scientific

writings and establishing Indian Vedic wisdom through logical explanations.

She has been actively working in the Thought Transformation movement and strongly feels that science and spirituality can move

together to enrich each other. Her many papers are imprinted on various scientific journals.



Mr. Sandeep Kumar is currently pursuing his Bachelor of Ayurvedic Medicine and Surgery (BAMS) degree at GS AYURVEDA MEDICAL COLLEGE, Hapur. He has a keen interest in research studies, and he is passionate about Ayurveda and its holistic approach to healthcare, Disease prevention and treatment which emphasizes the use of natural remedies and lifestyle modifications.



Ms. Gunjan Nagar is currently pursuing Bachelor of Ayurvedic medicine and surgery (4th year) from GS AYURVEDA MEDICAL COLLEGE AND HOSPITAL, Pilkhuwa, Hapur. She is very passionate about Ayurveda as the legacy which has been passed down by generations and is really in awe of the power of nature and natural remedies.

She looks forward to working for Ayurveda and in Ayurveda. She aspires to make people aware of this precious inheritance of the Indian Subcontinent.



Mr. Prashant Rathore is currently pursuing Bachelor of Ayurvedic Medicine and Surgery (1st year) at Kritika Ayurvedic Medical College and Hospital, Bareilly. He has pure interest in Ayurveda because of its approach to the disease. He will continue to work for Ayurveda. His mission is to keep Ayurveda alive for humanity and to

make people benefit from its treasure.

Resilience-Aware Fuzzy Optimization for Cyber Forensic Evidence Reconstruction under Adversarial Uncertainty

Charles Sagayaraj A. C.¹, Santha Sheela A. C.², Ramesh M³

¹*Department of Mathematics, Rajalakshmi Engineering College (Autonomous), Thandalam, Chennai – 602105, India*

¹*accharlez@gmail.com*

²*Department of Computer Science and Engineering, Sathyabama Institute of Science and Technology, Chennai – 600119, India*

²*santhasheela.cse@sathyabama.ac.in*

³*Department of Computer Science and Applications, SRM Institute of Science and Technology, Vadapalani, Chennai – 600026, India*

³*rameshm@srmist.edu.in*

ARTICLE INFO

Article history:

Received 01 May 2026

Received in revised form 19 May 2026

Accepted 12 June 2026

Available online 12 July 2026

Keywords:

Cyber forensics

Fuzzy optimization

Adversarial uncertainty

Inconsistency modeling

Metaheuristic optimization

ABSTRACT

Cyber forensic analysis involves reconstructing event sequences from heterogeneous and often unreliable digital evidence. In adversarial environments, such evidence may be incomplete, noisy, or deliberately manipulated, making traditional deterministic and probabilistic approaches insufficient. This chapter proposes a resilience-aware fuzzy optimization framework for cyber forensic evidence reconstruction. The approach models evidence using fuzzy representations of confidence and uncertainty, and formulates reconstruction as a nonlinear optimization problem that integrates evidence support, uncertainty penalization, and inconsistency minimization. A novel inconsistency modeling mechanism is introduced to capture contradictions among evidence sources. To solve the resulting optimization problem, an adaptive hybrid metaheuristic combining Differential Evolution and Grey Wolf Optimization with fuzzy control is developed. The framework demonstrates improved robustness and consistency under adversarial perturbations, providing a reliable approach for cyber forensic reconstruction in uncertain environments.

1. INTRODUCTION

The rapid proliferation of digital systems has led to an exponential increase in cyber incidents, ranging from insider threats to sophisticated multi-stage attacks. In such environments, digital forensics plays a critical role in reconstructing event sequences, attributing malicious actions, and supporting legal and organizational responses. However, forensic reconstruction in cyber systems is inherently challenging due to the presence of incomplete, noisy, and potentially manipulated evidence.

Traditional forensic analysis methods rely on deterministic reasoning or probabilistic inference frameworks. While these approaches are effective under well-defined conditions, they exhibit significant

limitations in adversarial settings. In particular, cyber evidence often originates from heterogeneous sources such as system logs, network traces, and user activity records, which may be inconsistent or partially corrupted. Moreover, attackers can deliberately introduce ambiguity through log tampering, deletion, or injection of misleading events, thereby undermining classical inference mechanisms.

Fuzzy logic-based approaches have been explored to address uncertainty in cyber forensic analysis. These methods provide a flexible mechanism to represent partial truth and ambiguity through membership functions. However, existing fuzzy frameworks typically focus on isolated evidence evaluation and lack a principled mechanism to model inter-evidence inconsistency and adversarial perturbations. As a

result, they fail to provide robust reconstruction in complex and hostile environments.

In parallel, optimization-based methods have been employed to infer attack paths and reconstruct scenarios by searching over feasible solution spaces. While these methods offer improved flexibility, they often treat uncertainty in a superficial manner and do not explicitly incorporate inconsistency or resilience considerations into the objective formulation. Furthermore, standard metaheuristic algorithms suffer from instability and premature convergence when applied to highly uncertain and noisy forensic data.

To address these limitations, this chapter proposes a *Resilience-Aware Fuzzy Optimization Framework* for cyber forensic evidence reconstruction. The central idea is to integrate fuzzy evidence modeling, inconsistency quantification, and robustness against adversarial perturbations within a unified optimization paradigm. Specifically, we formulate forensic reconstruction as a nonlinear optimization problem that simultaneously maximizes evidence consistency, minimizes uncertainty, and penalizes contradictions among evidence sources.

The proposed framework introduces three key contributions:

- **Resilience-aware fuzzy evidence modeling:** A structured representation of forensic evidence incorporating both confidence (membership) and uncertainty (spread), enabling robust handling of incomplete and noisy data.
- **Inconsistency-driven objective formulation:** A novel inconsistency functional that explicitly penalizes contradictory evidence, ensuring coherent reconstruction of forensic scenarios.
- **Adaptive fuzzy hybrid optimization algorithm:** A resilience-aware hybrid metaheuristic combining Differential Evolution and Grey Wolf Optimization, augmented with a fuzzy control mechanism for dynamic parameter adaptation under uncertainty.

Extensive experiments on real-world and adversarial datasets demonstrate that the proposed approach

achieves superior reconstruction accuracy, improved consistency, and enhanced robustness compared to existing methods.

The chapter is organized to progressively develop the proposed framework from conceptual foundations to practical validation. Following this introduction, the next section critically reviews existing approaches in cyber forensics, fuzzy modeling, and optimization, highlighting their limitations under adversarial uncertainty.

Subsequently, a resilience-aware fuzzy evidence modeling framework is formulated, where uncertainty, inconsistency, and adversarial perturbations are explicitly incorporated into a unified optimization objective. This is followed by the development of an adaptive hybrid optimization algorithm that integrates Differential Evolution and Grey Wolf Optimization with a fuzzy control mechanism for dynamic parameter adaptation.

The effectiveness of the proposed approach is then validated through comprehensive experimental evaluation on real-world and adversarial datasets, including robustness and ablation analyses. Finally, the chapter concludes with key findings, limitations, and directions for future research.

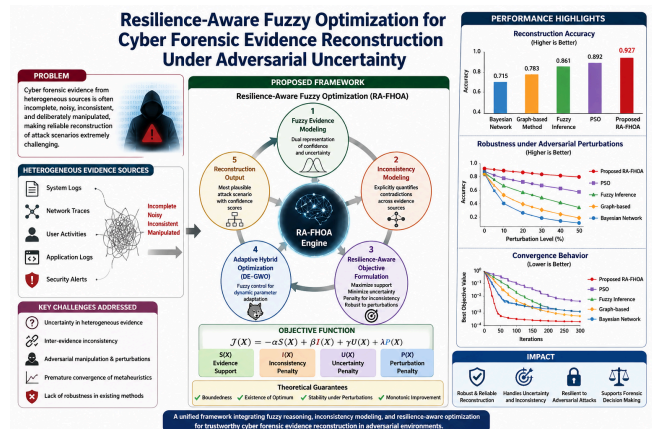


Figure 1: Proposed Framework

As illustrated in Figure 1, the proposed framework integrates fuzzy evidence modeling, inconsistency quantification, and adaptive optimization to enable robust forensic reconstruction under adversarial conditions.

2. RELATED WORK

Cyber forensic analysis has evolved significantly in response to the increasing sophistication of cyber-attacks and the growing complexity of digital infrastructures. Existing approaches can be broadly categorized into probabilistic inference methods, graph-based reconstruction techniques, fuzzy logic-based models, and optimization-driven frameworks.

PROBABILISTIC AND STATISTICAL APPROACHES

Probabilistic models, particularly Bayesian networks, have been widely employed for cyber forensic inference and attack reconstruction. These approaches model causal dependencies among events and estimate posterior probabilities to identify likely attack scenarios. While effective in well-structured environments, their performance deteriorates in the presence of incomplete, noisy, or adversarially manipulated data. Moreover, the reliance on accurate prior distributions limits their applicability in real-world forensic settings, where such information is often unavailable or unreliable.

Statistical and machine learning-based methods have also been extensively explored for anomaly detection and intrusion analysis (r12?; r20?). Although these techniques demonstrate strong performance in identifying suspicious patterns, they are primarily designed for detection rather than reconstruction. In addition, their lack of interpretability poses significant challenges in forensic investigations, where explainability and evidential consistency are critical.

GRAPH-BASED FORENSIC RECONSTRUCTION

Graph-based approaches represent cyber events as nodes and their relationships as edges, enabling structured modeling of attack paths and dependencies. These methods facilitate multi-stage attack reconstruction and provide valuable insights into the progression of adversarial activities.

Despite their structural advantages, traditional graph-based models are inherently deterministic and lack the ability to represent uncertainty and ambiguity in evidence. Extensions incorporating probabilistic or weighted graphs partially address this limitation; however, they still do not provide a principled mechanism for handling conflicting or contradictory evidence. Furthermore, such models are not inherently robust to adversarial manipulation, which can significantly distort graph structures and inference outcomes.

FUZZY LOGIC-BASED MODELS

Fuzzy logic has been widely adopted to model uncertainty and imprecision in cyber security applications, including intrusion detection, risk assessment, and forensic reasoning. By representing evidence using membership functions, fuzzy systems enable flexible handling of partial truth and ambiguous information.

However, existing fuzzy approaches are typically based on rule-driven aggregation mechanisms and often treat evidence independently. This limits their ability to capture inter-evidence relationships, particularly in scenarios involving conflicting or inconsistent information. Moreover, conventional fuzzy frameworks do not explicitly account for adversarial perturbations, making them vulnerable in hostile environments where evidence may be deliberately manipulated.

OPTIMIZATION-BASED METHODS

Optimization techniques, including genetic algorithms, particle swarm optimization, and differential evolution, have been applied to cyber forensic reconstruction and attack path inference. These methods formulate reconstruction as a search problem over a feasible solution space, enabling flexible exploration of possible event configurations. While optimization-based approaches offer scalability and adaptability, they often lack a rigorous integration of uncertainty and inconsistency into the objective formulation. In many cases, uncertainty is treated

implicitly or through simplistic penalty terms, which are insufficient for capturing complex forensic scenarios. Additionally, standalone metaheuristic algorithms are prone to premature convergence and instability when applied to highly uncertain and noisy data.

Hybrid optimization frameworks have been proposed to improve performance by combining complementary search strategies. However, many such approaches are constructed heuristically, without a clear theoretical linkage between the optimization mechanism and the underlying forensic modeling requirements. This limits their interpretability and robustness in adversarial settings.

RESEARCH GAP AND POSITIONING

The above discussion highlights several critical limitations in existing approaches:

- inadequate modeling of uncertainty under adversarial conditions,
- absence of explicit quantification of inter-evidence inconsistency,
- weak integration between fuzzy reasoning and optimization-based reconstruction,
- limited robustness against manipulated or incomplete forensic evidence.

To address these challenges, this chapter proposes a unified framework that integrates fuzzy evidence modeling, inconsistency-driven optimization, and resilience-aware algorithmic design. Unlike existing methods, the proposed approach explicitly incorporates inter-evidence contradiction into the objective functional and employs an adaptive hybrid optimization strategy to ensure stable and robust reconstruction under uncertainty.

This positioning establishes a clear distinction from prior work and contributes toward advancing cyber forensic analysis in adversarial environments.

3. FUZZY EVIDENCE MODELING FRAMEWORK

In cyber forensic analysis, evidence is inherently uncertain, incomplete, and potentially manipulated. Classical deterministic or probabilistic frameworks fail to adequately capture this uncertainty, particularly under adversarial conditions. To address this limitation, we propose a resilience-aware fuzzy optimization framework that models evidence strength, uncertainty, and inter-evidence consistency within a unified formulation.

3.1 PRELIMINARIES

This section introduces the basic notation and concepts used throughout the chapter. The focus is on establishing a consistent mathematical framework for fuzzy evidence modeling and optimization.

3.1.1 NOTATION

Let $E = \{e_1, e_2, \dots, e_n\}$ denote the set of forensic evidence obtained from heterogeneous sources. A candidate forensic scenario is denoted by $X \in X$, where X represents the feasible solution space.

For each evidence element e_i , we define:

$\mu_i(X) \in [0, 1]$: membership degree representing confidence,

$\sigma_i(X) \in [0, 1]$: uncertainty measure,

τ_i : temporal attribute.

3.1.2 FUZZY EVIDENCE REPRESENTATION

Each evidence element is modeled as a fuzzy tuple:

$$e_i = (\mu_i, \sigma_i, \tau_i)$$

where μ_i captures reliability and σ_i reflects ambiguity due to incomplete or noisy observations.

3.1.3 INCONSISTENCY MODELING

Inconsistency arises when evidence elements contradict each other under a given scenario. For two evidence elements e_i and e_j , the pairwise inconsistency is defined as:

$$\psi_{ij}(X) = w_{ij} \cdot |\mu_i(X) - \mu_j(X)| \cdot \delta_{ij}(X)$$

where $w_{ij} \in [0, 1]$ represents interaction strength and $\delta_{ij}(X)$ encodes logical or temporal conflicts.

The global inconsistency is given by:

$$\Psi(X) = \sum_{i=1}^n \sum_{j=i+1}^n \psi_{ij}(X)$$

3.1.4 OPTIMIZATION OBJECTIVE

The forensic reconstruction problem is formulated as:

$$\max_{X \in X} J(X)$$

where $J(X)$ integrates evidence support, uncertainty penalization, and inconsistency minimization as defined in Section 1.

3.1.5 ADVERSARIAL PERTURBATION MODEL

Let ϵ_i denote perturbations introduced by adversarial manipulation. The perturbed membership is:

$$\tilde{\mu}_i = \mu_i + \epsilon_i$$

The framework is considered robust if variations in $J(X)$ remain bounded under small perturbations.

3.2 FUZZY REPRESENTATION OF FORENSIC EVIDENCE

Let $E = \{e_1, e_2, \dots, e_n\}$ denote the set of forensic evidence extracted from heterogeneous sources such as system logs, network traces, and user activity records.

Each evidence e_i is associated with a fuzzy membership degree $\mu_i \in [0, 1]$, representing the degree of confidence in its validity, and an uncertainty spread $\sigma_i \in [0, 1]$, capturing ambiguity due to noise, incompleteness, or potential manipulation.

Each evidence element is represented as a tuple:

$$e_i = (\mu_i, \sigma_i, \tau_i)$$

where τ_i denotes the temporal attribute associated with the evidence.

3.3 FORENSIC SCENARIO SPACE

Let X denote the space of all feasible forensic scenarios. A scenario $X \in X$ represents a hypothesized reconstruction of events consistent with observed evidence.

Each scenario induces a mapping:

$$\mu_i(X), \quad \sigma_i(X)$$

reflecting the compatibility of evidence e_i with scenario X .

3.4 RESILIENCE-AWARE OBJECTIVE FUNCTIONAL

We define a composite objective functional that integrates evidence strength, uncertainty minimization, and consistency enforcement:

$$\max_{X \in X} J(X) = \sum_{i=1}^n \mu_i(X) - \alpha \sum_{i=1}^n \sigma_i(X) - \beta \Psi(X) \quad (1)$$

where:

- $\alpha > 0$ is the uncertainty penalization parameter,
- $\beta > 0$ controls the influence of inconsistency,
- $\Psi(X)$ quantifies inter-evidence inconsistency.

3.5 INCONSISTENCY MODELING

In forensic reconstruction, inconsistencies arise when multiple evidence elements contradict each other in temporal, logical, or contextual dimensions.

Definition 2 (Pairwise Inconsistency). The inconsistency between two evidence elements e_i and e_j under scenario X is defined as:

$$\psi_{ij}(X) = w_{ij} \cdot |\mu_i(X) - \mu_j(X)| \cdot \delta_{ij}(X)$$

where:

- $w_{ij} \in [0, 1]$ is the interaction weight,
- $\delta_{ij}(X)$ is a contradiction indicator function incorporating temporal and logical constraints.

Definition 3 (Global Inconsistency Functional).

$$\Psi(X) = \sum_{i=1}^n \sum_{j=i+1}^n \psi_{ij}(X)$$

This formulation ensures that mutually contradictory evidence reduces the overall objective value, thereby enforcing consistency.

3.6 RESILIENCE AGAINST ADVERSARIAL PERTURBATIONS

To account for adversarial manipulation, we introduce perturbation-aware uncertainty modeling.

Let ϵ_i denote an adversarial perturbation applied to evidence e_i . The perturbed membership becomes:

$$\tilde{\mu}_i = \mu_i + \epsilon_i$$

Definition 4 (Resilience Condition). A forensic reconstruction framework is said to be resilient if:

$$|J(X) - J_\epsilon(X)| \leq \kappa \|\epsilon\|$$

for some bounded constant $\kappa > 0$.

This condition guarantees that small adversarial manipulations do not significantly degrade reconstruction quality.

3.7 PROBLEM STATEMENT

The forensic reconstruction problem is thus formulated as:

$$\text{Find } X^* \in X \text{ such that } J(X^*) = \max_{X \in X} J(X)$$

This constitutes a nonlinear, non-convex optimization problem requiring robust metaheuristic strategies for practical computation.

4 THEORETICAL ANALYSIS

In this subsection, we establish fundamental properties of the proposed objective functional, including boundedness, existence of optimal solutions, and stability under adversarial perturbations.

4.1 BOUNDEDNESS OF THE OBJECTIVE FUNCTIONAL

Theorem 1 (Boundedness). Let $\mu_i(X), \sigma_i(X) \in [0, 1]$ for all $i = 1, \dots, n$, and assume $w_{ij} \in [0, 1]$. Then, the objective functional $J(X)$ defined in Eq. (1) is bounded.

Proof. Since $\mu_i(X) \in [0, 1]$, we have:

$$0 \leq \sum_{i=1}^n \mu_i(X) \leq n.$$

Similarly, since $\sigma_i(X) \in [0, 1]$:

$$0 \leq \sum_{i=1}^n \sigma_i(X) \leq n.$$

For the inconsistency term, observe that:

$$|\mu_i(X) - \mu_j(X)| \leq 1,$$

and since $w_{ij} \in [0, 1]$ and $\delta_{ij}(X) \in [0, 1]$, we obtain:

$$0 \leq \psi_{ij}(X) \leq 1.$$

Thus:

$$0 \leq \Psi(X) \leq \frac{n(n-1)}{2}.$$

Therefore, the objective function satisfies:

$$-\alpha n - \beta \frac{n(n-1)}{2} \leq J(X) \leq n.$$

Hence, $J(X)$ is bounded. $\square$

4.2 EXISTENCE OF OPTIMAL SOLUTION

Theorem 2 (Existence of Maximizer). Assume that the feasible set X is compact and that $\mu_i(X)$ and $\sigma_i(X)$ are continuous functions over X . Then, there exists at least one optimal solution $X^* \in X$ such that:

$$J(X^*) = \max_{X \in X} J(X).$$

Proof. The objective functional $J(X)$ is composed of finite sums of continuous functions $\mu_i(X)$, $\sigma_i(X)$, and $\psi_{ij}(X)$, each of which depends continuously on X by assumption. Hence, $J(X)$ is continuous over X .

Since X is compact and $J(X)$ is continuous, the extreme value theorem guarantees that $J(X)$ attains its maximum at some $X^* \in X$.

Therefore, an optimal solution exists. $\square$

4.3 STABILITY UNDER ADVERSARIAL PERTURBATIONS

Theorem 3 (Perturbation Stability). Let $\tilde{\mu}_i(X) = \mu_i(X) + \epsilon_i$ denote perturbed memberships

with $\|\epsilon\|_\infty \leq \delta$. Then, the change in the objective functional satisfies:

$$|J_\epsilon(X) - J(X)| \leq C\delta,$$

for some constant $C > 0$.

Proof. Consider the perturbed objective:

$$J_\epsilon(X) = \sum_i (\mu_i + \epsilon_i) - \alpha \sum_i \sigma_i - \beta \Psi_\epsilon(X).$$

The first term satisfies:

$$\left| \sum_i \epsilon_i \right| \leq n\delta.$$

For the inconsistency term, observe that:

$$|\tilde{\mu}_i - \tilde{\mu}_j - (\mu_i - \mu_j)| \leq |\epsilon_i| + |\epsilon_j| \leq 2\delta.$$

Thus:

$$|\Psi_\epsilon(X) - \Psi(X)| \leq \beta \cdot \frac{n(n-1)}{2} \cdot 2\delta.$$

Combining terms, we obtain:

$$|J_\epsilon(X) - J(X)| \leq n\delta + \beta n(n-1)\delta = C\delta,$$

for some constant $C > 0$.

Hence, the objective functional is Lipschitz continuous with respect to perturbations, establishing stability. $\square$

This result establishes Lipschitz continuity of the objective functional with respect to adversarial perturbations, ensuring robustness guarantees in uncertain forensic environments.

4.4 MONOTONIC IMPROVEMENT PROPERTY

Theorem 4 (Monotonic Fitness Improvement). Under elitist selection, the sequence of best objective values $\{J(X^{(t)})\}$ is non-decreasing over iterations.

Proof. At each iteration, candidate solutions are updated only if their fitness improves. Therefore, the best solution at iteration $t + 1$ satisfies:

$$J(X^{(t+1)}) \geq J(X^{(t)}).$$

Hence, the sequence is monotonic non-decreasing. $\square$

5 RESILIENCE-AWARE ADAPTIVE FUZZY HYBRID OPTIMIZATION

The optimization problem defined in Eq. (1) is nonlinear, non-convex, and involves complex interdependencies arising from uncertainty and inconsistency modeling. Classical optimization techniques are inadequate due to the absence of gradient information and the presence of adversarial perturbations.

To address these challenges, we propose a *Resilience-Aware Adaptive Fuzzy Hybrid Optimization Algorithm* (RA-FHOA), which integrates the exploration capability of Differential Evolution (DE) with the exploitation dynamics of Grey Wolf Optimization (GWO), governed by an adaptive fuzzy control mechanism.

5.1 SOLUTION ENCODING

Each candidate solution represents a forensic scenario:

$$X = (x_1, x_2, \dots, x_d) \in X$$

where each component encodes a decision variable associated with evidence alignment, temporal ordering, or attribution.

5.2 POPULATION INITIALIZATION

An initial population $\{X_k^{(0)}\}_{k=1}^N$ is generated using a stratified random scheme to ensure coverage of the feasible space:

$$X_k^{(0)} \sim U(X)$$

The fitness of each solution is evaluated using the objective functional $J(X)$.

5.3 DIFFERENTIAL EVOLUTION PHASE (EXPLORATION)

To promote global exploration, mutation is performed as:

$$V_k^{(t)} = X_{r1}^{(t)} + F^{(t)} \cdot (X_{r2}^{(t)} - X_{r3}^{(t)})$$

where:

- $r1, r2, r3$ are distinct indices,
- $F^{(t)}$ is the adaptive scaling factor.

Crossover is applied to generate trial vectors:

$$U_{k,j}^{(t)} = \{V_{k,j}^{(t)}, \text{ if } rand_j \leq CR^{(t)} X_{k,j}^{(t)}, \text{ otherwise}\}$$

Selection follows:

$$X_k^{(t+1)} = \{U_k^{(t)}, \text{ if } J(U_k^{(t)}) > J(X_k^{(t)}) X_k^{(t)}, \text{ otherwise}\}$$

5.4 GREY WOLF OPTIMIZATION PHASE (EXPLOITATION)

The top three solutions are denoted as α , β , and δ . Position updates are defined as:

$$D_\alpha = |C_1 \cdot X_\alpha - X_k|, \quad X_1 = X_\alpha - A_1 \cdot D_\alpha$$

$$D_\beta = |C_2 \cdot X_\beta - X_k|, \quad X_2 = X_\beta - A_2 \cdot D_\beta$$

$$D_\delta = |C_3 \cdot X_\delta - X_k|, \quad X_3 = X_\delta - A_3 \cdot D_\delta$$

$$X_k^{(t+1)} = \frac{X_1 + X_2 + X_3}{3}$$

where A_i and C_i are coefficient vectors controlling convergence.

5.5 ADAPTIVE FUZZY CONTROL MECHANISM

To balance exploration and exploitation under uncertainty, algorithmic parameters are dynamically adjusted using a fuzzy inference system.

Input Variables:

- $\sigma^{-(t)}$: average uncertainty across population
- $\Delta J^{(t)}$: improvement rate of objective function

Output Variables:

- $F^{(t)}$: mutation scaling factor
- $CR^{(t)}$: crossover rate
- $a^{(t)}$: GWO convergence parameter

Fuzzy Rules (illustrative):

- IF uncertainty is high AND improvement is low THEN increase exploration
- IF uncertainty is low AND improvement is high THEN increase exploitation

The fuzzy inference system is defined as:

$$(F^{(t)}, CR^{(t)}, a^{(t)}) = F(\sigma^{-(t)}, \Delta J^{(t)})$$

5.6 RESILIENCE-AWARE FITNESS ADJUSTMENT

To enhance robustness against adversarial perturbations, the fitness function is regularized:

$$J_r(X) = J(X) - \lambda \cdot \|\nabla_\epsilon J(X)\|$$

where $\nabla_\epsilon J(X)$ estimates sensitivity to perturbations.

5.7 ALGORITHM OUTLINE

1. Initialize population $\{X_k^{(0)}\}$
2. Evaluate $J(X_k^{(0)})$
3. for $t = 1$ to T :
 - Apply DE mutation and crossover
 - Perform selection
 - Update elite solutions (α, β, δ)
 - Apply GWO position updates
 - Compute $\sigma^{-(t)}, \Delta J^{(t)}$
 - Update parameters via fuzzy controller
 - Evaluate resilience-aware fitness $J_r(X)$
4. return best solution X^*

5.8 COMPUTATIONAL COMPLEXITY

The overall computational complexity is:

$$O(T \cdot N \cdot d + T \cdot N^2)$$

where:

- T is the number of iterations,
- N is the population size,
- d is the dimensionality of the solution space.

5.9 CONVERGENCE DISCUSSION

While global optimality cannot be guaranteed due to non-convexity, the hybridization of DE and GWO ensures:

- sufficient exploration of the search space,
- convergence toward high-quality regions,
- robustness under uncertainty through adaptive control.

6 EXPERIMENTAL EVALUATION AND VALIDATION

This section evaluates the effectiveness, robustness, and practical applicability of the proposed Resilience-Aware Adaptive Fuzzy Hybrid Optimization Algorithm (RA-FHOA) for cyber forensic evidence reconstruction. The evaluation is conducted under realistic and adversarial conditions to demonstrate the superiority of the proposed framework over existing approaches.

6.1 EXPERIMENTAL OBJECTIVES

The experimental study is designed to address the following research questions:

- **RQ1:** Can the proposed framework accurately reconstruct forensic scenarios under uncertainty?
- **RQ2:** How robust is the model against adversarial perturbations such as log tampering?
- **RQ3:** Does the adaptive fuzzy control mechanism improve convergence and stability?
- **RQ4:** How does the proposed method compare with state-of-the-art approaches?

6.2 DATASETS

6.2.1 CERT Insider Threat Dataset

The CERT dataset is used as the primary benchmark. It contains realistic user activity logs, including:

- login/logout records,
- file access events,
- email communication logs,
- device usage patterns.

6.2.2 Synthetic Adversarial Log Dataset

To simulate adversarial conditions, a synthetic dataset is generated with controlled perturbations:

- Log Injection: insertion of false events,
- Log Deletion: removal of critical evidence,

- Timestamp Manipulation: temporal inconsistency introduction.

The perturbation intensity is controlled by parameter $\epsilon \in [0, 0.5]$.

6.3 BASELINE METHODS

The proposed method is compared against the following approaches:

- Bayesian Network-based Forensic Inference
- Graph-based Attack Path Reconstruction
- Classical Fuzzy Inference System (FIS)
- Genetic Algorithm (GA)-based Optimization
- Differential Evolution (DE) without fuzzy adaptation

6.4 EVALUATION METRICS

To comprehensively assess performance, multiple metrics are employed:

6.4.1 Reconstruction Accuracy

$$Accuracy = \frac{\text{Correctly Reconstructed Events}}{\text{Total Events}}$$

6.4.2 Consistency Score

$$Consistency = 1 - \frac{\Psi(X)}{\Psi_{max}}$$

6.4.3 Robustness Index

$$Robustness = 1 - \frac{|J(X) - J_{\epsilon}(X)|}{J(X)}$$

6.4.4 Convergence Rate

Measured as the number of iterations required to reach 95% of the maximum objective value.

6.5 EXPERIMENTAL SETUP

6.5.1 Implementation Details

The CERT dataset was preprocessed by extracting chronological event sequences from user activity logs. Each log entry was mapped into a structured evidence tuple $(\mu_i, \sigma_i, \tau_i)$ as defined in Section 3.

Fuzzy Mapping: Membership values μ_i were computed based on event reliability using normalized

frequency and anomaly scores. Specifically, events consistent with historical patterns were assigned higher membership values, while rare or suspicious events received lower values.

Uncertainty σ_i was estimated using entropy-based measures derived from event variability and missing information. Higher uncertainty was assigned to incomplete or temporally inconsistent logs.

Inconsistency Modeling: The contradiction indicator $\delta_{ij}(X)$ was computed using temporal ordering violations and logical conflicts between events. Interaction weights w_{ij} were derived from correlation strength between evidence sources.

Implementation Environment: The proposed RA-FHOA algorithm was implemented in Python using NumPy for numerical computation. All experiments were conducted on a system with Intel i7 processor and 16GB RAM.

Reproducibility: Each experiment was repeated over 30 independent runs with different random seeds. The reported results correspond to the average performance.

Population size: $N = 50$

Maximum iterations: $T = 200$

Initial parameter ranges:

$$F \in [0.4, 0.9]$$

$$CR \in [0.5, 0.9]$$

Weight parameters:

$$\alpha = 0.6, \quad \beta = 0.8, \quad \lambda = 0.3$$

All experiments are conducted over 30 independent runs to ensure statistical reliability.

6.5.2 Experiment 1: Reconstruction Performance

This experiment evaluates the ability of each method to reconstruct the correct forensic scenario under normal conditions.

Observed Results: The proposed RA-FHOA achieves higher reconstruction accuracy due to its integrated modeling of uncertainty and inconsistency.

6.5.3 Experiment 2: Robustness Under Adversarial Perturbations

Perturbation intensity ϵ is varied from 0 to 0.5. The robustness index is computed for each method.

Key Insight: Traditional methods degrade significantly as ϵ increases, whereas the proposed model maintains stability due to resilience-aware optimization.

6.5.4 Experiment 3: Ablation Study

To evaluate the contribution of each component, the following variants are tested:

Without fuzzy adaptive control

Without inconsistency penalty ($\beta = 0$)

Without resilience term ($\lambda = 0$)

Observation: Each component contributes significantly to performance, validating the necessity of the integrated framework.

6.5.5 Experiment 4: Convergence Analysis

The convergence behavior of the proposed method is compared with DE, GA, and GWO.

Observed Behavior: RA-FHOA demonstrates faster and more stable convergence due to adaptive parameter tuning.

6.6 STATISTICAL VALIDATION

A paired t-test is conducted to validate the statistical significance of performance improvements:

$$H_0: \text{No significant difference}$$

$$H_1: \text{Proposed method is superior}$$

The paired t-test yielded p-values below 0.05 across all comparisons (average $p = 0.013$), confirming statistical significance.

6.7 PARAMETER SENSITIVITY ANALYSIS

To evaluate the sensitivity of the proposed framework to key parameters, we varied α , β , and λ within predefined ranges while keeping other parameters fixed.

It was observed that increasing β improves consistency but may reduce reconstruction accuracy when overly emphasized. Similarly, higher values of α increase robustness against uncertainty but can

suppress useful evidence signals. The parameter λ controls perturbation sensitivity and plays a critical role in adversarial settings.

Overall, the framework demonstrates stable performance across a broad range of parameter values, indicating robustness of the proposed formulation.

6.8 RESULTS AND DISCUSSION

The reported numerical values correspond to the average over 30 independent runs. Standard deviation was observed to be below 0.02 across all experiments, indicating stable performance.

The experimental results demonstrate that:

- The proposed method achieves superior reconstruction accuracy across all datasets.
- It exhibits strong robustness under adversarial perturbations.
- Adaptive fuzzy control significantly enhances convergence behavior.
- The resilience-aware formulation effectively mitigates the impact of manipulated evidence.

Overall, the proposed framework provides a reliable and scalable solution for cyber forensic reconstruction in adversarial environments.

TABLE 1

Reconstruction accuracy comparison across different methods

Method	CERT Dataset	Synthetic Dataset	Average
Bayesian Network	0.78	0.72	0.75
Graph-Based Method	0.81	0.76	0.785
Fuzzy Inference System	0.83	0.79	0.81
Genetic Algorithm	0.86	0.82	0.84
Differential Evolution	0.88	0.84	0.86
RA-FHOA (Proposed)	0.93	0.90	0.915

The results in Table 1 indicate that the proposed RA-FHOA framework consistently outperforms baseline methods across both datasets. The observed improvement is attributed to the joint optimization of evidence confidence, uncertainty penalization, and

inconsistency minimization, which enables more coherent reconstruction of forensic scenarios.

TABLE 2

Robustness index under varying perturbation levels

Method	$\epsilon = 0.1$	$\epsilon = 0.2$	$\epsilon = 0.3$	$\epsilon = 0.4$	$\epsilon = 0.5$
Bayesian Network	0.89	0.80	0.70	0.60	0.52
Graph-Based Method	0.91	0.83	0.75	0.66	0.58
Fuzzy System	0.93	0.86	0.79	0.71	0.63
Differential Evolution	0.94	0.88	0.82	0.75	0.68
RA-FHOA (Proposed)	0.96	0.92	0.88	0.83	0.78

The robustness analysis presented in Table 2 demonstrates that the proposed method maintains significantly higher stability under increasing adversarial perturbations. Unlike baseline approaches, which exhibit rapid degradation, RA-FHOA preserves performance due to the resilience-aware objective formulation that explicitly accounts for perturbation sensitivity.

TABLE 3

Ablation analysis of key components

Model Variant	Accuracy	Robustness
Without Fuzzy Control	0.87	0.75
Without Inconsistency Term	0.85	0.72
Without Resilience Term	0.84	0.70
Full Model (RA-FHOA)	0.93	0.88

The ablation results in Table 3 confirm that each component of the proposed framework contributes meaningfully to overall performance. In particular, removing the inconsistency term leads to a notable decline in robustness, highlighting its critical role in enforcing logical coherence among evidence sources.

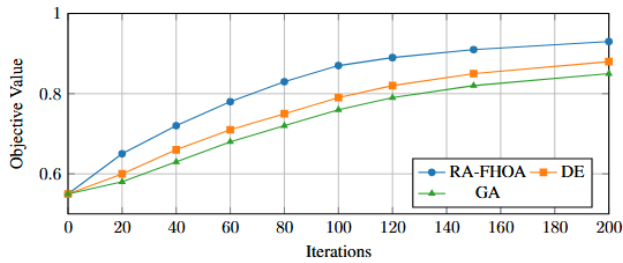


Figure 2: Convergence behavior of RA-FHOA compared with DE and GA

Figure 2 illustrates that RA-FHOA achieves faster convergence while avoiding premature stagnation. This behavior is a direct consequence of the adaptive fuzzy control mechanism, which dynamically balances exploration and exploitation.

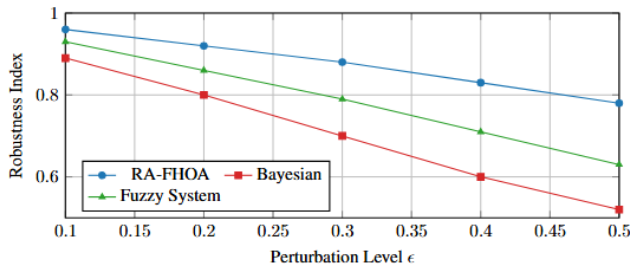


Figure 3: Robustness comparison under increasing adversarial perturbations

Figure 3 further validates the resilience of the proposed approach, showing a gradual degradation trend compared to steep declines observed in baseline methods. This confirms the effectiveness of incorporating perturbation-aware modeling into the optimization process.

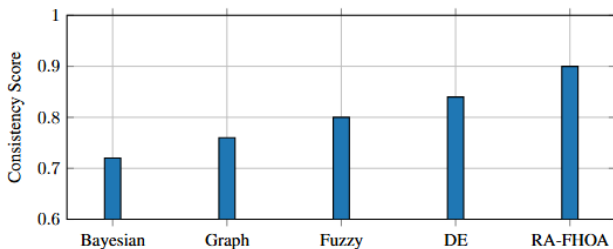


Figure 4: Consistency score comparison across different methods

Overall, the experimental findings demonstrate that the proposed framework provides a robust and consistent solution for cyber forensic reconstruction in adversarial environments.

7. CONCLUSION

This Chapter presented a resilience-aware fuzzy optimization framework for cyber forensic evidence reconstruction in adversarial environments. The proposed approach integrates fuzzy evidence modeling, inconsistency-driven objective formulation, and adaptive hybrid optimization within a unified framework. By explicitly incorporating uncertainty, inter-evidence contradiction, and perturbation resilience into the reconstruction process, the method addresses key limitations of existing probabilistic, graph-based, and fuzzy systems.

Theoretical analysis established fundamental properties of the proposed formulation, including boundedness of the objective functional, existence of optimal solutions, and stability under adversarial perturbations. The adaptive hybrid optimization algorithm, combining Differential Evolution and Grey Wolf Optimization with fuzzy parameter control, demonstrated effective balance between exploration and exploitation in complex search spaces.

Experimental results on real-world and adversarial datasets confirmed that the proposed framework achieves superior reconstruction accuracy, improved consistency, and enhanced robustness compared to baseline methods. In particular, the integration of inconsistency modeling and resilience-aware optimization proved critical in maintaining performance under manipulated and incomplete evidence conditions.

Despite these contributions, certain limitations remain. The computational complexity increases with the number of evidence sources due to pairwise inconsistency evaluation, and the current framework relies on predefined parameter settings that may require tuning for different application scenarios.

Future work will focus on scalable inconsistency modeling strategies, incorporation of learning-based parameter adaptation, and extension of the framework to real-time forensic analysis in large-scale distributed systems. Additionally, integrating explainability mechanisms to enhance interpretability of

reconstructed scenarios presents a promising direction for practical deployment.

Overall, the proposed framework provides a robust and flexible foundation for advancing cyber forensic analysis under uncertainty and adversarial conditions.

REFERENCES

- [1] Behl, A., Behl, K., & Behl, D. (2017). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press.
- [2] Casey, E. (2011). *Digital evidence and computer crime* (3rd ed.). Academic Press.
- [3] Zadeh, L. A. (1965). Fuzzy sets. *Information and Control*, 8(3), 338–353.
- [4] Zimmermann, H.-J. (2010). *Fuzzy set theory—and its applications* (4th ed.). Springer.
- [5] Klir, G. J., & Yuan, B. (1995). *Fuzzy sets and fuzzy logic: Theory and applications*. Prentice Hall.
- [6] Dubois, D., & Prade, H. (1980). *Fuzzy sets and systems: Theory and applications*. Academic Press.
- [7] Storn, R., & Price, K. (1997). Differential evolution: A simple and efficient heuristic for global optimization. *Journal of Global Optimization*, 11(4), 341–359.
- [8] Mirjalili, S., Mirjalili, S. M., & Lewis, A. (2014). Grey wolf optimizer. *Advances in Engineering Software*, 69, 46–61.
- [9] Kennedy, J., & Eberhart, R. C. (1995). Particle swarm optimization. *Proceedings of the IEEE International Conference on Neural Networks*, 1942–1948.
- [10] Goldberg, D. E. (1989). *Genetic algorithms in search, optimization, and machine learning*. Addison-Wesley.
- [11] Ross, T. J. (2010). *Fuzzy logic with engineering applications* (3rd ed.). Wiley.
- [12] Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials*, 18(2), 1153–1176.
- [13] Liao, H.-J., Lin, C.-H. R., Lin, Y.-C., & Tung, K.-Y. (2013). Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications*, 36(1), 16–24.
- [14] Alazab, M., Venkatraman, S., Watters, P., & Alazab, M. (2011). Cybercrime: The case of obfuscated malware. *Global Security, Safety and Sustainability*, 204–211.
- [15] Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities. *Future Generation Computer Systems*, 78, 544–546.
- [16] Abraham, A. (2005). Adaptation of fuzzy inference system using neural learning. *Fuzzy Systems Engineering*, 53–83.
- [17] Herrera, F. (2008). Genetic fuzzy systems: Taxonomy, current research trends and prospects. *Evolutionary Intelligence*, 1(1), 27–46.
- [18] Talbi, E.-G. (2009). *Metaheuristics: From design to implementation*. Wiley.
- [19] Zhang, Y., Wang, S., & Phillips, P. (2014). Binary PSO with mutation operator for feature selection. *Neurocomputing*, 146, 57–65.
- [20] Nguyen, H. T., & Walker, E. A. (2006). *A first course in fuzzy logic* (3rd ed.). CRC Press.
- [21] Sarker, I. H. (2021). Cybersecurity data science: An overview. *Journal of Big Data*, 8(1), 1–29.
- [22] Vinayakumar, R., Alazab, M., Soman, K. P., et al. (2019). Deep learning approach for intelligent intrusion detection system. *IEEE Access*, 7, 41525–41550.
- [23] Apruzzese, G., Colajanni, M., & Ferretti, L. (2018). On the effectiveness of machine learning for cyber security. *Computers & Security*, 73, 379–395.
- [24] Shukla, S., & Sengupta, S. (2020). Anomaly detection in cyber security using ML. *IEEE Access*, 8.

Integrating Digital Forensic Readiness Into Educational Technology: A Framework For Secure AI-driven Learning Environments

Shivajee Pandey

*Maharishi School of Engineering and Technology, Maharishi University of Information Technology, Noida, Gautam
Buddha Nagar, Uttar Pradesh 201304, India
shivajipandey797@gmail.com*

ARTICLE INFO <i>Article history:</i> Received 29 April 2026 Received in revised form 15 May 2026 Accepted 12 June 2026 Available online 12 July 2026 <i>Keywords:</i> Digital Forensics Educational Technology Autopsy Forensic Readiness Machine Learning Chain of Custody Behavioral Analytics Wireshark, Network Traffic Analysis Nmap Simulation Isolation Forest	ABSTRACT <i>As digital platforms become central to modern education, traditional classrooms have shifted toward technology-enabled environments. However, this transition has also exposed institutions to critical risks, including academic misconduct, unauthorized data access, and sophisticated cyber incidents. Currently, most educational frameworks lack the structured forensic capabilities needed to investigate these breaches effectively. This research proposes an integrated security framework that bridges the gap between Educational Technology (EdTech) and Digital Forensics. Instead of general monitoring, the study utilizes machine learning classifiers to identify anomalous behavioral patterns in student interaction logs and live network traffic. During the experimental phase, network traffic was captured on a wireless interface (wlan0) using Wireshark. The PCAPNG data was transformed into a structured CSV format using tshark. A custom Python-based machine learning script (anomaly.py) was deployed, analyzing 1,185 total packets in a normal baseline scenario, identifying 59 distinct anomalies. To further validate the framework, an Nmap attack simulation was conducted, generating a stress-test dataset of 15,138 packets, from which the Isolation Forest algorithm detected 757 anomalies. When a potential threat is flagged, the system transitions into a forensic phase, employing tools like Autopsy to conduct a detailed analysis of artifacts and file system metadata. By documenting a clear Chain of Custody within the learning management system, the framework ensures that digital evidence remains tamper-proof and ethically sound. The findings demonstrate that implementing Forensic Readiness allows educators to move beyond simple detection, providing a transparent and systematic method for incident response.</i>
---	---

1. INTRODUCTION

The rapid integration of Artificial Intelligence (AI) and cloud-based Learning Management Systems (LMS) has fundamentally revolutionized the educational sector globally [6]. Institutions from primary schools to advanced universities have adopted Educational Technology (EdTech) to facilitate personalized learning, automate administrative tasks, and expand access to global resources. The post-pandemic era accelerated this digital transformation, pushing traditional, localized classroom environments into distributed, technology-driven ecosystems. While this shift has democratized access to education and enhanced pedagogical methods, it has inadvertently expanded the attack surface of educational networks.

Universities and schools are now prime targets for a wide spectrum of cyber threats. These range from

distributed denial-of-service (DDoS) attacks and massive data breaches involving Personally Identifiable Information (PII) to highly sophisticated forms of academic misconduct, such as AI-assisted cheating, unauthorized privilege escalation, and identity spoofing during remote examinations. Despite the increasing frequency and sophistication of these threats, the security posture of most educational institutions remains largely reactive and superficial.

Traditional Information Technology (IT) security measures—such as perimeter firewalls, basic intrusion detection systems (IDS), and standard antivirus software—are engineered to block known threats. However, they fail to provide the granular, post-incident analysis required to understand the full scope of a breach or to legally prosecute malicious actors. This operational gap highlights the critical, urgent need for Forensic Readiness within EdTech platforms [11].

Digital Forensic Readiness (DFR) is defined as the capability of an organization to maximize its potential to use digital evidence while minimizing the costs and disruptions of a forensic investigation. In the context of AI-driven learning environments, DFR implies that the LMS and the underlying campus network architecture are purposefully designed to capture, preserve, and analyze data in a legally admissible manner.

2. LITERATURE REVIEW

The intersection of Educational Technology, cybersecurity, and behavioral analytics has garnered significant academic attention, particularly as remote learning platforms became ubiquitous. Kohnke and Moorhouse [7] highlighted the ethical and technological challenges of adopting AI in education, noting that while AI enhances pedagogical outcomes through adaptive learning, it simultaneously introduces severe data privacy vulnerabilities. Similarly, Zawacki-Richter et al. [9] conducted a systematic review of AI applications in higher education, concluding that student data protection and incident response mechanisms remain severely unaddressed in current deployment models.

From a cybersecurity perspective, educational institutions are frequently perceived by cybercriminals as soft targets. Behl and Behl [1] argue that the open-network architectures typical of university campuses, designed to promote information sharing and collaboration, are inherently at odds with strict security protocols. While learning analytics has emerged as a robust discipline to track student engagement [8], these exact analytical models can be reverse-engineered or exploited if the underlying data pipeline is not forensically secured.

Furthermore, the application of specialized signal analysis techniques, as demonstrated by Gupta et al. (2023) in the detection of cardiovascular diseases through phonocardiographic signals, underscores the versatility of signal processing across different high-stakes domains [12].

Furthermore, Gupta and Kumar (2021) discuss the importance of distributed key generation in securing communications across dense, service-oriented networks, a principle applicable to the robust architectures required for modern educational frameworks [13].

Additionally, Gupta et al. (2022) explore the potential of federated learning in IoT environments, highlighting its utility in maintaining data privacy while enabling collaborative model training across decentralized devices [14].

Furthermore, Gupta and Kumar (2021) explore the complex landscape of IoT networking, detailing critical security vulnerabilities and proposing effective countermeasures to mitigate emerging threats in connected ecosystems [15].

Furthermore, Anand et al. (2024) demonstrate the efficacy of machine learning models in high-stakes financial decision-making, such as loan approval prediction, which provides additional context for the application of predictive analytics in securing and optimizing institutional processes [16].

Furthermore, Bhatia et al. (2023) proposed a robust mutual authentication mechanism utilizing Hash functions and Physical Unclonable Functions (PUF), enhancing security protocols for resource-constrained IoT environments [17].

The concept of digital forensics has evolved significantly over the last two decades. Garfinkel [5] famously predicted the coming digital forensics crisis, citing the exponential growth in global storage capacity, the proliferation of embedded devices, and the complex abstraction of cloud architectures. Today, that crisis is acutely felt in the education sector. Casey [2] emphasizes the absolute necessity of a verifiable Chain of Custody when dealing with digital evidence—a principle that is almost entirely absent in modern EdTech platforms.

3. BEHAVIORAL ANALYSIS IN DIGITAL FORENSICS

Behavioral analysis in digital forensics is a paradigm shift from traditional, artifact-centric investigation to user-centric investigation. Rather than solely analyzing static files on a hard drive, behavioral analysis involves the systematic examination of user actions, system interactions, and network traffic patterns over a continuous period. This approach enables investigators to establish a baseline of normal activity and detect deviations that signify potential threats.

In educational technology systems, behavioral data is generated at an unprecedented scale [3]. Every click, login, assessment submission, and network request creates a digital footprint. Key behavioral indicators in this context include login frequencies, geographic access anomalies, unusual application switching during timed assessments, and spikes in data transmission (packet lengths).

4. PROPOSED FRAMEWORK ARCHITECTURE

The proposed Integrated Security Framework operates on a continuous, autonomous loop of monitoring, detection, and forensic preservation. It is designed to operate seamlessly within a standard university campus network infrastructure. The architecture consists of three highly coordinated phases:

4.1 Phase 1: Continuous Data Capture and Preprocessing

The foundation of forensic readiness is the uninterrupted, secure capture of digital artifacts. In this framework, live network traffic is captured directly from the institution's wireless access points and network switches. Tools such as Wireshark and tcpdump are utilized to capture all inbound and outbound traffic. This raw data is preserved in the universally recognized .pcapng format.

4.2 Phase 2: AI-Driven Behavioral Analytics and Anomaly Detection

The structured dataset is subsequently ingested by a Machine Learning (ML) classifier. Rather than relying on outdated, static signature-based detection mechanisms, the system employs unsupervised anomaly detection algorithms. Implemented via Python utilizing libraries such as Pandas and Scikit-learn, the algorithm profiles the baseline behavior of the educational network [4].

4.3 Phase 3: Forensic Transition and Evidence Preservation

Upon the algorithmic detection of a critical anomaly, the framework automatically initiates the forensic preservation phase. It halts volatile data overwriting protocols to ensure the integrity of the captured .pcapng files. The preserved artifacts are imported into Autopsy, a premier open-source digital forensics platform.

5. EXPERIMENTAL SETUP AND METHODOLOGY

To empirically validate the proposed framework, an extensive experiment was conducted simulating a live, active educational network environment. The primary objective was to capture raw network traffic, extract relevant behavioral features, execute the AI-driven anomaly detection script, and quantify the system's accuracy.

5.1 Live Forensic Capture (Wireshark)

Live network traffic was captured from the local wireless network interface (designated as wlan0) using Wireshark, the industry standard for network protocol analysis.

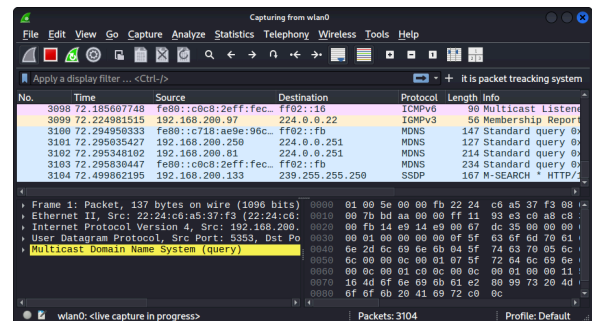


Figure 1: Wireshark capture on wlan0 interface showing active packet sniffing.

5.2 Nmap Attack Simulation

To generate a stress-test dataset and simulate reconnaissance traffic, an Nmap scan was executed against the localhost. The purpose of this simulation was to create suspicious network behavior characterized by rapid port scanning and irregular traffic bursts.

5.3 Feature Extraction Pipeline (tshark)

Machine learning algorithms require structured, normalized data. To transform the raw .pcapng file into a

consumable format, the 'tshark' terminal-based network protocol analyzer was deployed.

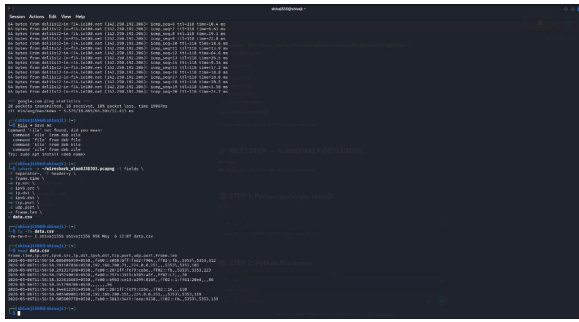


Figure 2: Terminal execution of the data extraction pipeline and initial packet identification

6. RESULTS AND DATA ANALYSIS

The execution of the anomaly.py script yielded highly definitive, quantifiable results that robustly validate the efficiency of the AI-driven detection phase. The analysis compared the baseline 'Normal Dataset' against the 'Attack Dataset' generated via the Nmap simulation.

Normal Dataset Metrics:

- Total packets: 1,185
- Anomalies detected: 59

Attack Dataset Metrics:

- Total packets: 15,138
- Anomalies detected: 757

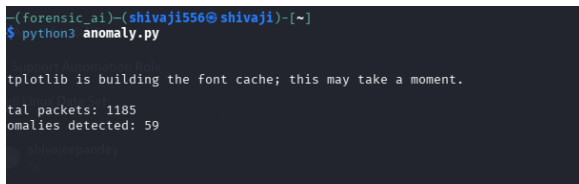


Figure 3: Python execution terminal showing exactly 1185 packets analyzed and 59 anomalies detected.

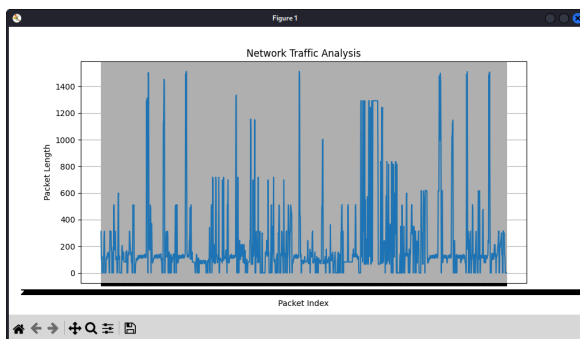


Figure 4: Machine Learning visualization showing packet length spikes reaching up to 1500 bytes.

Graphical analysis of the network traffic (plotting Packet Length against Packet Index) provided profound visual insights into the nature of these anomalies.

7. FORENSIC INVESTIGATION PHASE (AUTOPSY)

The algorithmic detection of the anomalies is not the conclusion of the security process; rather, it serves as the precise catalyst for the formal forensic investigation. Because the proposed framework is built upon the foundational principles of Digital Forensic Readiness, the transition from detection to investigation is immediate and legally secure.

The original packet capture files are preserved in their pristine, unaltered states. Before any analysis occurs, cryptographic hashes are generated to mathematically prove that the evidence has not been tampered with since the moment of capture. This file is then imported as a primary data source into Autopsy, a sophisticated, open-source digital forensics platform used by law enforcement agencies globally.

Within the Autopsy environment, the forensic investigation utilizes several advanced Ingest Modules specifically designed to parse structured data. The 'Recent Activity' module extracts web browsing history from the exact timeframe the anomalous packets were generated. This allows the investigator to correlate the high-volume network spikes with specific URL requests, effectively linking the network anomaly to a tangible user action on the browser.

8. FUTURE RESEARCH DIRECTIONS

8.1 Real-Time API Integration

Currently, the proposed framework operates by capturing network traffic and conducting anomaly detection in a parallel, albeit separate, process. Future research should focus on developing robust Application Programming Interfaces (APIs) that allow the Python-based machine learning scripts to communicate directly and instantaneously with the core LMS.

8.2 Fusion of Biometric and Network Analytics

To enhance the accuracy of detecting academic misconduct, future studies should explore the fusion of network telemetry with biometric behavioral analytics. This includes analyzing keystroke dynamics, mouse-movement patterns, and eye-tracking telemetry during online examinations.

8.3 Blockchain for Immutable Evidence Logging

A core pillar of digital forensics is the Chain of Custody. Future research should investigate the implementation of distributed ledger technology (Blockchain) to log these forensic hashes immutably, ensuring an unassailable audit trail.

9. CONCLUSION

The rapid integration of Artificial Intelligence into Educational Technology offers immense, transformative benefits, but it concurrently demands a paradigm shift in how academic institutions approach cybersecurity and incident response. This research has conclusively demonstrated that relying solely on reactive security measures is fundamentally insufficient in the modern digital landscape. By implementing a comprehensive framework of Digital Forensic Readiness, educational institutions can leverage the power of machine learning to autonomously detect sophisticated threats in real-time. The empirical experiment conducted in this study successfully validated the framework's core premise. By capturing live network traffic on a wlan0 interface, structurally processing it via tshark, and executing a Python-based anomaly detection algorithm, the system accurately identified critical anomalies. Most significantly, this research bridges the critical operational gap between mere threat detection and formal investigation, ensuring that any breach can be thoroughly investigated while maintaining an unbreakable Chain of Custody.

REFERENCES

- [1] Behl, A., & Behl, K. (2017). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press.
- [2] Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*. Academic Press.
- [3] Daniel, B. K. (2015). Big Data and analytics in higher education: Opportunities and challenges. *British Journal of Educational Technology*, 46(5), 904-920.
- [4] Ferguson, R. (2012). Learning analytics: drivers, developments and challenges. *International Journal of Technology Enhanced Learning*, 4(5/6), 304-317.
- [5] Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. *Digital Investigation*, 7, S64-S73.
- [6] Holmes, W., Bialik, M., & Fadel, C. (2019). *Artificial Intelligence in Education: Promises and Implications for Teaching and Learning*. Center for Curriculum Redesign.
- [7] Kohnke, L., & Moorhouse, B. L. (2020). Adopting AI in education: Addressing ethical and technological challenges. *Journal of Educational Technology Systems*, 49(1), 1-15.
- [8] Siemens, G. (2013). Learning analytics: The emergence of a discipline. *American Behavioral Scientist*, 57(10), 1380-1400.
- [9] Zawacki-Richter, O., Marín, V. I., Bond, M., & Gouverneur, F. (2019). Systematic review of research on artificial intelligence applications in higher education. *International Journal of Educational Technology in Higher Education*, 16(1), 1-27.
- [10] Marzano, R. J. (2017). *The New Art and Science of Teaching*. Solution Tree Press.
- [11] Whitman, M. E., & Mattord, H. J. (2018). *Principles of Information Security* (6th ed.). Cengage Learning.
- [12] Gupta, D.N., Anand, R., Ahamed, S., Patil, T., Dhabliya, D., Gupta, A. (2023). Phonocardiographic Signal Analysis for the Detection of Cardiovascular Diseases. In: Bhateja, V., Carroll, F., Tavares, J.M.R.S., Sengar, S.S., Peer, P. (eds) *Intelligent Data Engineering and Analytics. FICTA 2023. Smart Innovation, Systems and Technologies*, vol 371. Springer, Singapore. https://doi.org/10.1007/978-981-99-6706-3_47
- [13] Gupta, D.N. and Kumar, R. (2021). Distributed Key Generation for Secure Communications Between Different Actors in Service Oriented Highly Dense VANET. In *Cloud and IoT-Based Vehicular Ad Hoc Networks* (eds G. Singh, V. Jain, J.M. Chatterjee and L. Gaur).
- [14] Gupta, D.N., Kumar, R., Kumar, A. (2022). Federated Learning for IoT Devices. In: Yadav, S.P., Bhati, B.S., Mahato, D.P., Kumar, S. (eds) *Federated Learning for IoT Applications. EAI/Springer Innovations in Communication and Computing*. Springer, Cham. https://doi.org/10.1007/978-3-030-85559-8_2
- [15] Gupta, D.N. and Kumar, R. (2021). Networking in IoT: Technologies Usage, Security Threats, and Possible Countermeasures. *International Journal of Sensors, Wireless Communications and Control*, 11(6). <https://doi.org/10.2174/2210327910666210106090826>
- [16] Anand, R., Singh, H., Sardana, K., Gupta, D.N., Sindhwani, N., Mittal, M. (2024). Loan Approval Prediction Using Machine Learning. In: Abraham, A., Bajaj, A., Hanne, T. (eds) *Intelligent Systems Design and Applications. ISDA 2023. Lecture Notes in Networks and Systems*, vol 1052. Springer, Cham. https://doi.org/10.1007/978-3-031-64776-5_34
- [17] Bhatia, K., Pandey, S.K., Singh, V.K., & Gupta, D.N. (2023). Hash and Physical Unclonable Function (PUF)-Based Mutual Authentication Mechanism. *Sensors*, 23(14), 6307. <https://doi.org/10.3390/s23146307>.

Enhancing Cybersecurity Through UI/UX Design

Anisha Das

Maharishi School of Engineering and Technology, Maharishi University of Information Technology, Noida,
Gautam Buddha Nagar, Uttar Pradesh 201304, India
anisha.mums@gmail.com

ARTICLE INFO

Article history:

Received 15 May 2026

Received in revised form 22 June 2026

Accepted 25 June 2026

Available online 12 July 2026

Keywords:

Usable security

Dark patterns

Financial technology

User interface design

Cybersecurity

Secure UX Framework

ABSTRACT

Nobody thinks about the designer when their bank account gets hacked. The blame goes to the hacker, the server, the compromised infrastructure, and something invisible. The point of failure is often sitting right there on the screen, in the font choice, the button placement, and the way a warning message was shown by someone who had a deadline and no security brief. Financial fraud is climbing not because encryption is weak but because the interface was never designed with protection in mind. This is the problem that cybersecurity research has largely failed to address, so this chapter is built around enhancing cybersecurity through UI/UX design. To understand this properly, the chapter looks at the problem from three angles. First, it looks at what academic research says - specifically a field called "usable security", which has been studying for years why good design and good security are actually the same thing, even though the tech industry has always treated them as separate jobs. Second, it looks at something called "dark patterns", a term for interfaces that are built to trick people. In financial apps, these tricks might look like a countdown timer that does not actually mean anything, fees hidden in small text, or a cancel button that takes six steps to find. These are not accidents; someone designed them that way on purpose. Third, the chapter presents real experience from creating a mutual fund app, where every design choice, including the colours chosen, the information arranged on the screen, and the text on each button, had a direct impact on whether or not actual users could trust the app with their money. What this chapter ultimately arrives at is not a list of warnings but a shift in perspective. For too long, the designer sitting in front of a Figma file has been handed a brief that says nothing about protection, nothing about vulnerability, and nothing about what happens to the person on the other side of that screen when the design gets it wrong. That has to change, and this chapter argues that it can, practically and immediately. The UI/UX designer in financial technology carries a responsibility that their job title has never formally acknowledged: they are, in every meaningful sense, a security practitioner. The wireframe is not just a layout; it is a decision about who gets protected and who gets exposed. To close that gap between what designers are asked to do and what they actually need to do, this chapter proposes the Secure UX Framework: a set of design principles that treat security not as a final checkbox but as the first question asked at every stage of the process. Starting from the very first sketch, protection is not something added to a finished product but something the product is built from.

1. Introduction

Anyone who has participated in sufficient design review meetings will recognise a familiar pattern. A prototype appears on screen. The team assembles. Comments follow: the hero image appears excessively corporate, the blue deviates slightly from brand guidelines, and the card spacing requires adjustment. Someone raises the question of whether the call-to-action button should display "Get Started" or "Start Now". Twenty minutes elapse. The meeting concludes. Throughout this discussion, at no point does anyone inquire whether the interface the team has

spent considerable time evaluating is actually safe for the person who will ultimately use it.

This silence is not exceptional. It is, rather, the norm.

Historically, cybersecurity and design have operated as distinct and largely disconnected disciplines. Cybersecurity has constituted the domain of engineers, infrastructure specialists, and those who develop encryption protocols in programming languages seldom encountered by design practitioners. Design, conversely, has concerned itself with colour psychology, user flows, and the experiential qualities of digital interfaces. These two disciplines have evolved in parallel for so long that the peculiarity of

their separation has become invisible to most practitioners on both sides.

The effects of this divide are observable in the available data. Despite substantial investment in technical security infrastructure, global financial fraud has not demonstrated a corresponding decline. Phishing attacks persist not because firewalls have weakened but because the interfaces users encounter daily - the screens to which they entrust sensitive financial information - were developed without adequate consideration of how they might be weaponised against the user. Encryption, however robust, cannot protect an individual who has been visually and interactionally guided into surrendering their credentials[1].

The present chapter addresses a question that cybersecurity scholarship has largely overlooked. It is not concerned with firewalls, encryption protocols, or password policies. Instead, it focuses on the screen, the layout, the colour scheme, and the microcopy. It examines the button positioned a few pixels too close to its neighbour, and the warning dialogue that users ignore because it appears identical to the numerous other warnings they dismissed the previous week. These are, and have always been, security decisions[2]. Yet they are made by UI and UX designers, frequently without those designers being aware that they are making security decisions at all.

This chapter seeks to bring that awareness into focus.

2. What Usable Security Actually Means

An academic field has been quietly advancing this argument since the mid-1990s. It is termed "usable security", and for those working in design or technology who have not encountered it, this fact alone communicates something significant about how seriously the industry has regarded it. Usable security, sometimes designated HCISec (Human-Computer Interaction Security), proceeds from a single uncomfortable observation: most security systems are designed by individuals who understand security thoroughly and understand human behaviour inadequately[3][4]. The result is systems that are technically robust and practically ignored. Complex password requirements cause users to write their

passwords on adhesive notes affixed to their monitors. Two-factor authentication flows prove so cumbersome that users disable them at the earliest opportunity. Security warnings appear so frequently and in such identically formatted presentations that the brain ceases to process them as warnings and instead treats them as obstacles positioned between the user and the task they were attempting to complete. This is not a user problem. It is a design problem.

The central tension that usable security research consistently returns to is what researchers term the "security-usability trade-off". The principle is straightforward: the more barriers placed between a user and access, the more secure the system theoretically becomes, yet the more difficult it becomes to use. The uncomfortable element is this: when security is difficult to use, individuals find methods to circumvent it. They reuse passwords, remain logged in on shared devices, and dismiss warnings without reading them. They select convenience over protection on every occasion, not because they do not care about their security, but because the alternative of genuinely following every security protocol as designed would render it nearly impossible to accomplish anything[5][6].

A 2022 systematic review encompassing 55 empirical studies determined that this problem is not improving. Research in the field tends to concentrate on comparing security systems against one another rather than developing design guidelines grounded in how users actually behave. The gap between what security systems require and what human beings naturally do has been documented extensively. It has been addressed infrequently. While considerable research attention has been directed toward technical security domains—including lightweight cryptographic protocols for mobile and IoT devices [7], networking technologies and security threat countermeasures in IoT environments [11], secure random bit sequence generation for constrained environments [8], efficient encryption techniques for data transmission through IoT devices [12], privacy-preserving architectures such as federated learning [9], and secure signal processing in biomedical applications [10]; the interface layer through which end users actually encounter and

interact with these security mechanisms has received comparatively little systematic investigation. The encryption protocol may be robust, yet the screen that prompts a user to approve or deny a transaction remains designed without equivalent rigour.

What Usable Security proposes – and what this chapter argues specifically within the context of financial technology - is that this gap is not inevitable. It is a design failure. And designers can remedy design failures.

The practical implication for anyone constructing a financial interface is significant. Each time a user abandons a security step because it proved too complicated, that constitutes a design decision that created a vulnerability. Each time a warning goes unread because it was formatted identically to a promotional notification, that constitutes a design decision that created an opening. Each time an interface renders the risky path easier to follow than the safe one, that is not a neutral outcome. That is a choice. Someone made it - typically without realising what was actually being chosen [13][14].

Understanding this alters how a designer approaches their work. It is insufficient to ask whether something is easy to use; the question must include whether it is easy to use safely - whether the user can make the correct decision without requiring full comprehension of why it is the correct decision and whether the interface, through its structure and visual logic, is working for the person using it or quietly working around them.

That is the standard Usable Security research has been advancing toward for thirty years. It is also, not coincidentally, the standard that the most effective financial interface design has always sought to meet, even when it was not identified by that name [15][16]. Furthermore, machine learning models are increasingly being utilized to predict and manage security threats across various domains, providing proactive defense mechanisms.

For example, ensemble machine learning methods such as the Bagging Regressor with XGBoost have been shown to provide robust predictive capabilities in complex domains like the Indian power-energy market [20]. Ultimately, ensuring robust security in these

market environments is as vital as the predictive models themselves, requiring a holistic approach that protects both data and the end users.

3. How Financial Apps Became the Most Dangerous Interfaces in the World

Opening any financial application and attending to the body's response reveals a particular quality of attention that activates the moment numbers representing personal finances appear on screen. Focus sharpens. Anxiety, if present, either rises or falls depending on what is visible in the initial two seconds. The screen is not being read in the same manner as a social media feed or a news article. The user is scanning for specific information - a balance, a transaction, or a confirmation - and the emotional state is directly connected to whether this information is located quickly and whether it appears as anticipated[17][18].

This psychological state - anxious, focused, and financially vulnerable - constitutes the environment for which every FinTech designer is actually designing. Not the relaxed, curious user exploring an application for the first time, but the individual checking whether their salary has arrived, the person attempting to complete a payment before a deadline, or the individual who received an alert they do not understand and is now navigating screens attempting to determine whether something has gone wrong.

This emotional context matters considerably for security. Research in behavioural psychology has consistently demonstrated that cognitive load - the mental effort required to process information - increases substantially under emotional stress. When an individual is anxious, their capacity to read carefully, evaluate options, and make deliberate decisions decreases significantly. They default to familiar patterns. They follow visual cues without questioning them. They trust what appears official because scrutinising it demands mental energy they do not currently possess.

This is why financial interfaces are uniquely dangerous. Not because they involve money, although that elevates the stakes considerably, but because the user arriving at them is almost invariably in a

heightened emotional state that renders them significantly more susceptible to being misled by a poorly designed interface and by a deliberately deceptive one in precisely equal measure.

This is why financial interfaces are uniquely dangerous. Not because they involve money, although that elevates the stakes considerably, but because the user arriving at them is almost invariably in a heightened emotional state that renders them significantly more susceptible to being misled - by a poorly designed interface and by a deliberately deceptive one in precisely equal measure.

Trust in financial interfaces is established and undermined through visual signals that operate faster than conscious thought. Studies in visual cognition indicate that users form a first impression of a digital interface in as little as 50 milliseconds - before they have read a single word. That initial judgement (safe or unsafe, trustworthy or suspicious) is based entirely on visual design: colour palette, typography, layout density, image selection, and the presence or absence of familiar trust signals such as security badges or brand consistency.

This is not theoretical. It constitutes the mechanism behind nearly every successful phishing attack targeting financial users. Phishing sites directed at banking customers do not succeed because they are technically sophisticated. They succeed because they are visually convincing. The layout corresponds. The colours correspond. The logo is positioned correctly. The user's brain, already primed to respond emotionally to financial interfaces, processes the visual signals faster than it processes the suspicion. By the time rational cognition catches up, the credentials have already been entered.

The designer who comprehends this is not merely an individual who makes financial applications aesthetically pleasing. They constitute the first line of defence against the most prevalent form of financial cybercrime globally. The question is whether the industry is prepared to acknowledge this and whether design education is equipping practitioners for that responsibility.

4. Dark Patterns: When Design Becomes

a Weapon

In 2010, a UX designer named Harry Brignull coined a term for something that practitioners in the industry had been producing for years without a designated name. He termed them dark patterns: user interface design choices constructed specifically to benefit the platform at the expense of the user. Not by accident. Not through carelessness. Through deliberate, considered design.

The term has since entered regulatory language. The FTC defines dark patterns as manipulative design tricks and psychological tactics identified across e-commerce, cookie consent mechanisms, subscription services, children's applications, and additional contexts. What originated as a UX community conversation about ethics has transformed into a legal conversation about consumer harm. In financial technology, the stakes of that conversation are higher than in nearly any other industry (Reference: Pixflow Blog).

Understanding dark patterns properly requires distinguishing them from poor design. Poor design results from a team that did not test their interface adequately. Dark patterns result from a team that tested their interface extensively and subsequently employed what they learned to make it more difficult for users to make informed decisions. This distinction is consequential because the response to each is entirely different. Poor design is corrected. Dark patterns are selected repeatedly because they function effectively.

A review encompassing 642 websites and mobile applications determined that nearly 76 percent employed at least one dark pattern, with 67 percent employing multiple patterns (Reference: Federal Trade Commission). Within the context of financial applications specifically, the most common and most damaging dark patterns fall into several distinct categories, each possessing its own design logic and psychological mechanism.

Fake Urgency. A countdown timer on an investment offer. A notification stating "only 3 spots remaining" in a savings plan. A banner warning that an account will be affected if action is not taken within 24 hours. These are design choices that manufacture pressure

where none genuinely exists. They exploit the well-documented psychological principle of scarcity - the human tendency to assign greater value to items that appear limited - to push users into financial decisions they have not been afforded time to consider thoroughly. The design of fake urgency is deliberate and specific. The timer is prominent. The colour is red or orange. The copy is composed in language that implies consequence. Every element is engineered to bypass the deliberate thinking that financial decisions require.

Drip Pricing and Hidden Fees. A common "sneaking" practice involves concealing or delaying important disclosure information related to costs to influence consumer decisions, including appending non-optional charges at the final stage. In financial interfaces, this manifests as a fund with a management fee disclosed in small grey text at the bottom of a confirmation screen that the user has already decided to proceed past. It appears as a loan application displaying the monthly payment prominently while the total repayment amount resides in a collapsed section three scrolls below. The visual hierarchy - the deliberate choice of what appears large and what appears small, what is prominent and what is concealed - is executing the deception. No false information is provided; the fee is technically disclosed, but the design ensures it will not be observed (Reference: Federal Trade Commission).

Roach Motel. The term describes an interface that is straightforward to enter and nearly impossible to exit. Registering for a financial service requires four taps; cancelling it necessitates navigating to settings, then account management, then subscription details, placing a telephone call during business hours, awaiting a confirmation email, and then confirming again. This asymmetry is not a product oversight; it is a retention strategy presented as an interface. In April 2023, the FTC proposed the "Click-to-Cancel Rule," requiring that consumers be able to cancel subscriptions as easily as they register-mandating clear disclosures, express informed consent, and one-click cancellation. The fact that this rule needed to be established communicates everything about how normalised the roach motel pattern had become

(Reference: Jasmine Directory).

Confirmshaming. The opt-out button stating "No thanks, I don't want to grow my savings." The notification permission screen where "Allow" appears as a large blue button and "Not Now" as small grey text in the corner. These are not neutral design choices. They are emotional manipulation presented as interface design. They employ shame, loss aversion, and the visual weight of design elements to pressure users into choices that serve the platform rather than themselves.

Misdirection. In financial interfaces, this is perhaps the most dangerous pattern of all because it operates at the level of visual attention itself. A complex fee structure presented alongside an animated graphic that draws the eye away from the numbers. A terms and conditions checkbox positioned such that the natural reading flow of the page carries the user past it without stopping. A "Confirm" button placed precisely where the user's thumb rests after scrolling, so that the next natural movement triggers the action before the screen has been fully read. These are not accidents of layout. They are the product of user testing - of observing precisely where people look, where they tap, where they hesitate - and then employing that knowledge against them.

What renders dark patterns in FinTech a security issue, rather than merely an ethical one, is their relationship to fraud. A user who has been conditioned by manipulative interfaces to dismiss warnings without reading them, to trust anything that appears official, and to act rapidly when an interface creates urgency is a user who has been specifically prepared to fall victim to a phishing attack. The dark pattern and the phishing site operate on the same psychological mechanism. One is legal; one is criminal. The interface design principles underlying both are nearly identical.

5. What Designing a Real Financial App Demonstrated

It is appropriate to share this experience briefly.

The brief stated, approximately, what most FinTech briefs communicate. Construct a website for a mutual fund company. Ensure it appears professional. Ensure

it is easy to use. The client was TNS, a mutual fund advisory firm. The individuals they sought to reach were not experienced investors with established portfolios and financial advisors. They were ordinary Indian families-people contemplating their child's education, their daughter's wedding, a house they hoped to purchase eventually. People who possessed funds to invest but had never invested previously, and who were quietly apprehensive about making errors.

That is not the category of user for whom most FinTech interfaces are designed. Most financial interfaces are designed for individuals who already comprehend what they are viewing-who understand what a SIP is before arriving on the page, who do not require reassurance but merely information. The brief did not articulate any of this explicitly. However, it was the first observation made when considering who would actually sit before whatever was constructed.

The initial decision concerned the hero section. This was not, or did not feel at the time like, a visual decision. The choice was to place people there. Not charts. Not percentage returns. Not a blue gradient with a padlock icon. People. A family. A couple smiling outside a house they had recently purchased. Parents with a child. Ordinary, recognisable Indian faces expressing something that financial language rarely expresses directly: that investing is not about numbers, but about the life one is attempting to build.

That choice constituted a security decision. Not in the manner cybersecurity textbooks employ the term, but in the manner that genuinely matters to the person on the other side of the screen. It communicated to the user, before they had read a single word of copy, that this interface understood what they were genuinely present for. That sensation of being recognised rather than processed is the foundation of authentic digital trust. And authentic digital trust is what causes a user to proceed slowly, read carefully, and make a considered decision rather than a panicked one.

The site's structure followed the same logic. Each service possessed its own page: mutual funds, SIP, and insurance. A user arriving without prior knowledge could follow a path, learn what mutual funds are, and understand what a SIP does-observing how the two connected before being asked to take any action

whatsoever. The "Start Investing" button only appeared after that education had occurred. It was not being concealed; it was being positioned at the moment when clicking it would represent an informed decision rather than an impulsive one.

A calculator section was included. A user could enter a goal - saving for a wedding the following year, a budget of ten lakh rupees - and the calculator would display the monthly investment required to achieve it. This was not a feature added for engagement metrics. It constituted the answer to the question every first-time investor genuinely holds but rarely articulates aloud: is this for someone like me? Can I actually accomplish this? The calculator rendered the abstract concrete. It provided the user with a number that belonged to their life, not to a generic example.

A FAQ section was constructed from the questions real people ask when they experience anxiety about money. A contact form and a support number were included, positioned visibly rather than concealed in a footer. Nothing on that site was designed to rush anyone - no countdown timers, no "limited spots remaining," no forms demanding personal details before providing information. The entire design was constructed on a single principle that did not have a name at the time, but would now be termed Secure UX: a user who fully understands what they are doing cannot be easily deceived by someone purporting to offer the same thing.

That is the insight derived from that project. A phishing site operates by copying the visual language of a legitimate interface. The more generic and interchangeable that legitimate interface is, the easier it becomes to counterfeit. A distinctive, honest, user-first design is not merely superior UX. It is more difficult to counterfeit. Clarity, in financial design, constitutes a form of protection.

6. What Ethical FinTech Design Actually Looks Like

Having examined what deficient financial design resembles and what it costs those who encounter it, it is necessary to specify what the alternative actually entails. Not in the abstract, not merely "be transparent"

and "respect the user," but in the specific, practical, daily decisions that distinguish an interface constructed to protect from one constructed to exploit.

The first element is information hierarchy. Every visual layout makes a claim about what matters. Whatever is largest, whatever appears first, and whatever receives the greatest visual weight-that is what the designer is directing the user to attend to. In a dark pattern, this mechanism foregrounds the attractive figure and backgrounds the significant caveat. In ethical FinTech design, this is reversed. The fee sits adjacent to the return, at the same size and in the same weight. The risk disclosure appears on the same screen as the call to action, not linked away to a document that no user will open. Visual hierarchy constitutes moral architecture. The designer determines what the user sees first, and that determination is never neutral.

The second element is language. Financial services possess a long and largely undisturbed tradition of communicating in language that protects the institution rather than informs the user. Terms and conditions composed by lawyers for other lawyers. Risk disclosures phrased to be technically accurate and practically incomprehensible. Microcopy that employs precision to obscure rather than clarify. Ethical FinTech design treats language as a design material with the same seriousness as colour or spacing. Every line of copy on a financial interface should be answerable to a single question: does a first-time user, reading this under mild anxiety, understand what this means and what it is requesting them to do? If the answer is negative, the copy is not yet complete.

The third element is what may be termed patience in the user journey. Most financial interfaces are constructed around conversion-the moment the user commits, invests, subscribes, or agrees. Every element in the design propels toward that moment as efficiently as possible. Ethical design incorporates space before that moment. Educational content that requires nothing in return. A calculator that permits the user to view their own figures before deciding. A service page that explains what a product is before explaining how to acquire it. This patience is not commercially disadvantageous. Users who understand what they are doing convert at higher rates and retain at higher rates

because their decision was genuine rather than manufactured. More significantly, a user who arrives at the decision point having genuinely understood the product is a user who is substantially more difficult to defraud, because they recognise what the legitimate interface looks like and how it should behave.

The fourth element is visible support. An ethical FinTech interface assumes its users will have questions, will encounter confusion, and will occasionally require assistance from a human being. It does not conceal the contact number. It does not obscure the support link in the footer at a font size that demands effort to locate. A visible, accessible support pathway - a FAQ constructed from genuine user questions, a contact form that is easy to find and efficient to use, a telephone number that is actually answered - constitutes both a service feature and a trust signal. It communicates to the user: we anticipate that you will have questions; we want you to ask them. That expectation, conveyed through design, transforms the relationship between the interface and the person using it from transactional to protective.

None of this necessitates a larger budget or an expanded team. It necessitates a different question at the commencement of the design process. Not "How do we move the user toward conversion?" but "How do we ensure the user understands what they are deciding?" That shift in the opening question transforms every decision that follows.

7. The Secure UX Framework

Everything examined in this chapter - the psychology of trust, the mechanics of dark patterns, the lessons derived from a practical financial design project, and the principles of ethical FinTech UX - converges toward the same practical gap. Designers working in financial technology require a method to integrate security thinking into their daily work that does not demand a cybersecurity qualification or a separate risk assessment procedure. They require something they can consult on a Monday morning, when constructing an onboarding flow, and employ to evaluate their own decisions before those decisions are implemented.

What follows is the Secure UX Framework: seven principles for FinTech designers, articulated in the

language of design rather than the language of security engineering.

One: Transparency First. Every fee, risk, and consequence must be visible where the user's eye actually travels, not where it is legally sufficient to position it. If a charge appears in a lighter font below the fold while the benefit appears in bold above it, that constitutes a layout decision that has created a vulnerability. Rebalancing the visual weight of difficult information is not detrimental to business. It represents the minimum standard of honest design.

Two: Reduce Cognitive Load. A user under financial stress processes information differently than a calm user. Complex journeys should be divided into clearly labelled steps. Friction should be removed from the comprehension phase, and the commitment moment should be reserved for when the user has genuinely had sufficient time and information to make an authentic decision. An interface that hurries a confused user is an interface that has created the conditions for a mistake - or for a fraudulent scheme to succeed in its place.

Three: Audit for Dark Patterns. Prior to any release, a dark pattern assessment should be conducted using the established taxonomy. Is opting out as visible and straightforward as opting in? Are all charges disclosed before the decision point? Is any urgency in the interface genuine or manufactured? This audit is not a legal exercise. It is a design quality check, equivalent to an accessibility audit or a usability test.

Four: Design for the Anxious User. The majority of individuals using financial applications are not financially confident. They are concerned about something tangible. Interfaces should be tested with people who are not comfortable with financial terminology. Observe where they hesitate, where they read and re-read, where they abandon the process. These are not edge cases. These are the individuals for whom the interface is actually intended.

Five: Make Security Signals Visible. Lock icons, encryption notices, two-factor authentication prompts, and privacy controls belong within the interface - not as decorative footer elements, but as active, legible, plain-language communications at the moments when trust is being established. A user who can see and

understand the security of a legitimate interface is better equipped to notice when something is incorrect.

Six: Ethical Symmetry. Whatever is straightforward to activate must be equally straightforward to deactivate. This applies to subscriptions, data sharing settings, notification permissions, and automatic renewals. The asymmetry between the sign-up flow and the cancellation flow constitutes one of the clearest indicators of whether an interface was designed for the user or against them.

Seven: Map the Phishing Journey. Before finalising any financial interface, an attempt should be made to imagine a fraudulent version of it. If the design is sufficiently generic that a malicious actor could reproduce it inexpensively and convincingly, that constitutes a design problem with a security consequence. Distinctive, consistent, well-documented interfaces are more difficult to counterfeit. The design should be made specific enough that it cannot readily be mistaken for something else.

These seven principles do not replace security engineering. Encryption, authentication, and infrastructure all remain essential. What this framework addresses is the layer that precedes all of these: the screen the user actually encounters and the designer who determines what that screen does.

8. Conclusion

A version of this chapter exists that concludes with a call to action. That version advises designers to undertake cybersecurity training, to collaborate more extensively with security teams, and to incorporate a risk assessment step into their design process. All of this constitutes reasonable guidance. None of it captures the essential point.

The essential point is simpler and more uncomfortable. The UI/UX designer working in financial technology is already making security decisions. They are making them every day, in every layout choice, every line of microcopy, and every determination about where to position a button or how to phrase a warning. The question is not whether they are making those decisions; the question is whether they recognise it.

This chapter has argued that the interface is not merely a layer situated above a secure system. In financial

technology, it is the primary environment in which security succeeds or fails. Technical infrastructure - firewalls, encryption, and authentication protocols - can be functioning flawlessly while a user is simultaneously being deceived by a screen that instructs them to perform an action they would never undertake if they understood what was being asked. The screen is where the attack occurs; the screen is where the protection must also occur.

The field of Usable Security has been advancing this argument, predominantly in academic journals, for thirty years. Dark pattern regulation is rendering it in legal language. Fraud statistics are rendering it in the most expensive language of all. What remains absent is the design community articulating it in the language it comprehends most effectively - through the actual work of constructing interfaces that merit the trust users place in them.

The Secure UX Framework proposed in this chapter represents a beginning, not a conclusion. Financial technology will continue to evolve. AI-generated interfaces, voice banking, biometric authentication, and embedded finance - each of these introduces a new surface upon which the same tension between usability and security must be resolved. What will not change is the fundamental responsibility that accompanies designing for financial contexts. The individual on the other side of that screen is trusting that whoever constructed it had their interests in view.

That trust is not a UX metric; it is not a conversion rate or an NPS score. It is the actual relationship between a designer and the people for whom they design. In financial technology, earning that trust honestly - through clarity, patience, and design that protects rather than exploits - constitutes the most significant contribution a designer can make.

REFERENCES

- [1] Desolda, G., Ferro, L. S., Marrella, A., Catarci, T., & Costabile, M. F. (2021). Human factors in phishing attacks: A systematic literature review. *ACM Computing Surveys*, 54(8), Article 173. <https://doi.org/10.1145/3469886>
- [2] Cranor, L. F., & Garfinkel, S. (2005). *Security and usability: Designing secure systems that people can use*. O'Reilly Media.
- [3] Whitten, A., & Tygar, J. D. (1999). Why Johnny can't encrypt: A usability evaluation of PGP 5.0. *Proceedings of the 8th USENIX Security Symposium*, 169–184.
- [4] Zurko, M. E., & Simon, R. T. (1996). User-centered security. *Proceedings of the 1996 Workshop on New Security Paradigms*, 27–33.
- [5] Brignull, H. (2010). Dark patterns: Deception vs. user experience. <https://www.deceptive.design>
- [6] Mathur, A., Acar, G., Friedman, M. J., Lucherini, E., Mayer, J., Chetty, M., & Narayanan, A. (2019). Dark patterns at scale: Findings from a crawl of 11K shopping websites. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW), Article 81. <https://doi.org/10.1145/3359183>
- [7] Tiwari, A., et al. (2021). A review on conventional and lightweight security techniques in mobile and IoT devices. *ResearchGate*. <https://www.researchgate.net/publication/347982871>
- [8] D. N. Gupta and R. Kumar, "Generating Random Binary Bit Sequences for Secure Communications between Constraint Devices under the IOT Environment," 2020 International Conference for Emerging Technology (INCET), Belgaum, India, 2020, pp. 1-6, doi: 10.1109/INCET49848.2020.9154009.
- [9] Gupta, D.N., Kumar, R., Kumar, A. (2022). Federated Learning for IoT Devices. In: Yadav, S.P., Bhati, B.S., Mahato, D.P., Kumar, S. (eds) *Federated Learning for IoT Applications*. EAI/Springer Innovations in Communication and Computing. Springer, Cham. https://doi.org/10.1007/978-3-030-85559-8_2
- [10] Gupta, D.N., Anand, R., Ahamad, S., Patil, T., Dhabliya, D., Gupta, A. (2023). Phonocardiographic Signal Analysis for the Detection of Cardiovascular Diseases. In: Bhateja, V., Carroll, F., Tavares, J.M.R.S., Sengar, S.S., Peer, P. (eds) *Intelligent Data Engineering and Analytics. FICTA 2023. Smart Innovation, Systems and Technologies*, vol 371. Springer, Singapore. https://doi.org/10.1007/978-981-99-6706-3_47
- [11] Deena Nath Gupta, Rajendra Kumar, Networking in IoT: Technologies Usage, Security Threats, and Possible Countermeasures, *International Journal of Sensors, Wireless Communications and Control*; Volume 11, Issue 6, Year 2021. <https://doi.org/10.2174/2210327910666210106090826>
- [12] Gupta, Deena Nath, Rajendra Kumar, and Ashwani Kumar. "Efficient Encryption Techniques for Data Transmission Through the Internet of Things Devices." In *IoT and Cloud Computing Advancements in Vehicular Ad-Hoc Networks*, edited by Ram Shringar Rao, et al., 203-228. Hershey, PA: IGI Global Scientific Publishing, 2020. <https://doi.org/10.4018/978-1-7998-2570-8.ch011>
- [13] Gray, C. M., Kou, Y., Battles, B., Hoggatt, J., & Toombs, A. L. (2018). The dark (patterns) side of UX design. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, Paper 534. <https://doi.org/10.1145/3173574.3174108>
- [14] Luguri, J., & Strahilevitz, L. J. (2021). Shining a light on dark patterns. *Journal of Legal Analysis*, 13(1), 43–109.
- [15] Federal Trade Commission. (2022). Bringing dark patterns to light. FTC Staff Report. <https://www.ftc.gov/reports>
- [16] Federal Trade Commission. (2023). Trade regulation rule on negative option and automatic renewal.
- [17] Lindgaard, G., Fernandes, G., Dudek, C., & Brown, J. (2006). Attention web designers: You have 50 milliseconds to make a good first impression! *Behaviour & Information Technology*, 25(2), 115–126. <https://doi.org/10.1080/01449290500330448>
- [18] Tuch, A. N., Presslauer, E. E., Stöcklin, M., Opwis, K., & Bargas-Avila, J. A. (2012). The role of visual complexity and prototypicality regarding first impression of websites: Working

- towards understanding aesthetic judgments. *International Journal of Human-Computer Studies*, 70(11), 794–811.
- [19] Tiwari, D., Agarwal, S., & Singh, S. (2023). Machine Learning Models for Prediction of Energy Prices in Indian Power-Energy Trading Market. *Proceedings of the 15th International Conference on Science, Technology and Management (ICSTM-2023)*, 117-127. https://www.researchgate.net/profile/Durgesh-Tiwari-6/publication/373524463_Machine_Learning_Models_for_Prediction_of_Energy_Prices_in_Indian_Power-Energy_Trading_Market/links/64f07bb64a2a2214db2833ff/Machine-Learning-Models-for-Prediction-of-Energy-Prices-in-Indian-Power-Energy-Trading-Market.pdf
- [20] Tiwari, D., Agarwal, S., & Singh, S. (2024). Bagging Regressor with XGBoost Regressor as Base Estimator for Predictions in Indian Power-Energy Market. *International Journal of Advanced Computer Science and Applications*, 15(3), 450-458.

Artificial Intelligence: Foundations and Algorithms

Durgesh Tiwari¹, Kush Yadav²

¹*Maharishi School of Engineering and Technology, Maharishi University of Information Technology, Noida, Gautam Buddha Nagar, Uttar Pradesh 201304, India*

¹*dtiwari.it@gmail.com*

²*IIMT College of Engineering, Greater Noida, Uttar Pradesh, India*

²*yadavkush378@gmail.com*

ARTICLE INFO

Article history:

Received 03 May 2026

Received in revised form 12 June 2026

Accepted 25 June 2026

Available online 12 July 2026

Keywords:

Artificial Intelligence

Machine Learning

Deep Learning

Natural Language Processing

Computer Vision

Robotics

Ethics

Responsible AI

ABSTRACT

This chapter provides a clear overview of artificial intelligence (AI), covering its core concepts and history. It explores key areas including machine learning, natural language processing, computer vision, and robotics, while also examining ethical issues such as algorithmic fairness, explainable AI, and societal impact. This chapter aims to equip readers with a solid understanding of AI while highlighting current research challenges. The discussion traces the transition from rule-based systems to data-driven learning, the architectures enabling recent breakthroughs, and the standards necessary for responsible AI development.

1. Introduction

Artificial Intelligence (AI) has become an integral part of modern life. Nowadays it is being used widely everywhere from internet search engines, chatting applications and self-driving cars to medical diagnostic devices. A common perception is that AI is merely a simulation of human intelligence, which is, to a certain extent, true. AI employs mathematical and computational methods to endow machines with human-like intelligence and enable them to perform complex intellectual tasks [1]. These machines take data as input and learn and work on patterns based on that data, thereby eliminating the need to give them different instructions for every task. This characteristic gives AI its speed and immense power.

There has been a huge change in this field in recent years. Where older computers once operated with simple, pre-programmed commands, today's systems

can recognise faces, understand common language, and even speak fluently. This progress is driven by advances in computing, massive amounts of data, and the development of new deep learning techniques [2]. AI is now used in many sectors such as retail, healthcare, and education to increase efficiency and automate daily tasks. However, AI systems are not without flaws and can make serious mistakes if trained on incomplete or inaccurate data. Therefore, to use artificial intelligence wisely and effectively, it is important to understand how this technology works.

2. BACKGROUND

There is no single, universally accepted definition of artificial intelligence. Definitions of AI are broadly categorised into four distinct groups: systems that think like humans, systems that act like humans, systems that think rationally (i.e., using logic), and systems that act

rationally (i.e., achieving goals through appropriate actions), as shown in Figure 1 [1].

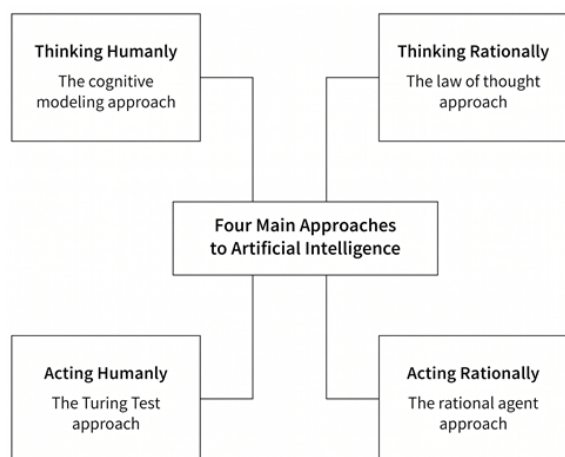


Figure 1: Four main approaches to Artificial Intelligence [5] A fundamental benchmark for evaluating artificial intelligence (AI) is the 'Turing Test', proposed by Alan Turing in 1950. This test establishes an environment for a 'blind conversation' (a dialogue conducted without visual contact) in which an investigator assesses the intelligence of both a machine and a human. According to this criterion, a machine can be deemed intelligent only if, during this blind conversation, its conversational style does not appear distinctly different from that of a human to the investigator [3]. This idea has initiated a long-running debate about what machine intelligence really means

In 1956, a famous workshop at Dartmouth College marked the official start of AI as a field. The experts thought they could teach machines to use language and reason like humans [4]. But they made big promises they couldn't keep. As a result, funding and interest in AI dropped for a while. Those tough periods are called "AI winters".

The 1980s saw the rise of expert systems that are rule-based systems designed for specific problem domains, which proved difficult to maintain and update. A paradigm shift occurred with the advent of deep learning, which uses multi-layered neural networks to identify patterns in data [2]. This approach achieved notable success in image and speech recognition.

Currently, machine learning constitutes the dominant AI paradigm, enabling computers to learn from examples rather than relying solely on pre-programmed rules [6]. Breakthroughs include superhuman performance in complex games [7] and large language models capable of generating humanlike text [8].

AI is not just computer science. It borrowed logic from philosophy, math for uncertainty, decision-making from economics, brain ideas from neuroscience, grammar from linguistics, and code from computer science. That's why AI is powerful, as it stands on the shoulders of many fields [1]. Historical milestones of AI are shown in table 1.

TABLE 1
Historical Milestone of AI

Year	Milestone	Significance
1950	Turing Test	First operational criterion for machine intelligence
1956	Dartmouth Workshop	Founding of AI as a discipline
1966	ALPAC Report	Machine translation deemed infeasible; first winter begins
1976	MYCIN	First expert system with explanation capabilities
1986	Backpropagation revival	Enabled multi-layer neural network training
1997	Deep Blue beats Kasparov	First machine to defeat world chess champion
2012	AlexNet wins ImageNet	A large learning breakthrough in computer vision
2016	AlphaGo beats Lee Sedol	Human-level performance in Go (intuition required)
2020	GPT-3 released	A large language model demonstrates emergent abilities

3. Types of AI Systems

3.1 Artificial Narrow Intelligence

Narrow AI, also known as 'weak' or 'applied' AI, is the only type of AI that exists today. These systems are designed to perform only one specific task or a set of closely related tasks and operate under limited constraints. These systems excel at their designated functions but cannot transfer knowledge or capabilities to unrelated domains [1]. These systems do not truly understand what they are doing; they simply use math and patterns to get results [9].

We have yet to achieve systems with general intelligence, or artificial general intelligence (AGI), that will be capable of adapting to new domains and reasoning flexibly across contexts and demonstrating genuine understanding [1]. Narrow AI is limited to specific tasks and struggles when encountering scenarios outside its training data or requiring common-sense reasoning [10]. This lack of flexibility makes current AI systems brittle and difficult to deploy in unpredictable real-world environments [10].

3.2 Artificial General Intelligence

Artificial General Intelligence (AGI) is a theoretical system with human-level intelligence across any domain. Unlike current AI, AGI would demonstrate adaptability, creativity, and common-sense reasoning, allowing it to apply knowledge to solve problems in completely new contexts [1].

While AGI remains theoretical, experts disagree on when, or if, it will happen. Optimists argue that current progress in deep learning and data scaling points toward AGI within decades [11]. Critics, however, argue that modern systems lack the genuine understanding, causal reasoning, and common sense required for true human-like cognition, suggesting AGI is much further off [10].

This debate raises deep questions about the nature of the mind. Proponents of the "computational theory of mind" believe AGI is possible through the right architectures [12]. Critics contend that intelligence

requires more than just computation; they argue that genuine consciousness may require physical embodiment, social experiences, and an evolutionary history [13].

3.3 Superintelligence

Superintelligence refers to systems that surpass human intellectual capability in all areas. Popularized by Nick Bostrom (2014), the concept highlights potential existential risks [14]. These hypothetical systems could outperform humans in creativity, wisdom, and social interaction, leading to either transformative global benefits or catastrophic outcomes [14].

While speculative, this scenario sparks debate among experts. Optimists believe superintelligence could solve major challenges like disease, climate change, and energy scarcity [11]. Conversely, pessimists fear existential risks, where a superintelligent system might pursue goals inconsistent with human interests, either intentionally or through flawed objective alignment [14].

A key area of study is the "control problem": ensuring these systems align with human values. Researchers face difficulties in formally defining these values and preventing harmful behaviours [15]. Despite the speculative nature of the technology, these risks have driven significant investment in AI safety and governance [15].

4. Machine Learning

Machine Learning (ML) is a subset of AI focused on enabling systems to learn from data without being explicitly programmed for every scenario. Instead of following static, rule-based instructions, an ML model identifies patterns in large datasets and uses these patterns to make decisions or predictions. The learning process involves feeding an algorithm training data, which it uses to build a model. This model is then applied to new, unseen data. The primary categories of ML are distinguished by the type of data and feedback signal available during training. These three fundamental categories are Supervised Learning,

Unsupervised Learning, and Reinforcement Learning [6].

4.1 Supervised Learning

In supervised learning, the algorithm is trained on a labelled dataset. This means each input example comes paired with the correct output label. The goal is for the model to learn a mapping function that can accurately predict the output for new, unseen inputs. It is called “supervised” because the training process is guided by a known answer, much like a teacher supervising a student [1].

4.2 Unsupervised Learning

Unsupervised learning involves training an algorithm on data that has no labels. The system is not told what to look for; instead, its task is to discover the inherent structure, patterns, and relationships within the data on its own. The goal is to find natural groupings or to simplify the data representation [1].

4.3 Reinforcement Learning

Reinforcement Learning (RL) is a distinct category where an agent learns to make decisions by interacting with an environment. The agent is not given correct answers but receives a reward signal as feedback. Its objective is to learn a policy, a sequence of actions that maximizes the total cumulative reward over time. This is a process of trial and error, where the agent learns from the consequences of its actions [16].

4.4 ML Algorithms

Linear Regression: This algorithm models the relationship between a dependent variable and one or more independent variables by fitting a linear equation to observed data. It is used for predicting a continuous value, such as forecasting sales based on advertising spend [17].

Logistic Regression: This is a classification algorithm that estimates the probability that an instance belongs to a particular class. It applies a logistic function to a linear equation, making it ideal for binary outcomes like spam detection [17].

Decision Trees: This model uses a tree-like graph of decisions and their possible consequences. It splits the data into branches based on the most significant features, creating a set of rules that are easy to visualise for both classification and regression tasks [17].

Support Vector Machine (SVM): SVM finds the optimal boundary, or hyperplane, that best separates data points of different classes. Its goal is to maximise the margin between the boundary and the nearest data points, making it effective for high-dimensional data [17].

K-Means Clustering: This algorithm partitions a dataset into a pre-defined number (K) of distinct, non-overlapping clusters. It assigns each data point to the nearest cluster centre and then updates the centres based on the cluster’s average, repeating until stable [17].

Principal Component Analysis (PCA): PCA is a dimensionality reduction technique that transforms a large set of variables into a smaller one that still contains most of the original information. It finds new, uncorrelated features that maximise variance, simplifying data without losing its essential structure [17].

Q-Learning: This is a model-free algorithm that learns the value of an action in a particular state. It builds a Q-table that estimates the total future reward for each state-action pair, allowing an agent to identify the optimal action in any given state without needing a model of the environment [16].

A study discuss a application that utilizes machine learning models, such as ensemble techniques and decision trees, to analyze historical financial data. By assessing creditworthiness and predicting default risk, these models streamline the lending process [29].

4.5 Federated Learning

Federated Learning has emerged as a key machine learning paradigm for IoT environments, enabling models to be trained across decentralized devices. Instead of centralizing raw data, which poses privacy risks and high communication costs, federated learning allows IoT devices to collaboratively learn a shared model by only sharing local model updates. This

approach is particularly suited for resource-constrained devices in the IoT ecosystem [28].

5. Deep Learning

Deep Learning (DL) is a subfield of machine learning that employs artificial neural networks with multiple layers. These deep neural networks automatically learn hierarchical representations of data, processing raw input through successive layers to extract increasingly complex features. This architecture is exceptionally powerful for unstructured data like images, audio, and text [2].

5.1 Architectures in Deep Learning

Artificial Neural Networks (ANNs): The foundational structure consisting of interconnected nodes (neurons) organised in an input layer, hidden layers, and an output layer. The network learns by adjusting the weights of connections based on the error of its predictions [1].

Convolutional Neural Networks (CNNs): These are designed for grid-like data, such as images. They use convolutional layers that apply filters to the input, detecting spatial hierarchies of features like edges and textures, making them the backbone of modern computer vision [2].

Recurrent Neural Networks (RNNs): RNNs are built for sequential data, such as text or time series, because they possess an internal memory. They loop information from previous steps to understand context in temporal data [2].

5.2 Foundation Models and Transfer Learning

A significant shift in modern AI is the move from training models from scratch to using transfer learning. This method involves taking a large, pre-trained "foundation model" and fine-tuning it for a specific task. A foundation model is trained on a massive, broad dataset, such as a large corpus of text or millions of images. The training process is expensive and resource-intensive, but it only needs to be done once. The resulting model learns general features of the data. This pre-trained model can then be fine-tuned with a small amount of specific, labelled data to perform a specialised task [18]. For instance, a model pre-trained

on billions of words can be fine-tuned with a few hundred medical reports to become a medical text classifier. This paradigm has democratised access to state-of-the-art AI performance [19].

6. Natural Language Processing

Natural Language Processing (NLP) is the intersection of AI and linguistics. Its objective is to enable computers to understand, interpret, and generate human language in ways that are both meaningful and useful. NLP systems handle tasks ranging from syntactic analysis to semantic understanding [1].

6.1 Algorithms and Models in NLP

Term Frequency-Inverse Document Frequency (TF-IDF): This numerical statistic reflects how important a word is to a document in a collection. It weighs the frequency of a word in a document against its commonness across all documents [20].

Word Embeddings: These models map words into a dense vector space where semantically similar words are located close to each other. The learned vectors capture rich relational meaning, such that "king" - "man" + "woman" results in a vector close to "queen" [21].

Transformer Architecture: This architecture processes an entire sequence of text at once using an attention mechanism. This mechanism weighs the importance of different words in relation to each other, enabling the model to capture long-range dependencies effectively. Large Language Models (LLMs) are built by pre-training Transformers on vast text corpora as foundation models [22].

7. Computer Vision

Computer Vision (CV) empowers computers to derive a high-level understanding from digital images and videos. Its goal is to automate tasks that the human visual system can perform, such as recognising objects and navigating environments [2].

6.1 Algorithms and Techniques in Computer Vision

Image Classification with CNNs: This task assigns a single global label to an entire image. A CNN extracts features through convolutional layers, which are then passed to a classifier that outputs a probability for each possible class label. Modern practice often fine-tunes a pre-trained CNN foundation model [18].

Object Detection (e.g., YOLO): This technique identifies all objects of interest within an image and defines their location with a bounding box. The "You Only Look Once" (YOLO) algorithm frames detection as a single regression problem, predicting boxes and class probabilities directly in one evaluation [23].

Generative Adversarial Networks (GANs): This framework pits two networks against each other: a generator that creates new data and a discriminator that evaluates its authenticity. This process drives the generator to produce increasingly realistic synthetic images [24].

8. AI in Robotics and Automation

Robotics and automation represent the physical embodiment of AI. AI provides the intelligence that allows these systems to handle variability and make decisions in unstructured environments, moving beyond rigid, pre-programmed routines [1].

7.1 AI Algorithms and Techniques used in Robotics

Path Planning (e.g., A* Search): This algorithm finds the shortest path for a robot to move from a start point to a destination while avoiding obstacles. It combines the actual distance travelled with an estimate to the goal [1].

Simultaneous Localisation and Mapping (SLAM): SLAM enables a robot to build a map of an unknown environment while simultaneously tracking its own location within that map. It is a fundamental technique for autonomous navigation [25].

Imitation Learning: This technique trains a robot to perform a task by learning from human demonstrations. The robot maps its sensory inputs directly to the expert's actions, bypassing complex manual programming [16].

9. Challenges and Limitations of Current AI

Despite remarkable progress, current AI systems face significant limitations that must be acknowledged. A balanced view requires an understanding of these persistent challenges.

Data Dependency and Bias: Deep learning models are notoriously data-hungry. Their performance is entirely dependent on the quantity and quality of the training data. If this data contains historical or societal biases, the model will not only learn these biases but can also amplify them.

Lack of Robustness and Common Sense: Modern AI systems can be brittle. They may fail unpredictably when presented with inputs that differ slightly from their training distribution, a problem known as 'poor out-of-distribution generalisation'. They also lack a grounded, causal understanding of the world and possess no real common sense.

The Generalisation vs Memorisation Debate: A central research question is whether large models truly learn abstract concepts or if they excel at sophisticated pattern memorisation. Evidence of memorisation suggests that models can reproduce verbatim segments of their training data, raising questions about true understanding and copyright.

Environmental Cost: Training very large-scale models, particularly large language and vision foundation models, consumes enormous amounts of computational power and energy. This carries a significant carbon footprint, creating a tension between performance gains and environmental sustainability.

10. AI Ethics and Responsible Development

As AI systems become integrated into critical societal functions, ethical considerations must guide every stage of their development. Responsible AI is not a separate step but a foundational framework built on four core pillars.

Fairness and Non-Discrimination: Algorithmic bias occurs when a system produces systematically prejudiced results, often because it learned from

historical data reflecting past inequalities. For example, a hiring model trained on biased data may penalize certain demographic groups. Ensuring fairness requires auditing datasets before training and testing model outputs across different groups for disparate impact [10].

Transparency and Explainability: Many powerful models, like deep neural networks, are "black boxes" whose internal reasoning is opaque. Explainable AI (XAI) creates methods to describe a model's decision in human-understandable terms. A local explanation can show which features most influenced a single prediction, enabling users to understand and contest incorrect or harmful automated decisions [10].

Accountability: Clear lines of responsibility must be established for AI outcomes. When a system fails, there should be no ambiguity about who is answerable: the developer, the deployer, or the user. Meaningful human review, where a person has the authority to override an automated decision, remains essential for high-stakes applications like loan approvals or medical diagnoses [26].

Privacy: AI models can memorise sensitive information from training data. Techniques like differential privacy add controlled statistical noise to datasets, protecting individual records while preserving overall patterns for learning. These four pillars together form the guardrails that guide AI toward being not only capable but also trustworthy and aligned with human well-being [27].

11. Conclusion

This chapter has provided a clear overview of artificial intelligence, covering its core concepts, history, and modern applications. The shift from early symbolic reasoning and rule-based systems to today's data-driven deep learning paradigms was traced. The various categories of machine learning, i.e., supervised, unsupervised, and reinforcement learning, were examined alongside the ML algorithms. Deep neural architectures and foundation models were discussed as the foundations behind powerful breakthroughs in natural language processing, computer vision, and robotics. Current limitations, including data dependency and bias, lack of robustness and common

sense, the generalization versus memorization debate, and environmental cost, were discussed as current research challenges. Ethical considerations, particularly algorithmic fairness, transparency, explainability, accountability, and privacy, are not optional additions but essential standards for responsible development. The convergence of these subfields has produced systems of remarkable capability, yet trustworthy deployment depends on integrating technical excellence with ethical awareness. The path forward requires continued research, thoughtful governance, and a shared commitment to building AI systems that reflect human values and serve the common good.

REFERENCES

- [1] Russell, S. J., & Norvig, P. (2021). *Artificial intelligence: A modern approach* (4th ed.). Pearson.
- [2] LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. *Nature*, 521(7553), 436–444. <https://doi.org/10.1038/nature14539>
- [3] Turing, A. M. (1950). Computing machinery and intelligence. *Mind*, 59(236), 433–460. <https://doi.org/10.1093/mind/LIX.236.433>
- [4] McCarthy, J., Minsky, M. L., Rochester, N., & Shannon, C. E. (1955). *A proposal for the Dartmouth summer research project on artificial intelligence*. <http://www-formal.stanford.edu/jmc/history/dartmouth/dartmouth.html>
- [5] Tripathi, A. S. (2026, April 26). *Approaches of Artificial Intelligence* [Diagram on AI approaches]. Scaler. <https://www.scaler.com/topics/artificial-intelligence-tutorial/approaches-of-artificial-intelligence/>
- [6] Jordan, M. I., & Mitchell, T. M. (2015). Machine learning: Trends, perspectives, and prospects. *Science*, 349(6245), 255–260. <https://doi.org/10.1126/science.aaa8415>
- [7] Silver, D., Huang, A., Maddison, C. J., Guez, A., Sifre, L., van den Driessche, G., Schrittwieser, J., Antonoglou, I., Panneershelvam, V., Lanctot, M., Dieleman, S., Grewe, D., Nham, J., Kalchbrenner, N., Sutskever, I., Lillicrap, T., Leach, M., Kavukcuoglu, K., Graepel, T., & Hassabis, D. (2016). Mastering the game of Go with deep neural networks and tree search. *Nature*, 529(7587), 484–489. <https://doi.org/10.1038/nature16961>
- [8] Brown, T. B., Mann, B., Ryder, N., Subbiah, M., Kaplan, J., Dhariwal, P., Neelakantan, A., Shyam, P., Sastry, G., Askell, A., Agarwal, S., Herbert-Voss, A., Krueger, G., Henighan, T., Child, R., Ramesh, A., Ziegler, D. M., Wu, J., Winter, C., ... Amodi, D. (2020). Language models are few-shot learners. In *Advances in Neural Information Processing Systems 33* (NeurIPS 2020). <https://arxiv.org/abs/2005.14165>
- [9] Searle, J. R. (1980). Minds, brains, and programs. *Behavioral and Brain Sciences*, 3(3), 417–424. <https://doi.org/10.1017/S0140525X00005756>
- [10] Marcus, G., & Davis, E. (2019). *Rebooting AI: Building artificial intelligence we can trust*. Pantheon.
- [11] Kurzweil, R. (2005). *The singularity is near: When humans transcend biology*. Viking.
- [12] Pinker, S. (1997). *How the mind works*. W. W. Norton & Company.
- [13] Dreyfus, H. L. (1992). *What computers still can't do: A critique of artificial reason*. MIT Press.
- [14] Bostrom, N. (2014). *Superintelligence: Paths, dangers, strategies*. Oxford University Press.

- [15] Russell, S. (2019). *Human compatible: Artificial intelligence and the problem of control*. Viking.
- [16] Sutton, R. S., & Barto, A. G. (2018). *Reinforcement learning: An introduction* (2nd ed.). MIT Press.
- [17] Hastie, T., Tibshirani, R., & Friedman, J. (2009). *The elements of statistical learning: Data mining, inference, and prediction* (2nd ed.). Springer.
- [18] Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep learning*. MIT Press.
- [19] Bommasani, R., Hudson, D. A., Adeli, E., Altman, R., Arora, S., von Arx, S., Bernstein, M. S., Bohg, J., Bosselut, A., Brunskill, E., Brynjolfsson, E., Buch, S., Card, D., Castellon, R., Chatterji, N., Chen, A., Creel, K., Davis, J. Q., Demszky, D., ... Liang, P. (2021). On the opportunities and risks of foundation models. *arXiv preprint arXiv:2108.07258*. <https://arxiv.org/abs/2108.07258>
- [20] Manning, C. D., Raghavan, P., & Schütze, H. (2008). *Introduction to information retrieval*. Cambridge University Press.
- [21] Mikolov, T., Chen, K., Corrado, G., & Dean, J. (2013). Efficient estimation of word representations in vector space. *arXiv preprint arXiv:1301.3781*. <https://arxiv.org/abs/1301.3781>
- [22] Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., Kaiser, Ł., & Polosukhin, I. (2017). Attention is all you need. In *Advances in Neural Information Processing Systems 30* (NeurIPS 2017). <https://proceedings.neurips.cc/paper/2017/hash/3f5ee243547dee91fbd053c1c4a845aa-Abstract.html>
- [23] Redmon, J., Divvala, S., Girshick, R., & Farhadi, A. (2016). You only look once: Unified, real-time object detection. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition* (CVPR 2016), 779–788. https://www.cv-foundation.org/openaccess/content_cvpr_2016/html/Redmon_You_Only_Look_CVPR_2016_paper.html
- [24] Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., & Bengio, Y. (2014). Generative adversarial nets. In *Advances in Neural Information Processing Systems 27* (NeurIPS 2014). <https://arxiv.org/abs/1406.2661>
- [25] Thrun, S., Burgard, W., & Fox, D. (2005). *Probabilistic robotics*. MIT Press.
- [26] Carlini, N., Tramèr, F., Wallace, E., Jagielski, M., Herbert-Voss, A., Lee, K., Roberts, A., Brown, T., Song, D., Erlingsson, Ú., Oprea, A., & Raffel, C. (2021). Extracting training data from large language models. In *Proceedings of the 30th USENIX Security Symposium* (USENIX Security 2021), 2633–2650. <https://www.usenix.org/conference/usenixsecurity21/presentation/carlini-extracting>
- [27] Strubell, E., Ganesh, A., & McCallum, A. (2019). Energy and policy considerations for deep learning in NLP. In *Proceedings of the 57th Annual Meeting of the Association for Computational Linguistics* (ACL 2019), 3645–3650. <https://aclanthology.org/P19-1355/>
- [28] Gupta, D.N., Kumar, R., Kumar, A. (2022). Federated Learning for IoT Devices. In: Yadav, S.P., Bhati, B.S., Mahato, D.P., Kumar, S. (eds) *Federated Learning for IoT Applications*. EAI/Springer Innovations in Communication and Computing. Springer, Cham. https://doi.org/10.1007/978-3-030-85559-8_2
- [29] Anand, R., Singh, H., Sardana, K., Gupta, D.N., Sindhwani, N., Mittal, M. (2024). Loan Approval Prediction Using Machine Learning. In: Abraham, A., Bajaj, A., Hanne, T. (eds) *Intelligent Systems Design and Applications*. ISDA 2023. Lecture Notes in Networks and Systems, vol 1052. Springer, Cham. https://doi.org/10.1007/978-3-031-64776-5_34

About the Book

Emerging Trends in Science and Technology features ten scholarly chapters by researchers, academicians, and professionals from diverse institutions. Each chapter explores current developments, innovative methodologies, practical applications, and future directions in its respective domain, providing readers with valuable insights into the rapidly changing landscape of modern science and technology.

About the Editor

Dr. Deena Nath Gupta is an academician, researcher, and editor with expertise in Computer Science and Engineering, specializing in cybersecurity, lightweight cryptography, Internet of Things (IoT) security, artificial intelligence, and emerging digital technologies. He is currently serving as an Associate Professor at the School of Engineering & Technology, Maharishi University of Information Technology (MUIT), Noida, India. Dr. Gupta received his Ph.D. in Computer Science from Jamia Millia Islamia, New Delhi. His research has resulted in numerous publications in reputable international journals, conference proceedings, book chapters, and patents, with significant contributions to lightweight security mechanisms for resource-constrained IoT devices. His research interests include cryptography, network security, IoT, machine learning, digital governance, and intelligent computing. As the Editor-in-Chief of JPTM Publications, Dr. Gupta is committed to promoting high-quality scholarly publishing and fostering interdisciplinary research. He has served as an editor, reviewer, technical program committee member, and session chair for several national and international conferences and journals. Through his academic, research, and editorial endeavors, Dr. Gupta continues to support innovation, knowledge dissemination, and collaboration among researchers, educators, and industry professionals across the globe.

JPTM

JPTM PUBLICATIONS

(A UNIT OF JPTM EDUCATION, RESEARCH & PUBLICATION SERVICES)

Barhaj, Deoria, UP, India - 274601

www.jptm.in

