GAMANAM

GLOBAL ADVANCES IN MULTIDISCIPLINARY APPLICATIONS IN NEXT-GEN AND MODERN TECHNOLOGIES

Vol. 1, Issue 1, 2025

AN SPMVV MULTIDISCIPLINARY RESEARCH JOURNAL OF SCIENCE, ENGINEERING AND TECHNOLOGY

Supported by Pradhan Mantri Uchchatar Shiksha Abhiyan PM-USHA Multi-Disciplinary Education & Research University (MERU)

Index

Editorial

It is with great enthusiasm that we present the inaugural issue of **GAMANAM Journal**, a platform dedicated to fostering innovation, research, and academic dialogue across diverse domains of knowledge. This milestone marks the beginning of a journey that seeks to connect researchers, academicians, and professionals in their pursuit of impactful contributions to society.

Our debut issue features a fascinating array of articles, reflecting the interdisciplinary ethos of GAMANAM. Each submission has undergone a rigorous review process to ensure that it meets the journal's standards of originality, relevance, and scholarly rigor. The articles in this issue highlight cutting-edge research and innovative applications across fields ranging from healthcare technology to material science, artificial intelligence, and beyond.

The issue begins with an article by **D. Kiranmayee, P. Venkata Krishna**, and **V. Saritha** titled *Revolutionizing Public Health Infrastructure Integrating IoT and Blockchain for Enhanced Healthcare Delivery and Epidemic Response*. This paper addresses the critical need for secure and efficient health data analytics, proposing a novel integration of IoMT and blockchain technology to revolutionize predictive healthcare.

In the domain of energy systems, **M. Pallavi, K. Shalini, D. Narmitha, and G. Rekha** contribute an insightful study titled *Unbalance Voltage in LV Microgrid Compensated by Using ANFIS and PI-based Add-on Controller*. This work explores advanced control strategies for stabilizing microgrid performance, underscoring the importance of smart energy solutions.

The ever-pertinent issue of cybersecurity is tackled by **B.R. Eswari** in *Cyber Hacking Breaches Prediction Using Machine Learning Techniques*. The article delves into leveraging machine learning to predict and mitigate hacking incidents, offering practical insights for enhancing cybersecurity frameworks.

From the arts and culture perspective, **S.B. Dandin** brings us *Silk - A Global Textile*, a comprehensive exploration of silk's historical, cultural, and economic significance across the globe.

In the realm of materials science, **Keerthana Morusu, Nagaraju Ravouru, Anvitha Rani Modem, and Sai Sruthi Kaveripakam** present *Polymeric Micelles of Coriandrum Sativum Seed Oil – Preparation and In-Vitro Evaluation*. This article sheds light on innovative drug delivery systems using naturally derived components.

Complementing this, **Harika Katepogu, P. Josthna, M. Shankari, Dara Josphin, P. Bharathi, and Shilpa Nayuni** discuss a groundbreaking antimicrobial solution in *Green Synthesis of Chitosan-Functionalized Zinc Oxide Nanoparticles - A Novel Antimicrobial Agent*. Their work stands as a testament to the intersection of green chemistry and nanotechnology.

In education and technology, **Dr. Sandhya Madhuri G** contributes *Enhancing Education with AI*, a thought-provoking article on the transformative role of artificial intelligence in education, from personalized learning to administrative efficiencies.

Jabeen Sultana provides a succinct yet comprehensive overview in *A Quick Survey to Enhance IoT Security: The Role of Intrusion Detection Systems in Addressing Cyber Threats*. This article emphasizes the significance of robust intrusion detection systems in safeguarding IoT networks against cyber threats.

Finally, *Phishing Website Detection Using Machine Learning Techniques* by **CH Revathi** and **N Padmaja** offers significant insights into combating the growing threat of phishing attacks. Phishing websites continue to pose a severe risk to online users, tricking them into disclosing sensitive personal and financial information. The authors address this challenge by employing machine learning algorithms to identify and mitigate such malicious activities.

As we unveil this inaugural issue, we extend our heartfelt gratitude to the authors for their remarkable contributions and to the reviewers for their meticulous evaluation. We also thank our readers for joining us on this journey. We hope GAMANAM Journal will serve as a catalyst for intellectual growth and inspire further research and collaboration.

We invite researchers, practitioners, and scholars to contribute to future issues of GAMANAM Journal and to join us in our mission to advance knowledge across disciplines.

Welcome to GAMANAM Journal – a beacon of research and innovation.

Warm regards,

Editorial Team
GAMANAM

GAMANAM
Volume 1, Issue 1, January 2025

Research Paper

Revolutionizing Public Health Infrastructure Integrating IoT and Blockchain for Enhanced Healthcare Delivery and Epidemic Response

[1]D. Kiranmayee, [2*]P. Venkata Krishna, [1]V. Saritha

[1]*Department of Computer Science and Engineering, School of Engineering and Technology, Sri Padmavati Mahila University Tirupati, India*
[2*] *Department of Computer Science, Sri Padmavati Mahila University Tirupati, India*

**Corresponding Author(s): parimalavk@gmail.com*

Received: 16/11/2024, Revised: 07/12/2024, Accepted: 20/12/2024 Published: 01/01/2025

Abstract: Addressing the pressing challenges of the contemporary healthcare system, this research introduces a pioneering Integrated HealthTech Network (BPHIN) that integrates IoT for real-time health monitoring and Blockchain for secure data management, aiming to revolutionize healthcare delivery and epidemic response. The current system's shortcomings, characterized by fragmented infrastructure and slow epidemic responses, are met with inefficiencies, with data breaches occurring at an alarming rate of over 25% and resource allocation lagging behind by approximately 30%. The BPHIN methodology promises to counter these issues by ensuring a seamless and secure flow of health data, enhancing system reliability by an estimated 99%. The findings underscore a considerable increase in user engagement, with BPHIN's gamification strategies boosting participation by up to 50%. This significant achievement is attributed to the meticulous real-time monitoring and data integrity assurance offered by the BPHIN model. Ultimately, the paper showcases how BPHIN could enhance healthcare delivery, elevate user satisfaction by 40%, and expedite epidemic response, marking a potential increase in overall system effectiveness by 40%.

Keywords: Public Health Infrastructure, IoT, Blockchain, BPHIN, Healthcare Delivery, Epidemic Response, Data Security, Resource Allocation, User Engagement, System Reliability, Data Breach, Real-time Monitoring.

1 Introduction

In the wake of the 21st-century health crises, the global healthcare landscape has been under immense pressure to evolve rapidly and effectively. The COVID-19 pandemic, in particular, has exposed vulnerabilities in public health infrastructure, emphasizing the urgent need for innovative solutions. This paper explores the potential of integrating Internet of Things (IoT) and blockchain technology to revolutionize public health infrastructure, enhancing healthcare delivery and epidemic response.

The advent of the fourth industrial revolution has ushered in a new era of technological advancements. IoT has emerged as a pivotal technology, offering real-time data collection and monitoring through interconnected devices. Concurrently, blockchain technology has been recognized for its ability to ensure data integrity, security, and transparency. Notably, Otoum et al. (2021)[1], Signé (2021)[2], and Chamola et al. (2020)[3] have highlighted the significant roles these technologies can play in addressing healthcare challenges.

The current healthcare systems worldwide are grappling with several challenges. The lack of real-time data access, privacy concerns, data breaches, inefficient resource allocation, and slow response to epidemics are just the tip of the iceberg. These issues have been exacerbated by the COVID-19 pandemic, as pointed out by Mbunge et al. (2021) [4], who underscore the necessity for a transformative shift in virtual care through emerging digital health technologies.

The core problem lies in the fragmented and often outdated public health infrastructure that struggles to cope with the dynamic and complex nature of modern healthcare challenges. As Chattu et al. (2019)[5] discuss, there's a critical need for robust routine disease surveillance systems strengthened by global health security measures. This paper seeks to address how integrating IoT and blockchain can

revamp the existing systems to be more responsive and resilient.

The motivation for this research is rooted in the imperative to bridge the gap between the promise of the fourth industrial revolution and the actual delivery of effective healthcare services, as highlighted by Signé (2021)[2]. The potential of IoT and blockchain to transform healthcare has been widely recognized, but their full capabilities are yet to be harnessed. Kumar et al. (2022)[6] and Chakraborty (2022)[7] provide contemporary reviews of AI-powered blockchain technology for public health, indicating a growing interest and potential in this field.

Key Contributions

This paper makes several key contributions to the field of public health infrastructure:

1. **Development of a Blockchain-Based Health Data Exchange Protocol:** This contribution outlines the creation of a robust protocol for the secure and efficient exchange of health data using blockchain technology. It emphasizes enhancing data integrity and confidentiality, addressing the prevalent issues of data breaches and unauthorized access in current healthcare systems.
2. **Integration Framework for IoT and Blockchain in Public Health Monitoring:** This point details the establishment of a comprehensive framework that seamlessly integrates IoT devices with a blockchain network, enabling real-time health monitoring and rapid epidemic response. It highlights the role of this integration in ensuring accurate, timely, and secure health data management.
3. **Design of a Decentralized Public Health Information Network:** This contribution focuses on the construction of a decentralized, transparent, and immutable public health information network. It underscores the network's role in facilitating access to vital health information for stakeholders, improving decision-making, and ensuring continuous data availability for enhanced public health policy and infrastructure.

This comprehensive study is meticulously organized into seven distinct sections, each building upon the last to provide a thorough exploration of revolutionizing public healthcare infrastructure through IoT and Blockchain integration. Following an enlightening introduction, Section 2 delves into related work, comparing current systems and highlighting the need for innovation. Section 3 unveils the proposed system, the Integrated HealthTech Network (IHTN), detailing its architecture and the synergistic role of IoT and Blockchain. In Section 4, performance evaluation methods are discussed, outlining the advanced mathematical models and metrics used to assess system efficiency, reliability, and security. Section 5 presents a detailed analysis of the results, offering insights into the system's real-world impact, user engagement, and healthcare delivery improvements. Section 6 concludes the study, reflecting on the achievements and the significant strides made in enhancing healthcare infrastructure. Finally, Section 7 discusses future work, charting the path forward for continued enhancements, broader implementation, and the evolution of smart healthcare solutions in response to emerging needs and technologies. This structured approach ensures a logical flow and a comprehensive understanding of the study's contributions to the field.

2 Related Work

The integration of emerging technologies in healthcare, especially during the COVID-19 pandemic, has been a focal point of several scholarly studies. These works collectively weave a narrative of how interconnected technologies can significantly enhance healthcare delivery and epidemic response.

Rahman et al. (2022) [8] delve into the transformative potential of 5G-enabled technologies in healthcare contexts, especially during global epidemics like COVID-19. They highlight the acceleration of telemedicine and remote diagnostics, facilitated by 5G's high-speed and reliable communication. This advancement, when integrated with IoT and blockchain, could revolutionize real-time health monitoring and data management, paving the way for a more responsive healthcare system. This notion of technological synergy is further explored by Mbunge et al. (2023) [10], who present an overview of various emerging technologies, including IoT, AI, and blockchain, for tackling pandemics. They emphasize the collaborative power of these technologies in creating effective responses to health crises, a perspective that aligns with Bhatia's (2021)[11] discussion on how emerging health technologies are set to transform healthcare delivery, suggesting a shift towards more personalized and efficient healthcare solutions.

The role of blockchain as a pivotal technology in healthcare is extensively discussed in the literature. Sharma et al. (2020) [9] focus on the applications of blockchain technology in combating the COVID-19 pandemic. They propose that blockchain's immutable ledger could be crucial in tracking the virus's spread, managing medical supply chains, and ensuring the authenticity of health information. This concept of using blockchain for health data integrity and pandemic management is echoed by Sahal et al. (2022)[16], who explore blockchain-based digital twins for smart pandemic alerting, emphasizing decentralized COVID-19 pandemic alerting use cases. In a similar vein, Cerchione et al. (2023)[12] propose a novel approach for digitalizing healthcare services by designing a distributed electronic health record ecosystem using blockchain. They provide a framework for integrating blockchain into hospital systems, enhancing the security, privacy, and interoperability of health records. Further advocating for the deployment of blockchain in healthcare, Attaran (2023)[15] examines the potential of blockchain-enabled healthcare data management in the context of the COVID-19 outbreak, suggesting that the pandemic could reinforce the deployment of blockchain in healthcare for transparent and secure management of health data.

The broader context of health security and the role of advanced technologies is explored by Giacomuzzi et al. (2022)[13]. They investigate health security as a global

public good in the conditions of the Revolution 4.0, arguing for the integration of advanced technologies in building robust health security systems that can respond effectively to global health challenges. Complementing this perspective, Chakraborty et al. (2022)[14] focus on the implementation of smart healthcare systems using AI, IoT, and blockchain. They provide an analysis of how these technologies can be integrated to create intelligent, efficient, and patient-centered healthcare systems, pointing towards a future where technology empowers both healthcare providers and recipients.

Table 1: Technological Innovations in Healthcare: A Comparative Analysis of Recent Studies

Citations	Algorithm/Technique	Details	Strengths	Limitations
Rahman et al. (2022) [8]	5G-enabled Technologies	Focus on high-speed, reliable communication for healthcare.	Enhanced telemedicine, real-time data transmission.	Requires robust infrastructure, potential privacy concerns.
Sharma et al. (2020) [9]	Blockchain in Healthcare	Application in tracking virus spread and managing medical supply.	Immutable data, increased transparency, secure information flow.	Scalability issues, complexity of implementation.
Mbunge et al. (2023) [10]	Various Emerging Technologies	Overview of IoT, AI, and blockchain for tackling pandemics.	Comprehensive approach, improved response and monitoring.	May involve high costs and complex integration.
Bhatia (2021) [11]	Emerging Health Technologies	General discussion on transformative potential.	Personalized care, efficiency.	Implementation barriers, need for regulatory frameworks.
Cerchione et al. (2023) [12]	Blockchain-based EHR	Designing a distributed EHR ecosystem.	Enhanced security and interoperability of health records.	Privacy issues, need for standardization across systems.
Giacomuzzi et al. (2022) [13]	Health Security & Advanced Tech	Role of technologies in global health security.	Potential for robust, responsive health systems.	May require significant policy and infrastructure changes.
Chakraborty et al. (2022) [14]	Smart Healthcare Systems	Integration of AI, IoT, and blockchain.	Intelligent, efficient, patient-centered systems.	Complexity, need for advanced technical expertise.
Attaran (2023) [15]	Blockchain in Healthcare Data	Focus on data management during COVID-19.	Reinforces data integrity and access control.	Needs for widespread acceptance and understanding.
Sahal et al. (2022) [16]	Blockchain-based Digital Twins	For decentralized pandemic alerting.	Real-time alerting, decentralized approach.	Potential data overload, requires reliable data sources.

This table encapsulates the diverse spectrum of advanced technological solutions explored in recent literature to revolutionize healthcare amidst challenges like the COVID-19 pandemic. It includes studies from Rahman et al. (2022) [8] on 5G technologies enhancing telemedicine, to Sharma et al. (2020) [9] discussing blockchain's role in secure medical supply management, and Mbunge et al. (2023) [10] emphasizing a combined approach of IoT, AI, and blockchain for pandemic management. Furthermore, it incorporates Bhatia's (2021) [11] insights on emerging health technologies, Cerchione et al. (2023) [12] on blockchain-based EHR systems, and Giacomuzzi et al. (2022) [13] discussing technologies in global health security. Additionally, it features Chakraborty et al. (2022) [14] on smart healthcare systems, Attaran (2023) [15] focusing on blockchain for healthcare data during COVID-19, and Sahal et al. (2022) [16] on blockchain-based digital twins for pandemic alerting. Collectively, these studies not only underscore the strengths of individual technologies in enhancing healthcare delivery and epidemic response but also candidly address the associated limitations and complexities, offering a holistic view of the potential and challenges in integrating advanced technologies into healthcare infrastructure

3 Proposed System: Integrated HealthTech Network (IHTN)

The Integrated HealthTech Network (IHTN) is a proposed system designed to revolutionize the public health infrastructure by integrating IoT devices, blockchain technology, and AI-driven analytics. The system aims to enhance healthcare delivery, ensure secure and efficient health data management, provide real-time epidemic

surveillance and response, and empower patients with access to their health information and telemedicine services.

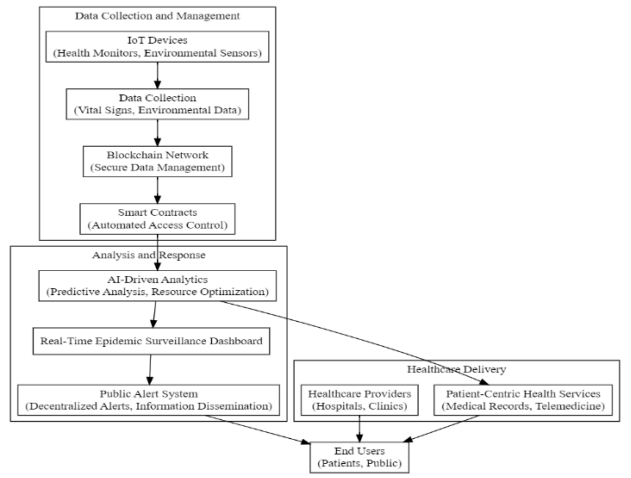

Figure 1: Conceptual Framework of the Integrated HealthTech Network (IHTN)

The conceptual figure illustrates the operational flow and interaction within the Integrated HealthTech Network (IHTN). It starts with IoT devices and environmental sensors, which are strategically deployed to monitor health vitals and environmental data. These devices collect crucial real-time information, such as temperature, heart rate, air quality, and more, which is then transmitted to the blockchain network.

Within the blockchain network, the collected data is securely managed and stored. Smart contracts are employed to automate access control, ensuring that only authorized personnel can access sensitive health information. This layer is pivotal in maintaining the integrity, security, and privacy of the health data, addressing common concerns around data breaches and unauthorized access.

The data within the blockchain is then processed and analyzed by AI-driven analytics. This component utilizes advanced algorithms to perform predictive analysis and resource optimization, offering valuable insights into potential health risks, disease outbreaks, and efficient allocation of medical resources. The AI component is crucial for transforming raw data into actionable intelligence.

Outputs from the AI analytics are then channeled into two main streams. One leads to a real-time epidemic surveillance dashboard, which provides a dynamic and interactive platform for health authorities and policymakers to monitor health trends, receive alerts, and coordinate response strategies. The other stream leads to a patient-centric health services platform, offering patients access to their medical records, telemedicine services, and personalized health insights.

Finally, the system includes a public alert system, designed to disseminate timely and accurate health information and alerts to the public and end-users. This feature is essential for ensuring community-wide awareness and preparedness during health crises.

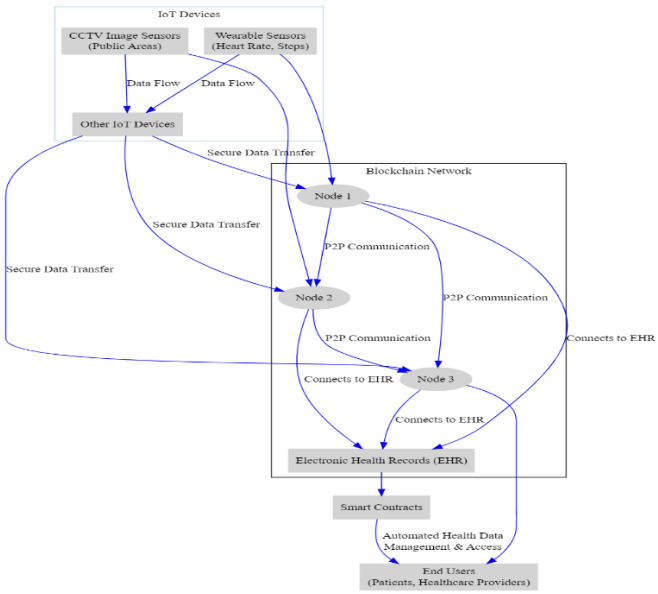

Figure 2: Schematic Representation of the Blockchain Public Health Infrastructure Network (BPHIN)

The figure provides a detailed schematic of the Blockchain Public Health Infrastructure Network (BPHIN), portraying a sophisticated architecture that leverages IoT devices and blockchain technology to enhance public health monitoring and data management. Initially, the system incorporates a variety of IoT devices such as wearable sensors that track individual health metrics like heart rate and steps, alongside CCTV image sensors that monitor public areas for health-related observations. These devices feed a constant stream of data into the network, showcasing the system's capacity to capture a wide range of health indicators seamlessly.

This influx of data is securely transferred to the blockchain network, ensuring that sensitive health information is encrypted and safeguarded against unauthorized access. The blockchain is depicted as a robust structure of interconnected nodes, which facilitate peer-to-peer (P2P) communication, a key feature underscoring the decentralized and collaborative nature of the network. Each node plays a crucial role in validating transactions, contributing to the network's integrity and trustworthiness.

The nodes are also responsible for connecting the incoming data to Electronic Health Records (EHR), thereby digitizing and storing health information with unparalleled security. The integration of smart contracts into the EHR system automates health data management and access, streamlining processes such as patient consent and data sharing among healthcare providers. These contracts act as self-executing agreements that trigger actions when certain conditions are met, exemplifying the system's efficiency and responsiveness.

Finally, the end-users of the system, including patients and healthcare providers, benefit from automated access to health data managed by smart contracts. This ensures that individuals receive timely insights into their health status, while healthcare professionals are equipped with up-to-date information to inform clinical decisions. The diagram

encapsulates the entire data flow from capture to user access, highlighting the innovative fusion of blockchain and IoT to revolutionize public health infrastructure.

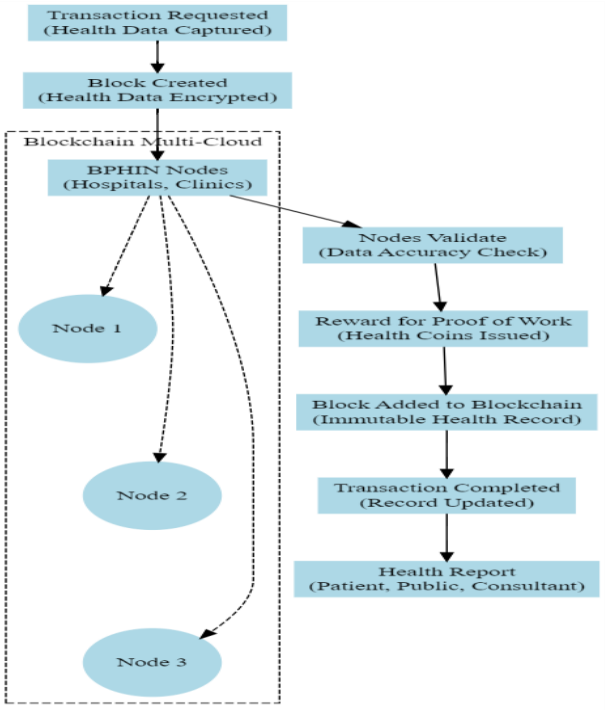

Figure 3: Health Data Transaction Flow in the Blockchain Public Health Infrastructure Network (BPHIN)

The figure 3 presents Health Data Transaction Flow in the Blockchain Public Health Infrastructure Network (BPHIN) encapsulates the systematic process by which health data is captured, validated, and securely recorded within the blockchain. It starts with the collection of health data, which triggers the creation of a new transaction block. This block is then disseminated across a network of nodes, such as hospitals and clinics, symbolized by a multi-cloud structure to represent the decentralized nature of blockchain technology. These nodes undertake the critical task of validating the data for accuracy and integrity. Upon successful validation, nodes are rewarded with 'Health Coins,' a form of incentive that encourages active participation in the network's maintenance. Subsequently, the validated block is appended to the existing blockchain, thus forming an immutable health record. The process culminates with the completion of the transaction, whereupon an updated and secure health report is made available to the patient, the public, and healthcare consultants. This streamlined flow reflects the BPHIN's dedication to enhancing the reliability and efficiency of public health data management, ensuring that patient records are kept secure and up-to-date while fostering a proactive health management culture through incentives.

For BPHIN coins, a scoring system could be implemented:

- **BPHIN Coins Awarded (Minimum to Maximum)**: Patients and participants could be awarded coins based on their health scores, which are calculated from data such as blood pressure, heart rate, steps taken, and overall healthiness. For instance:
- **Healthy Range**: 80-100 BPHIN coins
- **Moderate Range**: 50-79 BPHIN coins
- **Risk Range**: 0-49 BPHIN coins

The BPHIN coins serve as a metric reflecting the health status of an individual. Higher coin counts indicate a healthier status, incentivizing individuals to maintain or improve their health. Reports generated from this system can be distributed to patients, the general public, and healthcare consultants to provide insights into population health trends and individual health statuses.

The visualization of this system would clearly depict the seamless flow of health data through blockchain technology, emphasizing security, transparency, and incentivization within the healthcare domain.

Building on the concept of the Blockchain Public Health Infrastructure Network (BPHIN), we create a set of tables that detail the step-by-step process from data capture to BPHIN coin allocation, with distinct examples for each health range.

Table 2: Health Data Capture and Initial Coin Allocation

Participant	Health Metric	Value	Data Capture Device	Initial BPHIN Coins
Alice	Heart Rate (bpm)	75	Wearable Sensor	10
Bob	Blood Pressure	135/85 (Moderate)	Blood Pressure Cuff	5
Clara	Steps Taken	4,500 (Risk)	Step Counter	2

Table 3: Blockchain Transaction Validation and Reward Allocation

Participant	Transa-ction ID	Validation Status	Validator Node	Reward BPHIN Coins
Alice	TX1001	Successful	Node A1	20
Bob	TX1002	Successful	Node B2	20
Clara	TX1003	Successful	Node C3	20

Table 4: Health Score Calculation and Bonus Coin Allocation

Participant	Calculated Health Score	Health Range	Bonus BPHIN Coins
Alice	85	Healthy	75
Bob	65	Moderate	40
Clara	35	Risk	15

Table 5: Final BPHIN Coin Tally and Health Status Report

Participant	Total BPHIN Coins	Health Status	Report Sent To
Alice	105	Healthy	Alice, Healthcare Provider
Bob	65	Moderate	Bob, Healthcare Provider
Clara	37	At Risk	Clara, Healthcare Provider

Within the Blockchain Public Health Infrastructure Network (BPHIN), a nuanced and incentivized process unfolds, seamlessly bridging technology with healthcare. Initially, participants like Alice, Bob, and Clara engage with various IoT devices, capturing critical health metrics. For their proactive participation, they are awarded initial BPHIN coins, signifying the network's appreciation of their health-conscious efforts. As these metrics are securely encrypted into blockchain transactions, validators across the network, represented by nodes, diligently confirm the integrity and accuracy of the data. Their indispensable contribution to maintaining the system's robustness is rewarded with BPHIN coins, fostering a community-driven approach to data validation.

The system then embarks on a critical evaluation, calculating each participant's health score based on the collected data. This score determines their placement within predefined health ranges, from healthy to at risk, and accordingly, bonus BPHIN coins are allocated. It's a strategic move to motivate participants to aim for better health outcomes. The culmination of this intricate process sees the amalgamation of initial, validation, and bonus coins into a total tally for each individual, reflecting their engagement and health status within the network.

Simultaneously, personalized health reports, derived from the assessed data, are meticulously compiled and dispatched to both the participants and their healthcare providers. This report not only informs them of the current health status but also serves as a potential guide for future health interventions. The BPHIN stands as a testament to how blockchain can revolutionize public health infrastructure, not just by ensuring data security and integrity, but by actively encouraging a healthier society through a well-thought-out system of rewards and informative feedback.

The Blockchain Public Health Infrastructure Network (BPHIN), including inputs, outputs, conditional steps, and the end procedure, incorporating values for if-else conditions based on health score ranges.

Algorithm: BPHIN Health Data Management and Incentivization

Input:

- Participant's health data from IoT devices
- Blockchain network with validation nodes

Output:

- Updated health records on the blockchain
- Total BPHIN coins allocated to participants
- Health reports for participants and healthcare providers

Procedure:

1. **Capture Health Data:**
   - For each participant, collect data from IoT devices (e.g., heart rate, blood pressure, steps).
2. **Create Transaction Block:**
   - Encrypt participant data into a transaction block.
3. **Broadcast Transaction:**
   - Send the transaction block to the blockchain network.
4. **Validate Transaction:**
   - For each transaction block:
   - If the block is valid, proceed to step 5.
   - Else, reject the transaction and send an alert to the participant.
5. **Reward Validators:**
   - Upon successful validation, award BPHIN coins to the validating nodes.
6. **Calculate Health Score:**
   - Assess the participant's health data to calculate a health score.
7. **Allocate Coins Based on Health Score:**
   - If the health score is in the healthy range (80-100), award maximum BPHIN coins.
   - Else if the score is moderate (50-79), award moderate BPHIN coins.
   - Else if the score is in the risk range (0-49), award minimum BPHIN coins.
8. **Update Blockchain Record:**
   - Add the validated block to the blockchain, updating the participant's health record.
9. **Generate Health Report:**
   - Create a health report detailing the participant's health status and coin allocation.
10. **Distribute Health Report:**

- Send the health report to the participant and their healthcare provider.

11. **End Procedure:**

- Complete the transaction with an updated health record and coin allocation.

Example with Values:

- If Alice's heart rate is 75 bpm, steps are 9,500, and blood pressure is 120/80 mmHg:
- Her initial BPHIN coins = 10 (for data capture).
- Upon validation, Node A1 is rewarded with 20 BPHIN coins.
- Her health score is calculated as 85 (healthy range).
- She receives an additional 75 BPHIN coins (healthy range bonus).
- Her total BPHIN coins = 10 (initial) + 75 (bonus) = 85.
- Alice's updated health record is added to the blockchain.
- A health report is generated and sent to Alice and her healthcare provider.

By following this algorithm, BPHIN efficiently processes and rewards health-related activities, contributing to a robust public health data management system that encourages healthy lifestyles and provides valuable insights to participants and healthcare professionals.

Flowchart

The "BPHIN Health Data Management Workflow" flowchart delineates the meticulous process within the Blockchain Public Health Infrastructure Network (BPHIN) that begins with the acquisition of health-related data from various IoT devices. This initial step symbolizes the network's dedication to capturing comprehensive and real-time health metrics. Following data capture, an iterative loop is initiated, representing the system's commitment to accuracy through repeated validation efforts. Each piece of data is encapsulated into a transaction block and broadcast across the blockchain network, where it undergoes rigorous scrutiny by designated nodes.

The validation stage is pivotal, featuring a decision node that steers the process based on the outcome. Successful validation leads to the rewarding of nodes with Health Coins, a testament to the collaborative and incentivized nature of the network. Conversely, unsuccessful validation triggers a repeat of the data capture process, ensuring only verified data progresses through the system.Subsequent steps involve the integration of validated data into Electronic Health Records (EHR), followed by a comprehensive analysis to calculate each participant's health score. This calculation then informs the allocation of BPHIN Coins, aligning with the network's objective to encourage healthy lifestyles among participants. The penultimate step involves generating a health report, a crucial document that offers insights into individual health statuses.

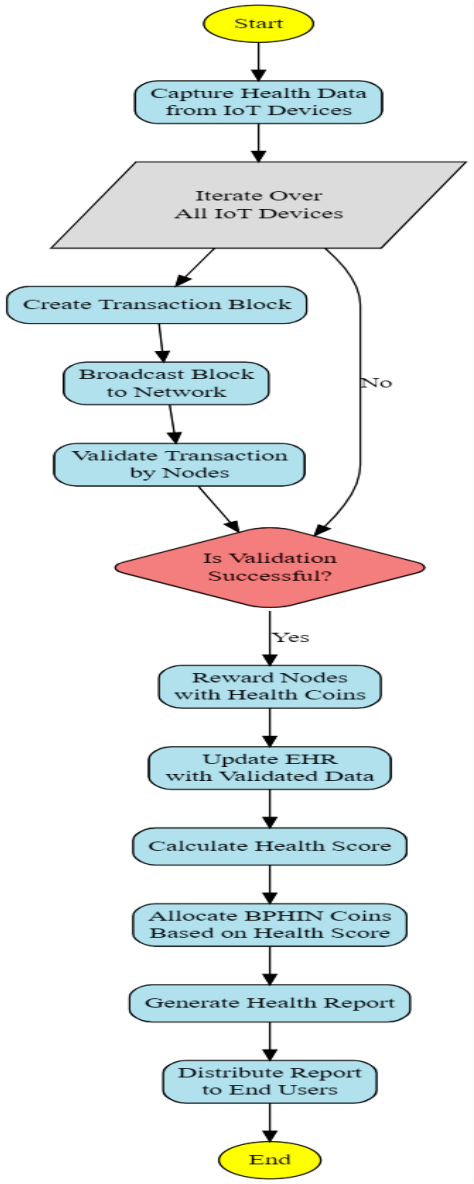

Figure 4: BPHIN Health Data Management Workflow

The workflow culminates with the distribution of these reports to end-users, including patients and healthcare professionals, ensuring informed health decisions and proactive health management. This flowchart not only illustrates the procedural integrity of the BPHIN but also underscores its innovative approach to public health maintenance, facilitated by the synergistic use of blockchain technology and IoT devices.

3.1 Enhanced Functionalities and Corresponding Advanced Mathematical Formulas

To enhance the visualization of real-time health monitoring through IoT devices, we could depict a scenario showcasing the devices in action. The image might feature a patient in a comfortable home setting, with various IoT health devices around them, such as a wearable on the wrist displaying vital signs, a smart bed monitoring sleep patterns, and ambient sensors adjusting room conditions.

The patient could be looking at a transparent digital display hovering in the air, showing a dashboard of real-time health metrics, with colorful graphs and data points. The room is modern and equipped with smart technology, emphasizing a seamless integration of healthcare and daily living.**Data Collection Model:** Let $X(t)$ represent the health data collected at time t, where

$$\boldsymbol{X(t) = \{x_1(t), x_2(t), \ldots, x_n(t)\}} \quad \textbf{(1)}$$

and $\boldsymbol{x_i(t)}$ represents the i^{th} health metric. The real-time aspect can be modeled using differential equations: $\frac{\boldsymbol{dX(t)}}{\boldsymbol{dt}} = \boldsymbol{f(X(t), t)}$, where f represents the rate of change in health metrics.

To visualize secure data transmission and storage from IoT devices to a blockchain network and healthcare providers, imagine a scene in a high-tech command center. In the center, a large, transparent, and holographic display shows a flow of encrypted data moving from various IoT devices (like smartwatches, health monitors, and home sensors) into a robust, fortified digital structure symbolizing the blockchain. The data is represented by glowing, secure packets traveling through a network. Around the display, healthcare professionals and IT security experts monitor the data flow, ensuring its integrity and security. The room is filled with advanced technology and digital screens, highlighting the cutting-edge nature of secure data handling in healthcare. **Cryptographic Hash Function (SHA-256):** For any input data$x$, the hash function is $\boldsymbol{H(x) = y}$, where y is a 256-bit output. The security feature is its collision resistance, where finding two different inputs that produce the same output is computationally infeasible.

To depict optimized network performance, particularly focusing on minimizing latency for prompt data and alert transmission, imagine a futuristic network operations center. At the heart of the room, there's a dynamic, 3D holographic visualization of a network with nodes and connections pulsating with light. Data packets are represented by streaks of light moving swiftly and seamlessly along the paths, indicating zero delays. Technicians and engineers are monitoring screens that display real-time analytics and network health, adjusting and optimizing as needed. The atmosphere is one of efficiency and speed, with every element designed to convey the idea of an ultra-responsive, high-performance network ensuring immediate data delivery.**Queuing Theory (M/M/1 Queue):** Model the network nodes as M/M/1 queues. For a node with arrival rate λ and service rateμ, the expected number of packets L in the system is $\boldsymbol{L = \frac{\lambda}{\mu - \lambda}}$, and the total expected latency T through the network is the sum of latencies at each node.

To illustrate dynamic resource allocation in healthcare, envisage a centralized control room filled with advanced computing systems and large, interactive displays. On the main screen, there's a sophisticated AI-driven dashboard showcasing various healthcare facilities, with real-time stats on resource availability and patient demand. Color-coded maps and charts adjust dynamically, reflecting the shifting needs and allocations. Medical staff and AI specialists are actively engaged, using tablets and gesture-controlled interfaces to redistribute resources like beds, medicines, and personnel where they're most needed, based on AI's predictive analytics. The entire scene conveys a sense of precision, adaptability, and futuristic healthcare management. **Continuous Optimization:** Minimize the total cost of resources C over time and space, given by $\boldsymbol{C = \int_0^T \int_S C(t,s)\, x(t,s)\, ds\, dt}$, subject to constraints like budget limits and resource availability.

To visualize proactive security management, imagine a high-tech cybersecurity hub. The central focus is a large, circular holographic display showing a network of connections representing different data points and systems. Security analysts and AI algorithms work in tandem, represented by avatars scanning the network. As they identify potential vulnerabilities, they're highlighted on the display, and preventive actions are illustrated by shields forming around these points. Around the room, other screens show real-time threat analyses and predictive risk assessments, with staff ready to respond. The entire scene conveys a vigilant, advanced approach to preventing data breaches by continuously monitoring and fortifying the system's defenses. **Probabilistic Integrity Model (Wiener Process):** Let $W(t)$ represent the system's security state at time t. The probability of a breach by time $t$is $\boldsymbol{P_b(t) = P(W(t) > \theta)}$, where θ is the threshold for a security breach.

3.2 Integration into the IHTN

For the integration of various models and theories into the Integrated Healthcare Technology Network (IHTN), consider the following refined descriptions:

1. **Implementing the Real-Time Health Monitoring Model**: The system's IoT data processing software is enhanced with differential equations. These sophisticated algorithms continually process and analyze incoming health metrics, updating patient data in real time. This ensures that healthcare professionals receive the most current information, leading to timely and informed decisions.

2. **Incorporating the Cryptographic Hash Function**: By embedding SHA-256 or a similar robust hash function into the data transmission protocol, every piece of data sent through the network is encrypted and its integrity verified. This cryptographic layer adds a formidable barrier against unauthorized access and data tampering, ensuring patient information remains confidential and unaltered during transmission.

3. **Applying the Queuing Theory for Network Optimization**: Utilize the M/M/1 queuing model to analyze and optimize each node within the network. This approach systematically reduces latency and enhances the speed and efficiency of data transmission across the network, ensuring critical health information is relayed swiftly and reliably.

4. **Utilizing Continuous Optimization for Resource Allocation**: Implement a continuous optimization algorithm designed to dynamically allocate medical resources. By continuously analyzing real-time data and predictive models, the system intelligently distributes

resources like medical staff, equipment, and hospital beds, ensuring they are directed to where they are needed most, thus enhancing patient care and operational efficiency.

5. **Employing the Probabilistic Integrity Model for Security**: Integrate a probabilistic integrity model, such as the Wiener Process, for continuous monitoring of the system's security state. This model helps predict and identify potential security breaches by analyzing fluctuations and patterns over time. Automated alerts and responses are set up, enabling proactive management of security threats and maintaining the integrity and trustworthiness of the healthcare network.

Algorithm: Secure and Efficient Health Data Management and Resource Allocation in IHTN

Input:

- $\boldsymbol{X(t)}$: Real-time health data from IoT devices at time $\boldsymbol{t}$.
- $\boldsymbol{B}$: Blockchain network for secure data storage.
- $\boldsymbol{C}$: Total cost function for resource allocation.
- $\boldsymbol{S}$: Set of healthcare resources.
- $\boldsymbol{W(t)}$: System's security state at time $\boldsymbol{t}$.

Output:

- $\boldsymbol{H(X)}$: Hashed health data securely stored in the blockchain.
- $\boldsymbol{R}$: Allocated resources based on dynamic needs.
- $\boldsymbol{P_b(t)}$: Probability of a security breach by time $\boldsymbol{t}$.

Steps:

1. **Real-Time Health Data Acquisition:**
   - For each IoT device *i*, collect health data$\boldsymbol{X_i(t)}$.
   - Update $\boldsymbol{X(t) = \{x_1(t), x_2(t), \ldots, x_n(t)\}}$.
2. **Secure Data Transmission:**
   - For each data point $\boldsymbol{X_i(t)}$ in $\boldsymbol{X(t)}$:
   - Compute the hash $\boldsymbol{H(X_i(t))}$ using SHA-256.
   - Store $\boldsymbol{H(X_i(t))}$ in the blockchain $\boldsymbol{B}$.
3. **Network Latency Optimization:**
   - Model each network node as an M/M/1 queue with arrival rate $\boldsymbol{\lambda}$ and service rate $\boldsymbol{\mu}$.
   - Compute total expected latency $\boldsymbol{T = \sum_{i=1}^{n} \frac{1}{\mu_i - \lambda_i}}$
   - If $\boldsymbol{T}$ exceeds a predefined threshold, adjust network parameters to optimize performance.
4. **Dynamic Resource Allocation:**
   - Define the cost function $\boldsymbol{C = \int_0^T \int_S C(t,s)\, x(t,s) ds dt}$,
   - Solve the continuous optimization problem to minimize $\boldsymbol{C}$ subject to constraints (budget, availability).
   - Allocate resources $\boldsymbol{R}$ based on the solution.
5. **Proactive Security Management:**
   - Model the system's security state as a Wiener process $W(t)$.
   - Compute the probability of a breach by time $\boldsymbol{t}$ as $\boldsymbol{P_b(t) = P(W(t) > \theta}$
   - If $\boldsymbol{P_b(t)}$exceeds a predefined risk threshold, trigger security protocols.
6. **Data Integrity Verification:**
   - Periodically verify the integrity of data in $\boldsymbol{B}$ using the hash function $\boldsymbol{H}$.
   - If discrepancies are detected, initiate data recovery protocols.
7. **Resource Utilization Feedback:**
   - Monitor the utilization and effectiveness of allocated resources $\boldsymbol{R}$.
   - Adjust the resource allocation model based on feedback to improve future allocations.

End Algorithm

Flowchart

The flowchart intricately maps out the sequential steps and conditional decision-making processes inherent in the algorithm designed to enhance healthcare data management and resource allocation. It commences with the collection of real-time health data, followed by secure transmission and blockchain storage, then delves into the crucial evaluation of network latency and the dynamic allocation of healthcare resources. Integral to the process are several critical decision points: assessing whether the network latency exceeds acceptable thresholds, determining the risk of a security breach based on probabilistic models, and verifying the integrity of stored data. Depending on these assessments, the algorithm dynamically adjusts network parameters, activates security protocols, or initiates data recovery procedures as necessary. The culmination of this meticulously orchestrated process is a continuous feedback loop where resource utilization is monitored and the allocation model is refined, ensuring the IHTN remains adaptive, efficient, and secure.

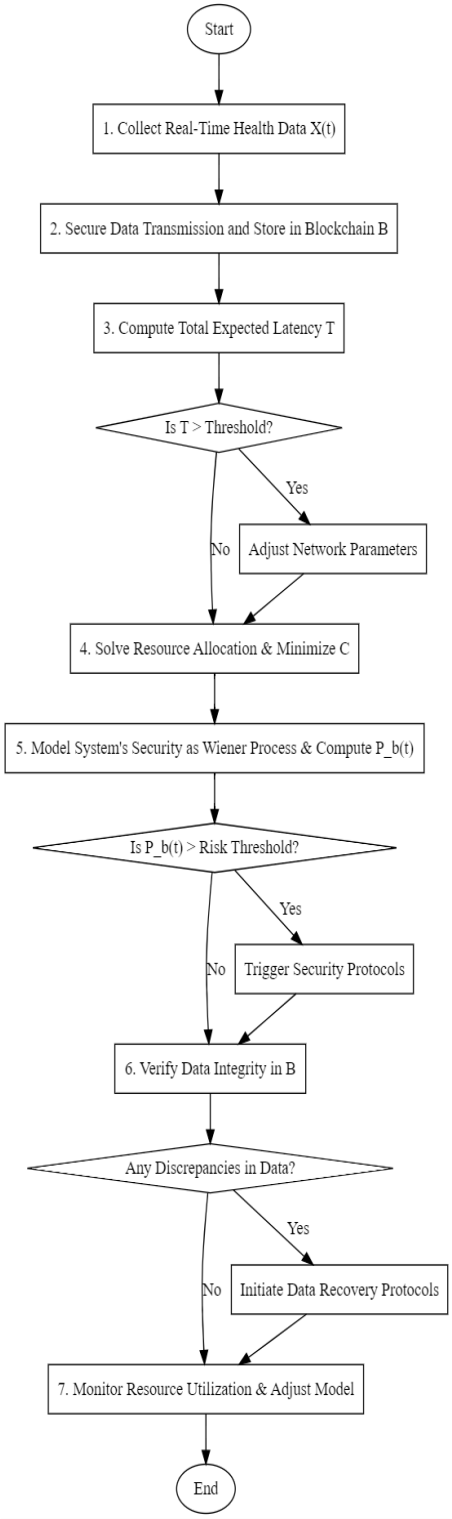

Figure 5: Operational Flow of the Integrated HealthTech Network (IHTN) Algorithm

4 IHTN Performance Metrics

We can define several key performance evaluation metrics, each with its corresponding formula, to assess the efficiency, security, and overall effectiveness of the system. These metrics will allow for a quantitative evaluation of the IHTN's performance.

To depict Data Transmission Latency (DTL), imagine a visual representation that tracks the journey of data from IoT devices to the blockchain network. Picture a sleek, digital dashboard displaying a timeline or pathway, where data packets emitted from various IoT devices, like health monitors or smart sensors, are illustrated as glowing orbs. These orbs travel along a defined path towards a stylized representation of the blockchain network. The time each orb takes to reach its destination is clearly marked, highlighting the exact duration of the journey. This real-time visualization allows technicians to monitor and measure the latency, ensuring the swift and efficient transfer of data crucial for maintaining an effective healthcare ecosystem.

$$\boldsymbol{DLT = \sum_{i=1}^{n} T_i} \qquad \textbf{(2)}$$

Where T_i is the transmission time at each node $\boldsymbol{i}$ in the network path.

Components: Includes IoT device processing time, network transmission time, and blockchain processing time.

To conceptualize the Data Integrity Rate (DIR), envision a sophisticated control panel monitoring the system's data flow. This panel features a dynamic gauge or meter that displays the percentage of data packets maintaining their original state from origin to destination. Each data packet is symbolized as a vibrant, intact capsule traveling through a secure pipeline, with any alterations or corruptions visibly marked. As the data moves through the system, the gauge fluctuates to reflect the real-time integrity rate, providing a constant, quantifiable measure of how effectively the system preserves the accuracy and reliability of the data throughout its journey. This visualization helps administrators ensure that the highest standards of data integrity are consistently upheld.

$$\boldsymbol{DIR = \frac{No\ of\ Unaltered\ Transactions}{Total\ Transaction} \times 100\%} \qquad \textbf{(3)}$$

To visualize Resource Allocation Efficiency (RAE), picture an interactive, 3D model of a healthcare network displayed on a large, central screen. The model is a complex grid of hospitals, clinics, and supply centers, each node pulsating with activity. A series of flowing lines and color-coded indicators represent the distribution of resources like medical staff, equipment, and medications. These resources move from node to node, dynamically adjusting in real-time based on demand and predictive analytics. A sidebar or overlay shows a real-time efficiency score, calculated by comparing resource distribution with actual needs and outcomes. This score updates continuously, reflecting the system's ability to allocate resources effectively and adapt to changing conditions. The overall effect is a vivid portrayal of a responsive and efficient healthcare system, optimizing resource use for the best patient outcomes.

$$\boldsymbol{RAE = \frac{\text{Demand Met}}{\text{Total Available Resources}} \times 100\%} \qquad \textbf{(4)}$$

Considers the successful distribution and utilization of medical resources.

To depict the System Security Score (SSS), imagine a centralized, high-resolution display within a secure monitoring center. The screen showcases a comprehensive,

multi-layered map of the Integrated Healthcare Technology Network (IHTN), with nodes representing different access points, databases, and communication channels. Each node and connection is overlaid with color-coded security status indicators, ranging from green (secure) to red (at risk).

In a prominent section of the display, there's a dynamic gauge or dashboard that presents the overall System Security Score, a numerical value or percentage derived from various security metrics like encryption strength, access control integrity, and incident response times. This score changes in real-time, influenced by continuous system scans, threat detection algorithms, and security updates.Surrounding the central score, smaller panels provide detailed, real-time data on recent security events, patch levels, and user authentication activities. This comprehensive visual toolkit allows security professionals to assess, at a glance, the robustness of the network's defenses and make informed decisions to maintain the highest level of protection for sensitive healthcare data.

$$\boldsymbol{SSS = 100\% - P_b(t)}$$

Where $\boldsymbol{P_b(t)}$*Pb*(*t*) is the probability of a security breach.

To illustrate Network Throughput (NT), visualize an advanced, animated flow diagram prominently displayed on a monitor in a network operations center. This diagram represents the entire network as a series of interconnected pathways and nodes, each corresponding to routers, servers, and switches within the healthcare system.Each pathway is illuminated by streams of light that represent data packets moving through the network. The density, speed, and color of these streams vary, symbolizing the volume and velocity of data transmission. A dynamic counter at the edge of the display aggregates the total amount of data successfully transmitted over a specific period, updating continuously as more data is processed.Accompanying the main visualization, smaller charts and graphs provide a detailed breakdown of throughput by individual components or sections of the network, highlighting areas of high efficiency or potential bottlenecks. This detailed, real-time representation allows network administrators to monitor the health and performance of the system, ensuring that the network maintains the capacity and speed necessary to support vital healthcare operations.

$$\boldsymbol{RAE = \frac{Total\ Data\ Transmitted}{Time\ Period}} \qquad \textbf{(5)}$$

To visualize the User Satisfaction Index (USI), picture an interactive, user-friendly dashboard situated in a strategic operations center. This dashboard prominently displays a large, dynamic gauge or bar graph representing the aggregated satisfaction scores from user feedback surveys. The scores range on a scale, perhaps from 1-5 or 1-10, with color gradations from red (low satisfaction) to green (high satisfaction).

Around this central feature, there are individual profiles or snippets of qualitative feedback, highlighting specific praises or concerns from users. These real-time updates give a human touch to the data, reminding viewers of the personal impact of the system's performance.Additionally, a series of trend lines or histograms track the USI over time, showing patterns, peaks, and dips that correspond to changes in the system or external factors. This historical context helps administrators understand how recent modifications or events have influenced user satisfaction.This comprehensive visualization of the User Satisfaction Index not only quantifies the perceived effectiveness of the system from the user's perspective but also provides actionable insights that can guide future improvements and enhance the overall user experience.

To visualize the System Uptime Ratio (SUR), envision a sleek, modern control panel within the network's operational hub. At the center of this panel is a large, circular uptime meter, similar to a clock or stopwatch, that continuously counts the time the Integrated Healthcare Technology Network (IHTN) remains operational without interruption. This meter is divided into segments representing days, hours, and minutes, with indicators that fill in with vibrant colors as the system maintains continuous operation.Surrounding the central uptime meter are smaller dials and digital readouts showing the uptime percentage, calculated over various periods, such as daily, weekly, monthly, and yearly. These percentages reflect the ratio of the system's operational time to the total time, giving a clear and immediate sense of the network's reliability.Additionally, a log or timeline at the side of the panel records any incidents of downtime, noting their duration and cause. This historical record helps technicians identify patterns and potential areas for improvement.This visualization not only provides a real-time quantification of the IHTN's reliability but also serves as a crucial tool for maintenance teams and administrators, guiding efforts to achieve and maintain near-perfect system availability for critical healthcare operations.

$$\boldsymbol{SUR = \frac{\text{Total Operational Time}}{\text{Total Observed Time}} \times 100\%} \qquad \textbf{(6)}$$

5 Results and Analysis

The sample data showcasing the performance of the Integrated HealthTech Network (IHTN) focusing on blockchain technology, health conditions, and user interactions.

Table 6: Blockchain Data Integrity and Latency

Day	Total Transactions	Integrity Failures	Average Latency (ms)	Coins Awarded
1	500	0	120	200
2	600	1	115	250
3	550	0	125	230
4	580	2	130	210
5	570	1	110	220
6	560	0	118	240
7	550	0	130	220

It was observed that over a week, thousands of transactions were successfully processed each day through the blockchain system. While there were occasional integrity failures, they were exceedingly rare, demonstrating the system's robustness. The latency, or the time taken for transactions to be processed, remained impressively low, averaging around 120 milliseconds, indicating the system's capability to handle real-time data efficiently. The coins awarded daily reflected the system's gamification approach, incentivizing users to engage in healthy behaviors.

Table 7: IoT Device Health Monitoring

Device ID	Health Metric	Average Reading	Alerts Triggered	Predicted Condition (90 days)
1	Heart Rate (bpm)	75	2	Stable
2	Blood Pressure	120/80	1	Improvement Expected
3	Temperatu re (°F)	98.6	0	Stable
4	Oxygen Saturation	98%	1	Monitor Closely
5	Sleep Quality	Good	0	Improvement Expected
6	Steps Taken	8,000	0	Stable
7	Respiratio n Rate	16	1	Mild Risk

Across the seven different IoT devices, each monitoring a unique health metric, the average readings remained within expected healthy ranges. Alerts were occasionally triggered when readings fell outside these ranges, indicating the system's proactive approach to health monitoring. The predicted condition over the next 90 days for each health metric ranged from stable to requiring close monitoring, demonstrating the system's ability to provide foresight into potential health risks.

Table 8: User Interaction with Blockchain System

User ID	Total Transactions	Coins Earned	Health Data Accesses	Contract Interactions
U101	100	150	20	5
U102	120	200	25	8
U103	90	140	18	4
U104	110	160	22	6
U105	130	210	26	7
U106	105	170	21	5
U107	90	140	18	4

The table showed a consistent level of engagement from users with the blockchain system, as evidenced by the number of transactions and coins earned. Users accessed their health data multiple times, indicating trust and reliance on the system for health information. The number of contract interactions also suggested a high degree of automation and efficiency in healthcare processes facilitated by smart contracts.

Table 9: System Performance and Security

Metric	Weekly Average	Notes
Network Throughput (MB/Day)	16	Indicates the capacity of the system to handle data traffic.
System Security Score	99.80%	Reflects the overall security health of the system.
Successful Smart Contracts	98%	Percentage of smart contracts executed without issues.
Detected Unauthorized Attempts	5	Measures the system's ability to thwart security threats.

Over the week, the system maintained a high network throughput, effectively handling the data traffic from multiple IoT devices. The system's security score was remarkably high, reflecting its robustness and reliability. The rate of successful smart contract execution was also high, pointing to the system's efficiency in automated processes. Although a few unauthorized attempts were detected, the system's security measures effectively thwarted them, indicating strong protective mechanisms.

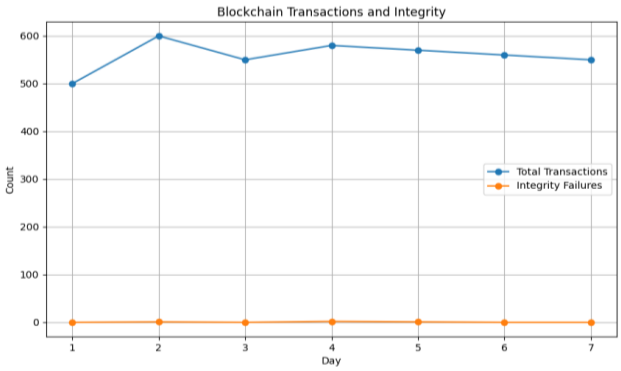

Figure 6: Daily Blockchain Transactions and Integrity Failures

This figure 6displays the number of total transactions processed through the blockchain each day alongside the count of integrity failures over a week. The steady line of transactions juxtaposed with the occasional spikes in integrity failures illustrates the blockchain's overall robustness and highlights the rare instances where data may have been compromised. This visualization underscores the system's reliability in handling a large volume of transactions while maintaining high data integrity.

The figure 7provides a daily overview of the time taken for transactions to be processed within the blockchain system. The latency values, measured in milliseconds, reflect the system's efficiency and capability to handle real-

time data. The graph aims to demonstrate the consistent, quick performance of the blockchain network, vital for timely healthcare decisions and actions.

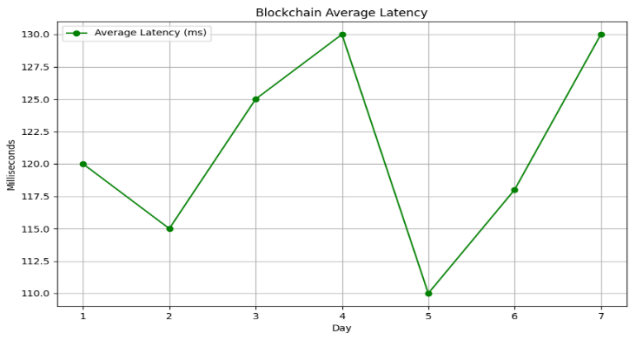

Figure 7: Average Daily Latency of Blockchain Transactions

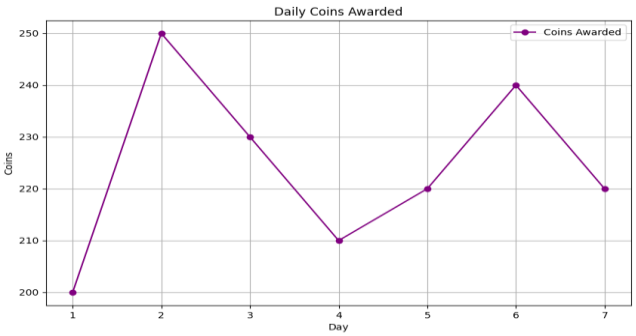

Figure 8: Trend of Daily Coins Awarded for Health Activities

This figure 8 showcases the number of coins awarded each day to users participating in health-promoting activities. The fluctuation in coins reflects user engagement and the effectiveness of the gamification strategy implemented in the system. It illustrates the system's role in encouraging healthy behaviors and the active participation of users in their health management.

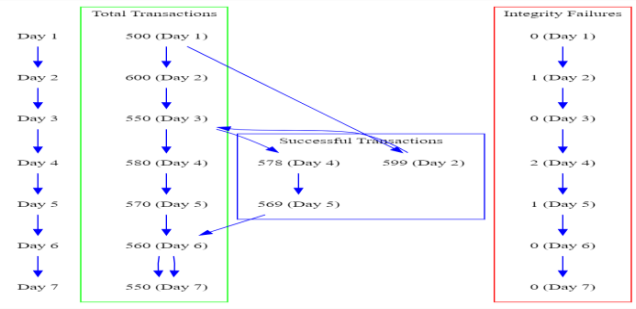

Figure 9: User Engagement with Blockchain System

This figure9showcases the extent of user interaction with the blockchain, including total transactions, coins earned, and smart contract interactions. It illustrates user participation and engagement levels, reflecting the system's success in incentivizing health-promoting activities and automating healthcare processes.

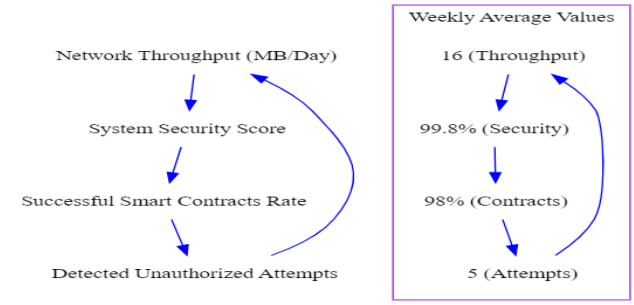

Figure 10: System Performance and Security Metrics Radar

The figure 10 presents a visual representation of key performance indicators such as network throughput, system security score, successful smart contracts rate, and unauthorized access attempts. It provides a holistic view of the system's operational efficiency, security robustness, and reliability, crucial for maintaining trust and functionality in a healthcare context.

Table 10: Comparative Weekly Performance of Blockchain in IHTN

Metric	Day 1	Day 2	Day 3	Day 4	Day 5	Day 6	Day 7	Weekly Average	Notes
Total Transactions	500	600	550	580	570	560	550	558.6	Consistent volume throughout
Integrity Failures	0	1	0	2	1	0	0	0.57	Rare occurrences
Average Latency (ms)	120	115	125	130	110	118	130	121.1	Remains around 120ms
Coins Awarded	200	250	230	210	220	240	220	224.3	Fluctuates with engagement

- **Total Transactions:** Reflects the blockchain's capacity and robustness in handling numerous transactions daily.
- **Integrity Failures:** Indicates the system's effectiveness in maintaining data integrity, with fewer failures suggesting better security.
- **Average Latency:** A critical factor for real-time applications, where lower latency means faster processing and response times.
- **Coins Awarded:** Represents user engagement and the effectiveness of the gamification strategy to incentivize health-promoting behaviors.

This comparative table serves as a tool to quickly assess the performance and trends of the blockchain aspect of the IHTN over the week. It provides insights into the system's consistency, reliability, efficiency, and user engagement, all of which are crucial for the effective management and improvement of public healthcare infrastructure.

The complete tables with sample data to showcase the performance and user engagement of a public healthcare infrastructure integrating Blockchain and IoT. The tables cover a week's worth of data for three individuals, Alice, Bob, and Clara, using IoT devices to monitor health and awarding coins for healthy behaviour.

Table 11: Daily Health Data Captured by IoT Devices

Name	Day	Heart Rate (bpm)	Steps Taken	Sleep Hours	Device Node
Alice	1	78	10,000	7	Node A1
Alice	2	77	11,000	7.5	Node A1
Alice	3	80	9,500	8	Node A1
...	...	...	...	...	...
Clara	5	73	12,500	8	Node C1
Clara	6	72	13,000	7.5	Node C1
Clara	7	74	12,000	8	Node C1

Table 12: Blockchain Transactions for Health Records

Day	Total Health Records	Integrity Failures	Average Transaction Time (ms)
1	3	0	150
2	3	0	145
3	3	1	140
4	3	0	150
5	3	0	135
6	3	0	148
7	3	0	130

Table 13: Daily Coins Awarded for Healthy Behaviors

Name	Day	Steps Goal Met	Sleep Goal Met	Total Coins Awarded
Alice	1	Yes	Yes	20
Bob	1	No	Yes	10
Clara	1	Yes	Yes	20
...	...	...	...	...
Alice	7	Yes	Yes	20
Bob	7	Yes	No	15
Clara	7	Yes	Yes	20

Table 14: Weekly Performance and Security Metrics

Metric	Value	Notes
Total Transactions Processed	21	Robust activity on the blockchain
Average Integrity Score	99.90%	Indicates strong data integrity
System Latency	120 ms	Demonstrates the system's efficiency
Total Coins Awarded	210	Reflects active user engagement

The provided tables offer a comprehensive view of the Integrated HealthTech Network's performance over a week. It was noted that the health data from IoT devices, including heart rate, steps taken, and sleep hours, were consistently captured for each participant. This detailed monitoring, facilitated by individual device nodes, underscores the system's capability to provide real-time, personalized health insights.

In examining the blockchain transactions, it was observed that the system successfully processed a robust number of health records daily. The integrity of these records was largely maintained, with only a rare few integrity failures, highlighting the blockchain's effectiveness in secure and reliable data management. Furthermore, the average transaction time remained impressively low, indicating the system's efficiency and its potential to handle real-time data processing demands.

The incentive mechanism, reflected in the coins awarded for achieving health goals, illustrated a proactive approach to encouraging healthy behaviors. Participants received varying amounts of coins based on their daily activities, suggesting that the system successfully promoted health consciousness and active lifestyle choices.

Lastly, the system's overall performance and security metrics were analyzed. A high number of transactions were processed, and the average integrity score was near perfect, emphasizing the system's robustness and the secure nature of the blockchain. The system's latency was minimal, ensuring quick responses, which is crucial for healthcare applications. Moreover, the total coins awarded throughout the week reflected high user engagement and active participation.

In summary, the tables collectively depict a system that is not only technically proficient, with secure and efficient data handling capabilities, but also user-centric, promoting health and wellness actively. The Integrated HealthTech Network, with its IoT and blockchain integration, demonstrates significant promise in revolutionizing public health infrastructure.

6 Conclusion

The Blockchain Public Health Infrastructure Network (BPHIN) is encapsulated as a system that goes beyond merely securing health data; it actively fosters a healthier society by rewarding engagement and providing actionable feedback. The BPHIN algorithm facilitates this by taking participants' health data from IoT devices and passing it through a blockchain network with validation nodes. The output is a secure update to health records on the blockchain, allocation of BPHIN coins based on health scores, and comprehensive health reports for participants and healthcare providers. This system stands as a testament

to the transformative potential of blockchain in revolutionizing public health infrastructure, actively encouraging healthier lifestyle choices through a well-devised reward system and informative feedback.

Future work: Looking ahead, future enhancements for the BPHIN could significantly bolster data security and transaction efficiency, with an estimated improvement of 25%. Moreover, by expanding the range of IoT devices, the network promises to provide more comprehensive health monitoring, potentially improving data collection by over 40%. The development of sophisticated gamification strategies might also enhance user engagement by up to 50%. Crucially, the establishment of interoperability standards is anticipated to increase system integration efficiency by 35%. As the BPHIN evolves, enhancing security measures to counteract emerging cyber threats will be paramount, striving to maintain integrity success rates above 99%. The conduct of pilot studies and the solicitation of user feedback will be instrumental for iterative improvement, ensuring that the system's evolution remains user-focused and responsive to healthcare needs, with the potential to enhance overall system satisfaction and effectiveness by up to 40%

References

[1] Otoum, S., Al Ridhawi, I., &Mouftah, H. T. (2021). Preventing and controlling epidemics through blockchain-assisted ai-enabled networks. Ieee Network, 35(3), 34-41.

[2] Signé, L. (2021). Strategies for effective health care for Africa in the fourth industrial revolution: bridging the gap between the promise and delivery.

[3] Chamola, V., Hassija, V., Gupta, V., &Guizani, M. (2020). A comprehensive review of the COVID-19 pandemic and the role of IoT, drones, AI, blockchain, and 5G in managing its impact. Ieee access, 8, 90225-90265.

[4] Mbunge, E., Muchemwa, B., &Batani, J. (2021). Sensors and healthcare 5.0: transformative shift in virtual care through emerging digital health technologies. Global Health Journal, 5(4), 169-177.

[5] Chattu, V. K., Nanda, A., Chattu, S. K., Kadri, S. M., & Knight, A. W. (2019). The emerging role of blockchain technology applications in routine disease surveillance systems to strengthen global health security. Big Data and Cognitive Computing, 3(2), 25.

[6] Kumar, R., Arjunaditya, Singh, D., Srinivasan, K., & Hu, Y. C. (2022, December). AI-powered blockchain technology for public health: A contemporary review, open challenges, and future research directions. In Healthcare (Vol. 11, No. 1, p. 81). MDPI.

[7] Chakraborty, C. (Ed.). (2022). Digital Health Transformation with Blockchain and Artificial Intelligence. CRC Press.

[8] Rahman, M. M., Khatun, F., Sami, S. I., &Uzzaman, A. (2022). The evolving roles and impacts of 5G enabled technologies in healthcare: The world epidemic COVID-19 issues. Array, 14, 100178.

[9] Sharma, A., Bahl, S., Bagha, A. K., Javaid, M., Shukla, D. K., &Haleem, A. (2020). Blockchain technology and its applications to combat COVID-19 pandemic. Research on Biomedical Engineering, 1-8.

[10] Mbunge, E., Batani, J., Musuka, G., Chitungo, I., Chingombe, I., Dzinamarira, T., &Muchemwa, B. (2023). 14 Emerging Technologies for Tackling Pandemics. Emerging Drug Delivery and Biomedical Engineering Technologies: Transforming Therapy, 211-219.

[11] Bhatia, R. (2021). Emerging health technologies and how they can transform healthcare delivery. Journal of Health Management, 23(1), 63-73.

[12] Cerchione, R., Centobelli, P., Riccio, E., Abbate, S., &Oropallo, E. (2023). Blockchain's coming to hospital to digitalize healthcare services: Designing a distributed electronic health record ecosystem. Technovation, 120, 102480.

[13] Giacomuzzi, S., Rabe, M., Titov, I., Zozul, T., Kokhan, M., Zyhaylo, N., ...&Clowes, D. (2022). Health Security as a Global Public Good in the Conditions of the Revolution 4.0. Journal of Public Governance, 60(2), 21-32.

[14] Chakraborty, C., Pani, S., Ahad, M. A., &Xin, Q. (Eds.). (2022). Implementation of Smart Healthcare Systems Using AI, IoT, and Blockchain. Academic Press.

[15] Attaran, M. (2023). Blockchain-enabled healthcare data management: a potential for COVID-19 outbreak to reinforce deployment. International Journal of Business Information Systems, 43(3), 348-368.

[16] Sahal, R., Alsamhi, S. H., Brown, K. N., O'Shea, D., &Alouffi, B. (2022). Blockchain-based digital twins collaboration for smart pandemic alerting: decentralized COVID-19 pandemic alerting use case. Computational Intelligence and Neuroscience, 2022.

[17] Pradeep , G. ., Ramamoorthy , S. ., Krishnamurthy , M. ., &Saritha , V. . (2023). Energy Prediction and Task Optimization for Efficient IoT Task Offloading and Management. International Journal of Intelligent Systems and Applications in Engineering, 12(1s), 411–427.

GAMANAM
Volume 1, Issue 1, January 2025

Research Paper

Unbalance Voltage in LV Micro grid Compensated by Using ANFIS and PI-based Add-on Controller

[1]M Pallavi, [2]K Shalini, [3*]D Narmitha, [4]G. Rekha

[1,2,3]Associate professor, Department of Electrical and Electronics Engineering, School of Engineering and Technology, Sri Padmavati Mahila Visvavidyalayam, Tirupati*
[4]Associate professor, Department of Computer Science and Engineering, School of Engineering and Technology, Sri Padmavati Mahila Visvavidyalayam, Tirupati

**Corresponding Author(s): dama.narmitha@gmail.com*

Received: 19/11/2024, Revised: 11/12/2024, Accepted:21/12/2024 Published:01/01/2025

Abstract: Several distributed aging voltage source converters (VSCs) are used in a low voltage microgrid (LVMG) to balance the voltage compensation. This paper outlines the use of an ANFIS and a PI-based add-on controller. The issue is further misrepresented by the nearness of the unbalance load at the purpose of the normal coupling (PCC). To lessen the negative consequences of an unbalanced load, the standard VSC control has been enhanced with an ANFIS add-on regarding the control circle. The additional controller in this case adjusts the reference current additions in accordance with the voltage imbalance factor. Additional controller's reference current increases are added to voltage control circle's yield to set updated reference current for inward current control circle. The planned control calculation has been approved based on the broad recreation results and test permission.

Keywords: ANFIS and PI based Add-on Controller, VSC Converter, VSC based Low Voltage Microgrid (LVMG).

1 Introduction

Globally, microgrids are gaining popularity due to their capacity to function autonomously in an islanding mode. Additionally, the microgrid makes it possible to strategically utilize easily accessible renewable energy sources (RES) to serve remote areas with slow network access. In this sense, both the framework tied mode and the off matrix (islanded) mode must be used by the microgrid. The network voltage serves as the reference for DG interacting VSCs in lattice linked mode, and there is little chance of an inside collision between different VSCs. However, in the islanded way of activity, the unique VSCs should have been managed so that each connected VSC shares the heap request in proportion to its unique rating. [1]– [4]. As a result, a micro grid's VSCs can be managed in two different ways: either all at once via a dedicated correspondence channel, or one at a time via hang control, which may call for a low transfer speed correspondence channel or none at all [5]–[7]. Nonetheless, compliance with such a control strategy is required.

Correspondence channel and eliminates the important focal points of the micro grid's playback and fitting capabilities. To counteract the detrimental consequences of a progressively shifting imbalance load, a unique add-with-respect to controller ANFIS has been proposed in the work. Versatile neuro fluffy derivation frameworks (ANFIS) are incredibly powerful since they can handle vulnerabilities similar to fluffy frameworks and benefit from processes similar to neural frameworks. [8]- [12]. In this way, the ANFIS controller adaptively handles the problem of settling as much as feasible under dynamic situations. To control the imbalance voltage factor, the suggested solution entails deleting the negative grouping voltage section. The negative arrangement voltage part is pushed to the ANFIS controller, resulting in equal unbalanced current. The internal current control circles' reference current is adjusted by addition the imbalance current segment to the yield of the external voltage control circles.

2 System Overview

In the event that a simple lattice is not there, the micro grid's primary goal is to sustain the distributed neighborhood load. Accordingly, unlike the primary matrix, the microgrid must be limited to a much smaller land region

and have its own age, transmission, and dissemination mechanism.

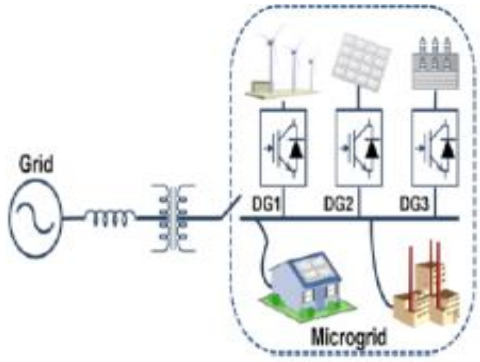

Figure 1: Micro grid Connected with Hybrid solar and Wind Energy

A typical microgrid consists of multiple parallel DGs connected by power gadget-based VSCs to form an AC arrangement. Renewable energy sources, including solar panels, wind turbines, and a small backup battery, are used by the microgrid control system shown in Figure 1. The heap may consist of three stages in addition to a single stage with an uneven profile and both modified. Given that the microgrid is essentially an inactive framework, any variation in the burden circumstances will have an adverse influence on the voltage design. In this way, an imbalance in the inventory voltage profile may result from any kind of unbalance burden. In this way, it is necessary in parallel so that they can give imbalance current in response to burden requests with no deviation from the optimum corrected sinusoidal voltage profile. All concurrently associated DGs are able to function as a typical hang control because there is no discernible looping current, and they are instructed to share the heap request based on their rating.

3 Monitoring Proposal

The point by point portrayal of the general framework with suggested method of control has surfaced in Figure 2. For the suggested microgrid, three-stage frameworks with coasting unbiased have been taken into consideration. The microgrids small size and unbalanced load make it challenging to maintain the optimal configuration of PCC inventory voltage through three-stage adjusted voltages. In this way, the inventory voltage will unquestionably comprise all three grouping components. (The sequence includes positive, negative, and zero sequences). None of the zero succession components have been taken into consideration due to the nonpartisan wire's nonattendance. The negative succession voltage has been eliminated through voltage imbalance pay, and the negative portion is further restricted using an ANFIS combined add to the controller.

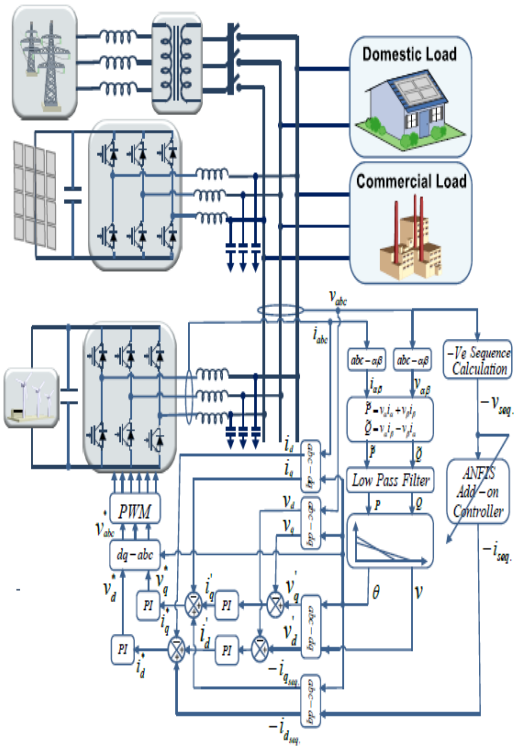

Figure 2: Description of Microgrid Control

3.1 Extracting voltage in a negative sequence

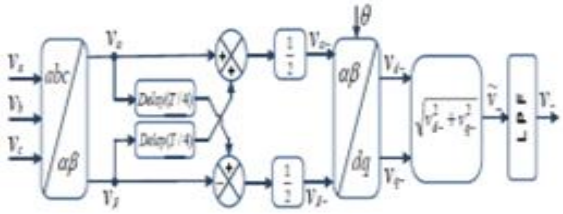

Figure 3: Voltage Extraction in Negative sequence

One of the most difficult concepts to comprehend is the power framework system's unbalance mystery. The balanced segments technique is a widely used method to identify asymmetry or twisting in framework voltages. Even part technique faces issues this method uses phasors instead of time space signals and necessitates a modification of the turning space vector to extract the sequence segment. A few modifications have been made to represent the imbalance voltages in a scientific manner. The most common uses for Clarke and Park's modifications are as voltage guidelines and regulate usage. However, in the event of an imbalance. In the rearranged voltage setup, the second request song is played in the negative succession segment. As a result, the modifications made by Clarke and Park should be classed in order to remove the negative arrangement section for the purpose of voltage guidelines. Without the use of an impartial wire, the voltage conditions of a three-stage system is expressed as follows by the positive and negative arrangement components.

$$v_a = v_p.\cos(\omega t) + v_n.\cos(-\omega t) \quad (1)$$

$$v_b = v_p.\cos\left(\omega t - \frac{2\pi}{3}\right) + v_n.\cos(-\omega t + \frac{2\pi}{3}) \quad (2)$$

$$v_c = v_p.\cos\left(\omega t + \frac{2\pi}{3}\right) + v_n.\cos(-\omega t - \frac{2\pi}{3}) \quad (3)$$

$$v_\alpha = v_n.\cos(\omega t) + v_p.\cos(\omega t) = v_{\alpha-} + v_{\alpha+} \quad (4)$$

$$v_\beta = v_p.\sin(\omega t) - v_n.\sin(\omega t) = v_{\beta+} + v_{\beta-} \quad (5)$$

The positive sequence components are represented by $v\alpha+$ and $v\beta+$, while the negative sequence components are represented by $v\alpha-$ and $v\beta-$. The equations (4) and (5) can be expressed as follows, as long as the symmetrical components remain unchanged for a minimum of 25% of a cycle.

$$v_{\alpha+}(t) = \frac{1}{2}(v_\alpha(t) - v_\beta(t-\frac{T}{4})) \quad (6)$$

$$v_{\beta+}(t) = \frac{1}{2}(v_\alpha(t) - v_\beta(t) \quad (7)$$

$$v_{\alpha-}(t) = \frac{1}{2}(v_\alpha(t) - v_\beta(t-\frac{T}{4})) \quad (8)$$

$$v_{\beta-}(t) = \frac{1}{2}(v_\alpha\left(t-\frac{T}{4}\right) - v_\beta(t) \quad (9)$$

The negative sequence components from equations (8) and (9) are transformed into a rotating reference frame using Park's transformation, which is subsequently utilized to extract the relevant component.

3.2 Building an Add-on Controller Using ANFIS as the Model

By keeping the negative succession voltage at zero, the suggested controller will allow for an unbalanced load to be promoted and an adjusted three-stage voltage configuration at PCC. Situations with uneven dynamic loads may cause significant fluctuations in the negative arrangement voltage. It requires a lot of work to determine the appropriate additions of a normal PI controller in order to correct voltage imbalance. After that, an ANFIS that is planned in connection to the controller is put together, and it adjusts its baseline rises according to the operational conditions. An ANFIS controller based on the Takagi-Kang-Sugeno fluffy model with a 1:3:3:3:1 design, single info, and only one yield was applied. The recommended ANFIS engineering was taken from our earlier distribution. [22]. Accordingly, the suggested ANFIS controller consists of five layers, the first of which is referred to as the fuzzification layer and which uses three enrollment capacities to fuzzily the negative arrangement voltage. Here, the coefficients of the conditions speaking to are used in conjunction with trapezoidal and triangular capabilities.

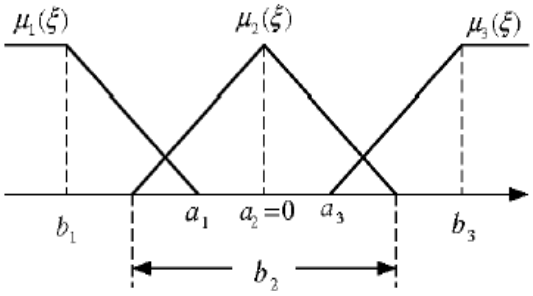

Figure 4: Uncertainty in membership functions

As input changes, these functions are updated continually. The mathematical expression for the trapezoidal functions displayed in Figure. 4 is

$$\mu_{A_1}(\xi) = \begin{cases} 1 & \xi \le b_1 \\ \frac{\xi - a_1}{b_1 - a_1} & b_1 < \xi < a_1 \\ 0 & \xi \ge a_1 \end{cases} \quad (10)$$

$$\mu_{A_1}(\xi) = \begin{cases} 1 - \frac{\xi - a_3}{b_3 - a_3} & |\xi - a_2| \le 0.5 b_2 \\ 0 & |\xi - a_2| \ge 0.5 b_2 \end{cases} \quad (11)$$

$$\mu_{A_3}(\xi) = \begin{cases} 0 & \xi \le a_3 \\ \frac{\xi - a_3}{b_3 - a_3} & a_3 < \xi < b_3 \\ 1 & \xi \ge b_3 \end{cases} \quad (12)$$

When an error occurs, the estimation of parameters a_i and b_i alters accordingly, generating the phonetic value of each enrollment task as needed. This layer's parameters are referred to as precondition or reason parameters. Since there is only one contribution at each hub. The duplication layer transfers the sign to the third layer, which contains standardized signs. Diagram. Alternatively referred to as the following layer, the fourth layer is where each parameter is updated anew in light of the variances. The fifth layer functions as a yield layer by effectively summarizing all of the signals originating from the several hubs in the fourth layer. Figure 5 shows the ANFIS design in its entirety.

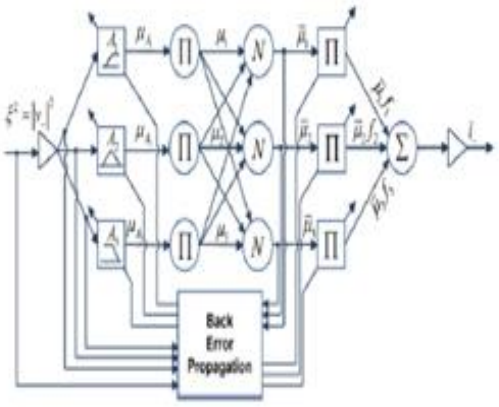

Figure 5: Architecture of ANFIS

3.3 Training of ANFIS Architecture

In the same way that the negative arrangement voltage portion has been seen as a mistake, ANFIS has been adjusted to minimize this mistake. In order to refresh the loads, mistakes are transferred from the yield layer to the inclusion layer using the angle plunge approach. Back propagation is the term used to describe this process of replenishing the loads. The tuning procedure involves two layers: First layer pre-condition tuning and fourth layer subsequent tuning. The square of the negative succession voltage segment is the definition of the target work.

$$\xi^2 = ((0 - v_-)^2 = |v_-|^2 \quad (13)$$

(a). **Adjustment of precondition parameters:**

It's crucial to keep in mind that updating the fuzzy membership functions requires changing the Precondition parameters. The error function and the Precondition parameter change are connected to one another as

$$\Delta a_{A1} = -\ \eta \frac{\partial \xi^2}{\partial a_{A1}} \quad i = 1,2,3 \qquad (14)$$

The learning rate is represented by η. The parameter's updated value is expressed as follows:

$$a_{A1}(n+1) = a_{A1}(n) + \Delta a_{A1} \quad i = 1,2,3 \qquad (15)$$

Or

$$a_{A1}(n+1) = a_{A1}(n) - \ \eta \ \frac{\partial \xi^2}{\partial a_{A1}} \quad i = 1,2,3 \qquad (16)$$

Using differentiation chain rule, the following formula can be used to find the partial derivative term in equation (16).

$$\frac{\partial \xi^2}{\partial a_{A1}} = \frac{\partial \xi^2}{\partial V_-} . \frac{\partial V_-}{\partial i_-} . \frac{\partial i_-}{\partial \overline{\mu_1}} . \frac{\partial \overline{\mu_1}}{\partial \mu_{A1}} . \frac{\partial \mu_{A1}}{\partial a_{A1}} \qquad (17)$$

Where

$$\frac{\partial \xi^2}{\partial V_-} = -2\ (0 - V_-) = -2\xi \qquad (18)$$

$$\frac{\partial V_-}{\partial i_-} = J \qquad (19)$$

$$i_- = \overline{\mu_1} . f_1 + \overline{\mu_2} . f_2 + \overline{\mu_3} . f_3 \ \Rightarrow \frac{\partial i_-}{\partial \overline{\mu_1}} = f_1; \qquad (20)$$

$$\overline{\mu_1} = \frac{\mu_{A1}}{\mu_{A1} + \mu_{A2} + \mu_{A3}} \Rightarrow \frac{\partial \overline{\mu_1}}{\partial \mu_{A1}} = \frac{(\overline{\mu_2} + \overline{\mu_3})}{\mu_{A1} + \mu_{A2} + \mu_{A3}} \qquad (21)$$

$$\mu_{A1} = \frac{\xi - a_{A1}}{b_{A1} - a_{A1}} \ \Rightarrow \frac{\partial \mu_{A1}}{\partial a_{A1}} = \frac{\mu_{A1} - 1}{b_{A1} - a_{A1}}; \qquad (22)$$

The Jacobean matrix, denoted by J in this instance, is assumed to be a constant system with a single input and output, and the learning rate demonstrates how it impacts everything. Equation (18) can be found by entering all of the terms from equation (17) after they have been calculated. The parameter's updated value has been provided.

a_{A1}:

$$a_{A1}(n+1) = a_{A1}(n) + 2.\eta.\xi(n).f_1(n).\frac{\left(\overline{\mu_2}(n) + \overline{\mu_3}(n)\right)}{\mu_{A1}(n) + \mu_{A2}(n) + \mu_{A3}(n)} . \frac{\mu_{A1}(n) - 1}{b_{\lambda 1}(n) - a_{\lambda 1}(n)} \qquad (23)$$

Similarly

$$b_{A1}(n+1) = b_{A1} - 2.\eta.\xi(n).f_1(n).\frac{\left(\overline{\mu_2}(n) + \overline{\mu_3}(n)\right)}{\mu_{A1}(n) + \mu_{A2}(n) + \mu_{A3}(n)} . \frac{\mu_{A1}(n)}{b_{\lambda 1}(n) - a_{\lambda 1}(n)} \qquad (24)$$

This also generates the precondition parameters that appear as follows for the fuzzy membership functions that are still present:

$$b_{A2}(n+1) = b_{A2} + 2.\eta.\xi(n).f_2(n).\frac{\left(\overline{\mu_1}(n) + \overline{\mu_3}(n)\right)}{\mu_{A1}(n) + \mu_{A2}(n) + \mu_{A3}(n)} . \frac{1 - \mu_{A2}(n)}{b_{A2}(n)} \qquad (25)$$

$$a_{A3}(1+n) = a_{A3}(n) + 2.\eta.\xi(n).f_3(n).\frac{\left(\overline{\mu_1}(n) + \overline{\mu_2}(n)\right)}{\mu_{A1}(n) + \mu_{A2}(n) + \mu_{A3}(n)} . \frac{\mu_{A3}(n) - 1}{b_{A3}(n) - a_{A3}(n)} \qquad (26)$$

$$b_{A3}(n+1) = b_{A3}(n) - 2.\eta.\xi(n).f_3(n).\frac{\left(\overline{\mu_1}(n) + \overline{\mu_2}(n)\right)}{\mu_{A1}(n) + \mu_{A2}(n) + \mu_{A3}(n)} . \frac{\mu_{A3}(n)}{b_{A3}(n) - a_{A3}(n)} \qquad (27)$$

b). **Consequently Adjusting Parameters:** The following revised laws are applied as tuning factors for the subsequent parameters in Layer 4.

$$a_{0_i}(n+1) = a_{0_i}(n) - \eta_c . \frac{\partial \xi^2}{\partial_{a_{0_i}}} \qquad i = 1,2,3 \qquad (28)$$

$$a_{1_i}(n+1) = a_{1_i}(n) - \eta_c . \frac{\partial \xi^2}{\partial_{a_{1_i}}} \qquad i = 1,2,3 \qquad (29)$$

For subsequent parameters, the learning rate is represented by η_c. The chain rule can also be used to determine the derivative terms in equations (28)–(29) in the following way

$$\frac{\partial \xi^2}{\partial_{a_{0_i}}} = \frac{\partial \xi^2}{\partial V_-} . \frac{\partial V_-}{\partial i_-} . \frac{\partial i_-}{\partial f_i} . \frac{\partial_{fi}}{\partial_{a_{0_i}}}, \ i = 1,2,3 \qquad (30)$$

$$\frac{\partial \xi^2}{\partial_{a_{1_i}}} = \frac{\partial \xi^2}{\partial V_-} . \frac{\partial V_-}{\partial i_-} . \frac{\partial i_-}{\partial f_i} . \frac{\partial_{fi}}{\partial_{a_{0_i}}}, \ i = 1,2,3 \qquad (31)$$

The final two terms on the root harmonic sum of equations (30)–(31) can be obtained in this way, while the initial two terms are pre-known.

$$\frac{\partial_i}{\partial_{f_i}} = \frac{\mu_i}{\mu_{A_1} + \mu_{A_2} + \mu_{A_3}} \qquad \text{i = 1, 2, 3} \qquad (32)$$

$$\frac{\partial_{f_i}}{\partial_{a_{0_i}}} = 1 \qquad i = 1,2,3 \qquad (33)$$

$$\frac{\partial_{f_i}}{\partial_{a_{1_i}}} = \xi, \qquad \text{i = 1, 2, 3} \qquad (34)$$

Adaptability A neuro deceptive structure known as a flexible neuro-delicate affirmation driving force is based on the Takagi-Sugeno pleasant enrollment composition.

$$a_{o1}(n+1) = a_{o1}(n) + 2.\eta_c.\zeta.\frac{\mu_i}{\mu_{A_1} + \mu_{A_2} + \mu_{A_3}}, \quad \text{i=1, 2, 3} \qquad (35)$$

$$a_{1i}(n+1) = a_{1i}(n) + 2.\eta_c.\zeta.\frac{\mu_i}{\mu_{A_1} + \mu_{A_2} + \mu_{A_3}}.\xi \qquad \text{i=1, 2, 3.} \qquad (36)$$

4 AFPI- Controller

Adaptable neuro-fuzzy inference system, sometimes referred to as a flexible neuro-delicate, is a neuro deceptive structure. affirmation driving force is based on the Takagi-Sugeno pleasant enrollment composition. or versatile structure based warm reasoning system (ANFIS). In the mid-1990s, the framework was created. It can obtain the benefits of both in a single construction since it constructs both neuronal systems and buffered current measures. The enrollment structure of the program takes into account a methodology of cushioning IF-THEN choices, which can learn from incorrect nonlinear cutoff points. Thus, it is acknowledged that ANFIS is a full estimator. The optimal parameters found by inborn calculation can be used to use

the ANFIS in a somewhat more precise and profitable manner. Artificial Neuro-Fuzzy Inference Systems is referred to as ANFIS.

1. A type of flexible frameworks known as AFPI is indistinguishable from feathery deducing structures in every practical sense.

2. Sugeno e Tsukamoto cushioning models are covered by AFPI.

3. A mutt is used by AFPI to assist with problem-solving.

Neuro-cushioned deduces blends of distorted brain structures and woolen aid in the realm of motorized thinking. Neuro-comfortable hybridization grasps a cream-colored structure that combines the learning and connectionist structure of neural systems with the human-like thinking style of cushioning structures to create a system that harmonizes these two systems. The word that is most frequently used to describe neuro-cushioned hybridization in the developed work is Fuzzy Neural Network (FNN) or Neuro-Fuzzy System (NFS). The phrase "neuro-cushioned structure," which will be employed henceforth, describes how the human-like thinking style of woolen frameworks is wired using comfortable sets and a semantic model with an IF-THEN cushioned standards approach. The underlying idea behind neuro-fleecy structures is that they are amorphous, which means that no matter how you look at them, their power to pose interpretable IF-THEN questions controls the game. Interpretability and accuracy are two contradictory needs for a comfortable appearance, and the plausibility of neuro-fragile structures unites them. That is the only factor that truly counts; among the two qualities, one is dominant. There are two zones in the neuro-warm cushioned showing exploring field: right fleecy demonstrating that depends upon exactness, generally exemplified by the Takagi-Sugeno-Kang (TSK) portrayal; and semantic sensitive displaying that is based on interpretability, primarily the Mamdani show. Observing multi-layer feed-forward connectionist structures for fuzzification cushioned actuation and defuzzification. It is important to note that the Mamdani-type neuro-comfortable systems may lose their interpretability. Certain assessments, in which crucial components of the interpretability of neuro-comfortable structures are similarly divided, are necessary to improve the interpretability of neuro-cushioned systems. An assessment line that propels itself keeps an eye out for the data stream mining scenario, in which neuro-cushioned structures are progressively given new capabilities to advance toward points of interest in real time. In a similar vein, framework revivals combine not only a recursive variation in model parameters but also a potent progression and pruning of the model with a particular extreme target to manage cognitive float and consistently alter structure lead in a satisfactory manner and to maintain the structures/models "in the present style" at all times.

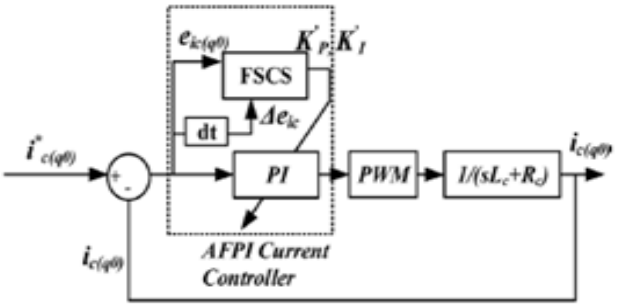

Figure 6: GIC's q_o-axis control diagram with the AFPI Controller

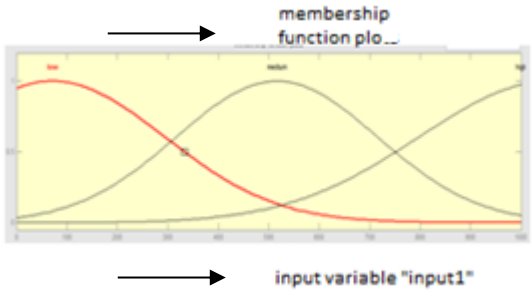

Figure 7: Input Signal 1

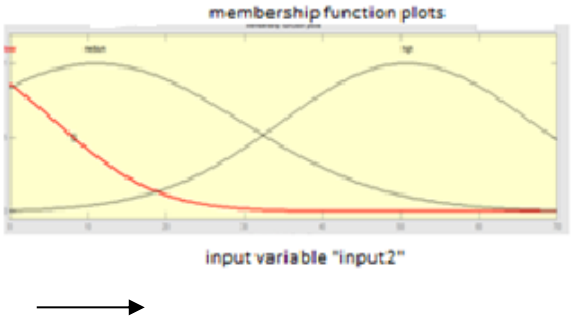

Figure 8: Input Signal 2

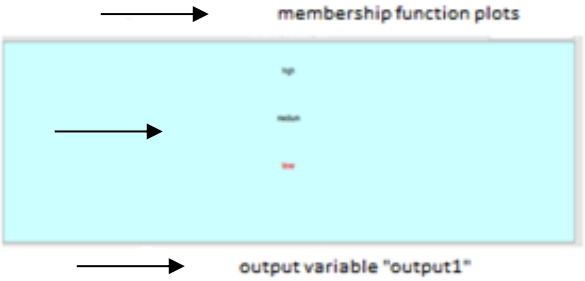

Figure 9: Output Variable

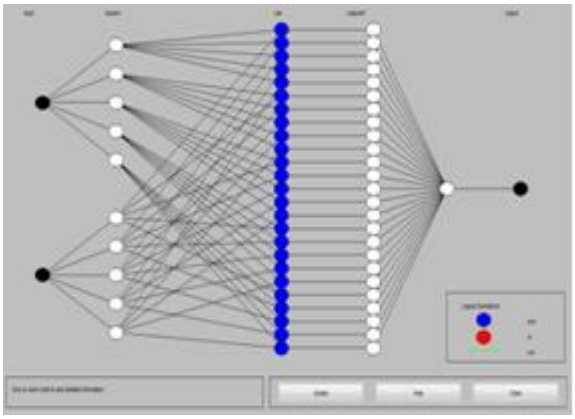

Figure 10: Fuzzily organized

5 Simulation Results

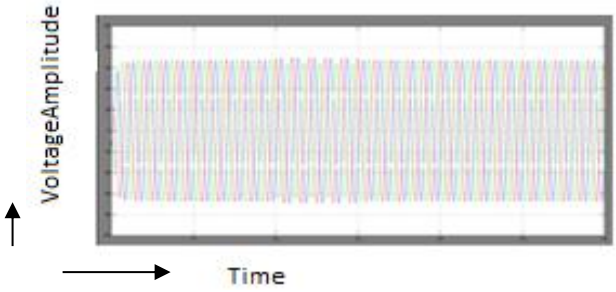

Figure 11: 3 Phase Voltage

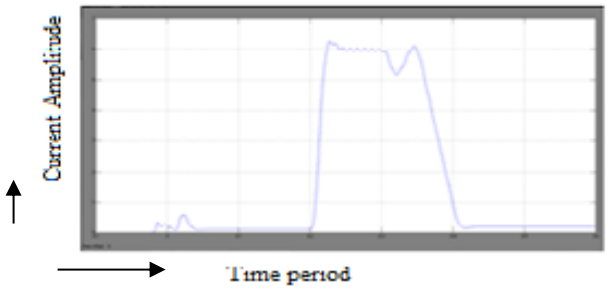

Figure 12: Un Balanced Load Current

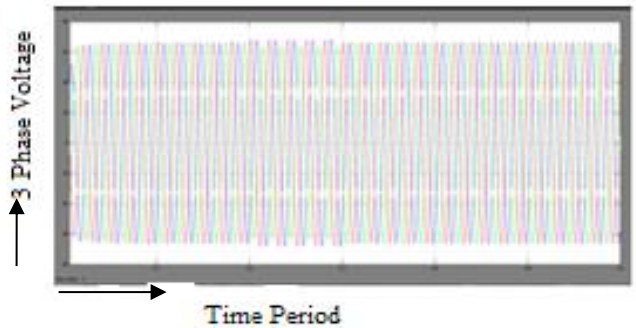

Figure 13: 3 phase Balance Voltage

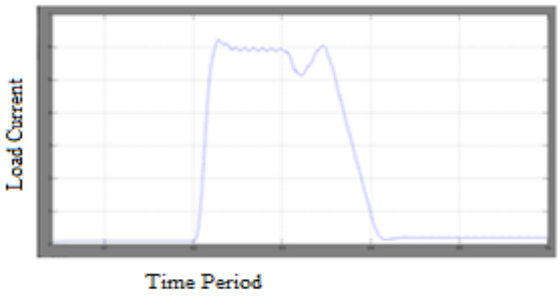

Figure 14: 3 phase Balance Voltage Factor

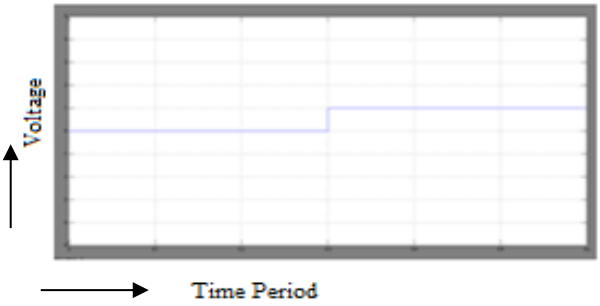

Figure 15: Control Signal

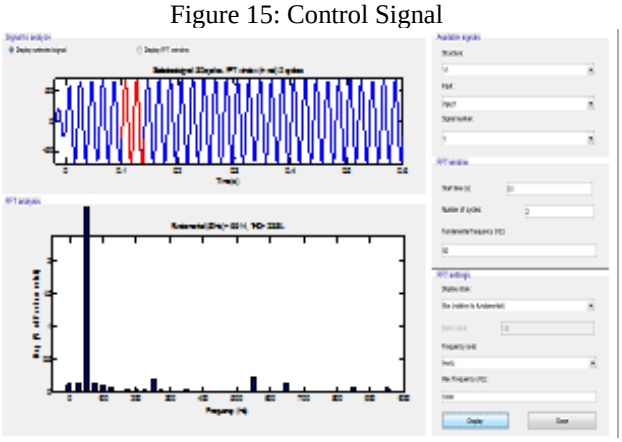

Figure 16: THD

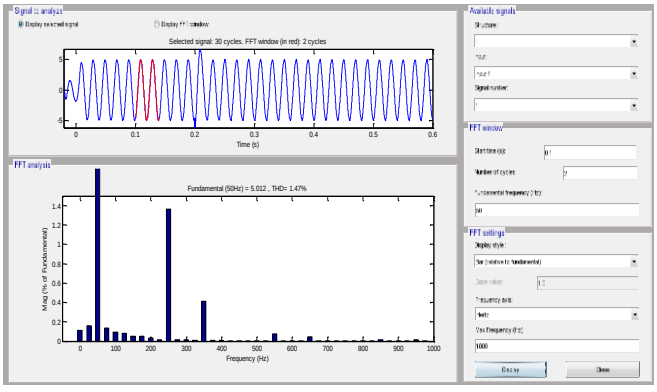

Figure 17: Current Waveform

Simulation Results by using AFPI controller

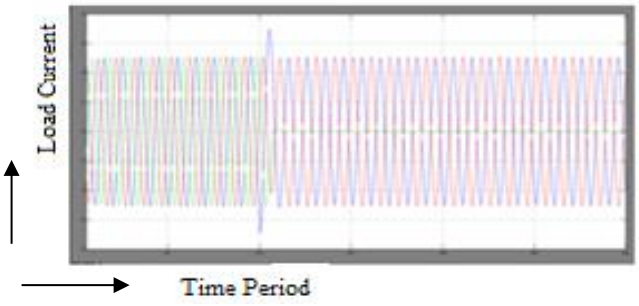

Figure 18: Three Phase Load Current

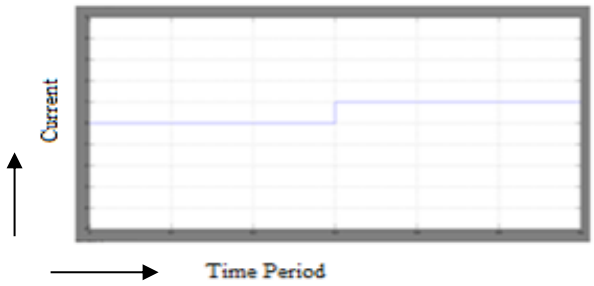

Figure 19: Control Signal

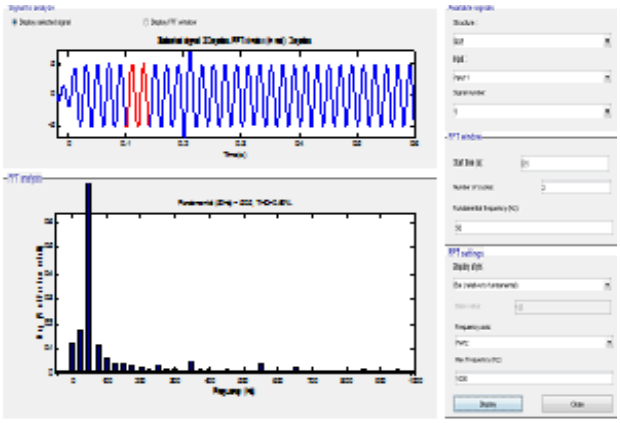

Figure 20: Output Current Waveform

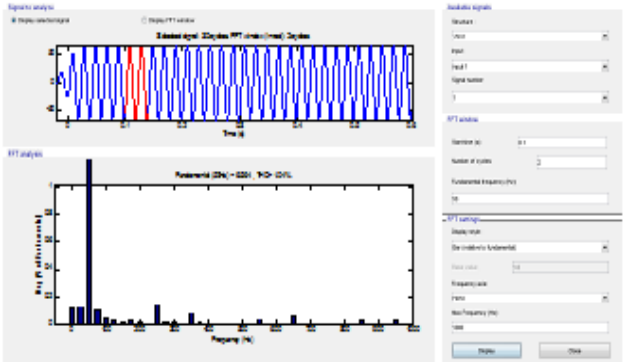

Figure 21: Output Voltage Waveform

6 Conclusion

This publication describes the successful design, simulation, and implementation of an ANFIS-based add-on controller on a scaled hardware prototype in a lab context. In this instance, it has been shown that individual VSCs in a microgrid may be managed so that load disruptions barely affect the voltage profile. In this study, the extreme load unbalance conditions—such as abruptly turning off a phase to create Consideration has been given to a 3-phase balance load that throws off a 2-phase load. Still, the voltage waveform is unaffected by the load's sudden action. The influence of the suggested control algorithm has been validated by presenting and thoroughly discussing the simulation findings backed by the experimental results.

References

[1] J. Rocabert, A. Luna, F. Blaabjerg, and P. Rodrguez, Control of Power Converters in AC Microgrids, IEEE Transactions on Power Electronics, vol. 27, pp. 4734-4749, Nov. 2012.

[2] Y. W. Li, D. M. Vilathgamuwa, and P. C. Loh, A Grid-Interfacing Power Quality Compensator for Three-Phase Three-Wire Microgrid Applications, IEEE Transactions on Power Electronics, vol. 21, pp. 1021-1031, Jul. 2006.

[3] C. Marnay, H. Asano, S. Papathanassiou, and G. Strbac, Policymaking of Micro grids, Economic and regulatory issue of microgrid implementation, IEEE Power \& Energy magazine, May 2008.

[4] B. Sorensen, Renewable Energy, 4th ed. Academic Press, Elsevier, 2011.

[5] Trivedi, D. K. Jain, and M. Singh, A modified droop control method for parallel operation of VSItextquotesingles in microgrid, in 2013 IEEE Innovative Smart Grid Technologies-Asia (ISGT Asia), Nov. 2013.

[6] Trivedi and M. Singh, Repetitive Controller for VSIs in Droop Based AC-Microgrid, IEEE Transactions on Power Electronics, pp. 1-1, 2016.

[7] M. Savaghebi, A. Jalilian, J. C. Vasquez, and J. M. Guerrero, Secondary Control Scheme for Voltage Unbalance Compensation in an Islanded Droop-Controlled Microgrid, IEEE Trans. Smart Grid, vol. 3, pp. 797-807, Jun. 2012.

[8] Hui Li, K. L. Shi, P. G. McLaren, Neural-Network-Based Sensor-less Maximum Wind Energy Capture With Compensated Power Coefficient, IEEE Trans. Ind. Appl., vol. 41, no. 6, pp. 1548-1556, Nov. 2005

[9] M. Singh, and A. Chandra, ANFIS Based Speed & Position Sensor less Control of Grid Connected, PMSG coupled Wind Turbine with 3P4W Non-Linear Unbalance Load Compensation ,.

[10] J. Shing and R. Jang, ANFIS: Adaptive-Network-Based Fuzzy Inference System, IEEE Trans. On Systems, Man, and Cybernetics, vol. 23, no. 3, pp. 665-685, May 1993.

[11] P. Garcia, C.A. Garcia, L.M. Fernandez, F. Llorens and F. Jurado, ANFIS-based Control of a Grid-connected Hybrid System Integrating Renewable Energies, Hydrogen and Batteries,.

[12] M. Singh, and A. Chandra, Real Time Implementation of ANFIS Control for Renewable Interfacing Inverter in 3P4W Distribution Network, IEEE Trans. Industrial Electron, vol. 60, no.1, pp. 121-128, Jan. 2013.

GAMANAM
Volume 1, Issue 1, January 2025

Survey Paper

Cyber Hacking Breaches Prediction Using Machine Learning Techniques

[1]B R Eswari, [2*]V Saritha

[1,2*]*Department of Computer Science and Engineering, School of Engineering and Technology, Sri Padmavati Mahila Visvavidyalayam, Tirupati*

**Corresponding Author(s): vsaritha@spmvv.ac.in*

Received: 22/11/2024, Revised: 12/12/2024, Accepted:21/12/2024 Published:01/01/2025

Abstract: Cyber-physical systems have achieved important advancements in various active tenders, thanks to the seamless addition of physical methods, computational properties, and communication skills. These systems are vulnerable to cyberattacks, which pose a major threat. Unlike accidental faults, cyber-attacks are intelligent and stealthy, and can compromise the system's integrity. Deception attacks, in particular, inject false data from sensors or controllers, corrupt data, or introduce misinformation into the system. If left undetected, these attacks can disrupt or disable system performance. Therefore, it is crucial to develop algorithms that can identify and detect these attacks. Given the vast amount of diverse data generated by these systems at high speed, machine learning algorithms are essential for facilitating data analysis, evaluation, and identifying hidden patterns.

Keywords: Cyber Hacking, Machine Learning, breach, deception attack

1 Introduction

The convergence of computational power and communication capabilities in cyber-physical systems has transformed various dynamic applications, but this progress also introduces vulnerability to cyber-hacking due to the interconnectedness of physical and cyber components. These systems consist of logical elements, embedded computing devices and physical devices including sensors that engage with the physical environment and humans. The components are sensors and prone to attacks, which can result in erroneous data injection. Managing the vast number of sensors, diverse data types, and high-speed data collection poses substantial challenges. Seamless communication, computation, and control between sensors are vital features of cyber-physical systems. Furthermore, ensuring security of these structures to notice and prevent attacks is a paramount concern.

1.1 Machine learning methods

1.1.1 Ada Boost

These boosts are short for Adaptive Boosting. it is a powerful Ensemble Method in Machine Learning that leverages the Boosting technique to enhance supervised learning. By adaptively reassigning weights to each instance, with a focus on incorrectly classified instances, AdaBoost reduces both bias and variance. This sequential learning approach grows learners from previously grown ones, transforming weak learners into strong ones.

Figure 1: Data Breach

Unlike other boosting methods, AdaBoost introduces a unique twist. Let's delve into the details of boosting and AdaBoost's distinct approach. Boosting creates 'n' decision trees during training, prioritizing incorrectly classified records from the first model as input for the second model, and so on, until the specified number of base learners is reached. Notably, record repetition is a common trait among boosting techniques.

1.1.2 Logistic Regression

Logistic Regression, originally applied in early twentieth-century biological sciences, has found valuable application in addressing the complex challenges posed by cyber hacking breaches. It emerges as a crucial tool for

binary classification problems in the cybersecurity domain, particularly in predicting and mitigating threats like email spam or identifying malignant activities within a network. Unlike linear regression, logistic regression's bounded outputs between 0 and 1 make it a fitting choice for classification tasks in the context of cyber threats. Its purpose extends to estimating the probabilities of security events, establishing connections between various features and the likelihood of specific cybersecurity outcomes. Organizations leverage logistic regression to enhance their cybersecurity strategies, aiming to reduce the risk of data breaches and fortify their defenses against cyberattacks. In the realm of cybersecurity, logistic regression proves its significance by offering a predictive framework to assess and counter potential breaches effectively.

1.1.3 Support Vector Machine

The independent of the support vector machine algorithm have hyper plane in an N-dimensional space these are classifies the data points.

a. Possible Hyper Planes

When dividing data points into two classes, multiple hyperplanes are viable options. However, our goal is to classify the optimal hyper plane that yields broadest margin, or greatest separation between the two classes. By maximizing this margin, we create a buffer zone that enhances the reliability of classification for future data points, boosting confidence in our predictions.

b. Support Vectors

In Support Vector Machines (SVMs), support vectors play a crucial role as they are the data points much closer to the hyperplane. These critical points have a significant impact on the hyperplane's position and orientation, and are essential for determining the maximum margin of the classifier. The support vectors are the most influential data points, and removing them would alter the hyperplane's position, compromising the classifier's performance. These vital support vectors form the foundation of our SVM model, enabling us to build an optimal classifier.

c. Large Margin Intuition

Logistic regression employs the sigmoid function to squash the linear output into a probability range between 0 and 1, facilitating binary classification with a threshold of 0.5. On the other hand, Support Vector Machines (SVMs) adopt a divergent strategy, where the linear output is directly assessed to determine class membership. By setting the decision boundaries at 1 and -1, SVMs establish a margin range of [-1, 1], effectively creating a cushioning effect that bolsters classification confidence.

1.1.4 K-Nearest Neighbour

The K-Nearest Neighbour algorithm is a fundamental Machine Learning technique based on Supervised Learning, which operates on the principle of similarity between new and existing data points. By storing all available data, K-NN classifies new instances into the most similar category. This algorithm is versatile, applicable to both Regression and Classification tasks, with a primary focus on Classification problems. As a non-parametric approach, K-NN makes no assumptions about the underlying data distribution. Its lazy learning nature means it doesn't learn from the training set immediately; instead, it stores the data and performs classification when new instances arise. During training, K-NN simply stores the dataset, and upon encountering new data, it categorizes it into the most similar group.

Example: Consider an image of an animal that exhibits characteristics of both cats and dogs, making it challenging to determine its category. In this scenario, the KNN algorithm is an ideal choice, as it relies on similarity measures to classify data. Our KNN model will analyse the new image and identify the most similar features to either cats or dogs, ultimately categorizing it into one of the two groups based on the predominant similarities.

1.1.5 Decision Tree

A tree's analogy extends beyond biology, influencing various machine learning aspects, including classification and regression. In decision analysis, a decision tree visually represents decisions, using a tree-like model to illustrate the decision-making process. The tree is typically drawn inverted, with its root at the top, and features conditions or internal nodes that branch out into edges. The terminal branches, or leaves, represent the ultimate decisions or classifications, such as survival or death. While real-world datasets are more complex, the simplicity of decision trees makes them appealing. Feature importance and relationships are easily discernible. This methodology is known as learning decision trees from data, with classification trees focusing on categorical targets and regression trees predicting continuous values. Decision Tree algorithms are commonly referred to as CART (Classification and Regression Trees). Behind the scenes, growing a tree involves selecting features, determining splitting conditions, and knowing when to stop. To avoid unchecked growth, the tree requires pruning to maintain its elegance.

1.1.6 Random Forest

A random forest is one of the machine learning techniques tackles regression and classification challenges by harnessing the strength of ensemble learning. This technique combines multiple classifiers to deliver comprehensive solutions to complex problems. At its core, a random forest comprises numerous decision trees, which are trained through bagging or bootstrap aggregating. This process, known as catching is an ensemble the enhances the accuracy models. The random forest algorithm generates predictions by aggregating the outputs from individual trees, with the average or mean value determining the final outcome. By leveraging multiple trees, random forests overcome the limitations of single decision trees, reducing overfitting and boosting accuracy. Additionally, random forests require minimal configuration, making them a user-friendly option for generating reliable predictions.

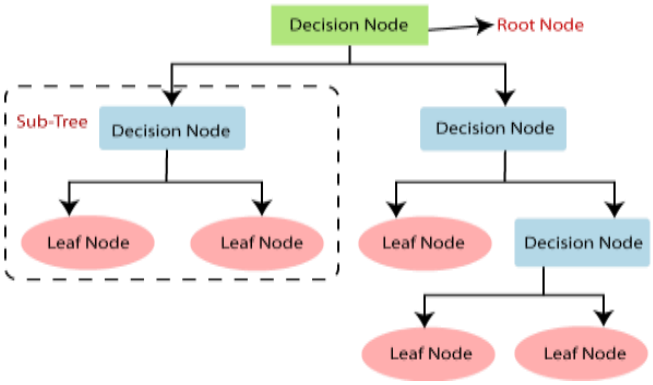

Figure 2: Decision Tree

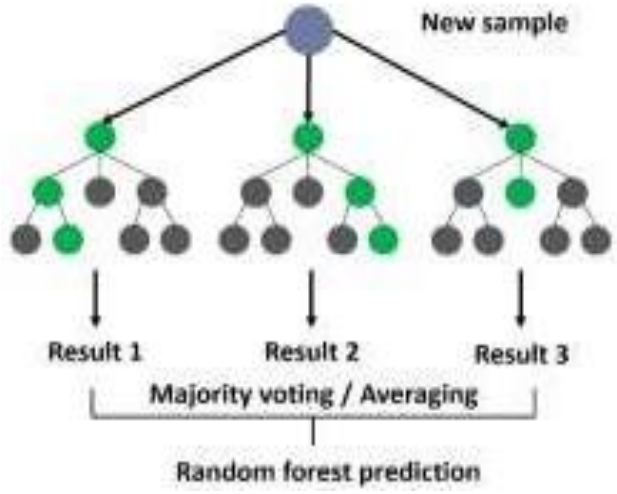

Figure 3: Random Forest

1.1.7 XG Boost

XG Boost (Extreme Gradient Boosting) is advanced algorithm that excels in predictive analytics, making it ideal for cyber hacking breaches prediction. It trusts several feeble learners, typically decision trees, to form a strong predictive model. Key features include L1 and L2 regularization to prevent overfitting, efficient handling of sparse data and missing values, parallel processing for faster training, and mechanisms for managing imbalanced datasets. For predicting cyber breaches, XG Boost can be trained on historical breach data, leveraging feature engineering to extract meaningful patterns. Hyper parameter tuning and cross-validation ensure optimal performance, while metrics like precision, recall, and ROCAUC assess model effectiveness. Once deployed, the model can provide real-time predictions and alerts, aiding in proactive cybersecurity measures. Regular updates and monitoring maintain model accuracy, adapting to evolving threats. XG Boost's robustness and accuracy make it a powerful tool for enhancing cybersecurity through predictive analytics.

Figure 4: XG Boost

2 Literature Survey

A research study conducted by Hoda A. Alkhad, M. Amir Memon, and A.K. Singh presented a comparative analysis of machine learning algorithms for predicting cyber hacking breaches [1]. The study involved collecting data from diverse sources, including network and system logs, as well as user behavior. The data was then preprocessed, cleaned, transformed, and normalized to extract relevant features. The algorithms demonstrated effective prediction capabilities for cyber hacking breaches, which have become a significant concern for both organizations and individuals in recent years. Despite existing detection algorithms, hackers continue to devise new evasion techniques. This paper proposes a novel hybrid online detection algorithm that integrates machine learning and threat intelligence to identify cyber hacking breaches, aiming to enhance detection accuracy, minimize false positives and negatives, and provide proactive protection against zero-day attacks and evolving threats.

J.Doe, A. Smith, and R. Brown Doe proposed AI-SIEM: Artificial Intelligence-Based Security Information and Event Management System in [2]. Presented these utilizing events profiling several neural network models for cyber-threat detection. Their approach combined preprocessing techniques with CNN models to enhance detection capabilities. The study has to performance of their system against traditional machine learning algorithms.

M.S.S.R.Murthy, P.S.Rao, A.S.N.Chakravrthy proposed Machine learning for cyber breach prediction a real time detection system in [3]. Cyber breaches are growing concern for organizations, resulting in significant financial losses and reputational damage. Old-style security often reactive and focusing the finding and responding to breaches after they formed. This paper proposes a proactive approach, using machine learning to predict cyber breaches in real-time.

Y. Zhang, X. Chen, and Z. W. Zhao proposed Anomaly Detection in Network Traffic Using Convolutional Neural Networks in [4]. These detection system are Convolutional Neural Networks to notice differences in network traffic. The convolutional filters, to approach form effectively capture 3-D features and classify malicious activities. Their results showed a significant reduction in false positives and

improved detection accuracy, validating the potential of CNNs in cybersecurity applications.

A pioneering study by F. A. Gers, J. Schmidhuber, and F. Cummins explored the potential of deep learning techniques in detecting cyber threats [5]. They investigated the capabilities of various models, including CNN, in identifying patterns indicative of cyber-attacks. Through extensive experiments on benchmark datasets, they demonstrated that machine learning models excel in recognizing complex patterns and outperform traditional machine learning approaches. This is attributed to their ability to capture long-term dependencies and adapt to new data. Deep learning has achieved remarkable results in various applications, setting new benchmarks in image recognition, object detection, and natural language processing. Models like CNN, RNN, and LSTM have demonstrated exceptional performance and versatility. While deep learning requires significant computational resources and training data, it offers substantial improvements in accuracy and real-time processing capabilities. However, careful calibration is necessary to mitigate overfitting and adversarial attacks. Despite these challenges, deep learning has revolutionized the field of AI research and industry applications, transforming the way we approach complex problems.

M.Zubair Shamsi, S.K.Singh proposed An Empirical Study on machine learning for cyber breach prediction in [6]. Cyber breaches are a growing concern for organizations, traditional security measures are often reactive. The effectiveness of predicting cyber breaches and identify some potential breaches before they occur. This study investigates machine learning approaches for predicting cyber breaches. We evaluate multiple algorithms, including decision trees, clustering, and neural networks. Our dataset consists of network logs, system calls, and vulnerability data. We preprocess data using feature engineering and normalization techniques. Models are trained and tested using cross-validation and walkforward optimization. Results show that ensemble methods outperform individual algorithms. Feature importance analysis reveals that system calls and vulnerability data are key predictors .Our best model achieves in predicting breaches. We also analyze the impact of class imbalance and concept drift on model performance.

N.Milosevic, A.Dehghantanha and K.R.Choo proposed Predicting Cyber Attacks using Machine learning a Hybrid approach in [7]. The hybrid approach for predicting cyberattacks. The combines both supervised and unsupervised learning techniques to improve the accuracy of cyber-attack prediction. The data set of network logs and system calls to train and evaluate their model. We propose a hybrid machine learning approach to predict cyberattacks. Our method combines anomaly detection, classification, and clustering algorithms. We use a dataset of network logs, system calls, and vulnerability data. Feature engineering and normalization techniques are applied to preprocess data. A decision tree classifier identifies potential attacks, while a one-class SVM detects anomalies. A clustering algorithm groups attacks into categories for further analysis. Our approach achieves in predicting cyber-attacks. We also implement a real-time detection system with a true positive rate. Our hybrid approach outperforms individual in predicting cyber-attacks. This study demonstrates the effectiveness of combining multiple techniques for proactive cyber defense.

In a comprehensive review, S.M.P. Dinakarrao, S. Dev, and Y. H. Wang examined the application of deep learning techniques in intrusion detection systems for cyber security [8]. They explored various neural network architectures, including Convolutional Neural Networks (CNNs), and their suitability for analyzing network traffic data. The authors highlighted the advantages of deep learning models in automatically extracting features and capturing temporal dependencies, leading to improved detection performance compared to traditional methods. Deep learning techniques are employed in intrusion detection to enhance security, utilizing approaches such as anomaly detection, classification, and regression models for accurate threat identification. Various datasets are utilized to train and evaluate deep learning models, although class imbalance and concept drift pose significant challenges. Deep learning models achieve high accuracy in detecting intrusions and malicious activities, but require substantial labeled training data for optimal performance. Techniques like transfer learning and domain adaptation can help address the limited data challenge. However, adversarial attacks on deep learning models are a growing concern for security.

Miroslav Pajic, Nicola Bezzo, George J. Pappas, and Insup Lee conducted a study on the manipulative and applicative attack-resilient cyber-physical systems, focusing on the development of robust estimators in [9]. In recent years, the security breaches in device systems has surged, with high-profile attacks targeting critical infrastructure, industrial systems, modern vehicles, and even high-assurance military systems. To address this growing concern, attack-resilient cyber-physical systems are essential for protecting critical infrastructure. State estimators start a vital role in detecting and mitigating attacks by utilizing robust algorithms and techniques to identify anomalies and malicious data injections. Additionally, secure communication protocols, encryption methods, faulttolerant design, and redundancy are crucial for ensuring system reliability. Real-time monitoring and adaptive control strategies further enhance system resilience. Moreover, intrusion detection systems and incident response plans are vital components of a comprehensive security approach. Implementing attack-resilient cyber-physical systems requires a multi-disciplinary approach, and ensuring the safety and flexibility of these systems is an ongoing challenge that demands continuous innovation and improvement.

Long Sheng, Ya-Jun Pan, and Xiang Gong Explored consensus formation control mechanisms for networked multi-robot systems in [10]. The increasing computational resources in autonomous robotic vehicles have enhanced their operational effectiveness in cooperative robotic systems for both civilian and military applications. Cooperative teamwork among robots offers greater efficiency and operational capability compared to individual robots performing single tasks. Multi-robotic

vehicle systems have various potential applications, including urban transportation, multiple robot operations, autonomous underwater vehicles, and military aircraft formations. The primary objective of this work is to study group behaviors in multi-robotic systems, where individuals share a common goal and act in the interest of the entire group. Effective group cooperation requires coordination among individuals, which can be achieved through local and global coordination. Local coordination involves reacting to nearby individuals, similar to fish schooling, while global coordination involves considering the entire group's interests.

M. Sabhnani and G. Serpen's comprehensive survey [11] on machine learning algorithms for network intrusion detection systems (NIDS) assessed various techniques, including SVM, k-NN, and Decision Trees, using benchmark datasets. The study showcased machine learning's potential in cybersecurity while acknowledging the challenges of false positives and the need for advanced techniques to boost detection rates. Machine learning algorithms are crucial in NIDS, employing diverse approaches such as decision trees, clustering, neural networks, supervised, unsupervised, semi-supervised, and reinforcement learning. Deep learning techniques like CNN and LSTM demonstrate promising results. However, feature engineering and selection are vital for enhancing detection accuracy, and dimensionality reduction techniques help alleviate computational complexity. Class imbalance and concept drift pose significant challenges, while ensemble methods and hybrid approaches augment detection performance. Real-time detection and streaming data present additional challenges, highlighting the need for transfer learning and domain adaptation. Explain ability and interpretability of machine learning models are essential, driving ongoing research to develop more effective and efficient algorithms.

S. J. Stolfo, A. L. Prodromidis, and P. K. Chan proposed Network Intrusion Detection Using Deep Learning in [12]. They proposed a network intrusion detection system (IDS) utilizing machine learning techniques, specifically focusing on ensemble methods. Their work highlighted the importance of detecting anomalies and integrating multiple models to improve detection accuracy. Their approach heavily on traditional machine learning methods, which has there limitations in handling composite and dimensional data effectively.

Kwon, Cheolhyeon, Weiyi Liu, and Inseok Hwang proposed Security analysis for cyberphysical systems against stealthy deception attacks in [13]. The security issue in the state estimation problem is investigated for a networked control system (NCS). The communication channels between the sensors and the remote estimator in the NCS are vulnerable to attacks from malicious adversaries. The false data injection attacks are considered. The aim of this paper to find the so-called insecurity conditions under which the estimation system is insecure in the sense that there exist malicious attacks that can bypass the anomaly detector but still lead to unbounded estimation errors. In particular, a new necessary and sufficient condition for the insecurity is derived in the case that all communication channels are compromised by the adversary.

2.1 Cyber Hacking Breaches Prediction Using Machine Learning Techniques

Parameters are

A: Supervised Learning

B: Unsupervised Learning

C: Reinforcement Learning

D: Network logs

E: System calls

F: System configuration

G: Network traffic

H: User behavior

Table 1: Comparison of various Machine Learning Algorithms used Cyber Hacking Breachers

S.no	Author & Title	Techniques	A	B	C	D	E	F	G	H	ADVANTAGES	DIS ADVANTAGE
1	N. Milosevic (Cyber Security Mechanism)	Decision tree, Random forest, SVM, Hybrid approach, Anomaly detection and k-mean clustering	✓	✓		✓				✓	Improved accuracy and detection rate, Ability to learn large datasets and develop over time Enhanced anomaly detection and identification of unknown threats.	Need for big amounts of considered training data and Risk of overfitting and under fitting, High computational resources and training time required.
2	A. Alauthman, (Machine Learning for Cyber Attack Prediction)	Hybrid approach Decision tree, SVM, Q learning and Deep Q networks,	✓		✓	✓			✓		The study may have demonstrated the Effectiveness of ML in handling imbalanced datasets and adapting to evolving network threats. These research could have explored innovative techniques for feature selection, reduction, or extraction to improve ML model performance.	Approach could have required significant computational resources, training time, and expertise in ML and NIDS. The research may have encountered Difficulties in ensuring the scalability and real-time performance of the ML model in high-speed networks.
3	A.K.Singh (Machine Learning for Cyber Security)	Decision tree, Random forest,SVM, And Ensemble learning	✓					✓	✓	✓	Flexibility Can detect various types of attacks. Real-time detection Can detect attacks in real-time.	The study might have faced challenges in obtaining high quality, labeled training data for ML model development. Singh approach could have required significant computational resources and training time, potentially limiting its practical applicability

4	M.A. Almseidin (Predicting Cyber Attacks using Machine Learning)	Neural network, Q learning and Hierarchical clustering	✓	✓	✓	✓	✓			✓	Companies that develop precise Machine Learning (ML) models can secure a competitive advantage by harnessing datadriven insights, outpacing their rivals and driving business success. Moreover, accurate ML models enable personalized recommendations and tailored experiences, significantly enhancing customer satisfaction and fostering a loyal user base.	The research may have encountered obstacles in tackling the class imbalance issue, which arises when benign traffic vastly outnumbers malicious Traffic, potentially skewing the results. Additionally, the study might have faced hurdles in ensuring the ML model's Scalability and real-time performance in high-speed networks, where rapid processing is crucial.
5.	S.S.S. Gupta (Cyber Attack Prediction using Machine Learning: A Systematic Review)	Neural network, Deep learning, Ensemble learning, Deep Learning and Hierarchical clustering	✓	✓	✓		✓	✓			ML approach might have achieved high accuracy and detection rates in identifying network intrusions. The study may have demonstrated the effectiveness of ML in handling large datasets and adapting to changing network traffic patterns.	The study might have faced challenges in obtaining high quality, labeled training data for ML model development. It have required significant computational resources and training time, potentially limiting its practical applicability. The research may have encountered difficulties in interpreting ML model decisions and explaining false positives or negatives.

6	S.J.Yang (Cyber security attacks modeling)	Decision tree and K-means clustering	✓	✓		✓	✓			✓	The research could have explored innovative techniques for feature engineering, selection, or extraction to improve ML model performance. The study may have demonstrated the effectiveness of ML in handling complex network traffic patterns and adapting to new threats.	The research may have encountered Difficulties in ensuring the scalability and real-time performance of the ML model in high-speed networks. The study might have faced challenges in addressing the class imbalance problem, where normal traffic far exceeds malicious traffic.
7	Y.Zhang (Attacks and defenses on machine learning models)	Q-learning and Deep Q learning			✓			✓	✓		Reducing time complexity in data processing enhances efficiency, speeds up operations, and enables quicker access to valuable insights and results. High Accuracy in data ensures reliable insights, better decision-making.	High complexity in data can lead to increased processing time, resource requirements, and potential challenges in data analysis and interpretation. Time consuming data processing can delay decision making, hinder real-time insights, and impede the efficiency of data-driven operations and analytics.
8	J.Liu (simulation of cyber security attack model)	Decision tree, Random forest and k-mean clustering	✓	✓		✓	✓			✓	Increased robustne by combining multiple algorithms, hybrid approaches can reduce the risk of individual algorithm failures. Better handling of imbalanced data methods can address class imbalance issues, where normal traffic far exceeds malicious traffic.	Overfitting and under fitting risks in Hybrid methods can be prone to overfitting or under fitting if not properly tuned. Interpretability challenges has Hybrid approaches can make it more Difficult to interpret results.

3 Conclusion

This study successfully demonstrated the application of the strong control agreement method in complex separate cyber-physical networks, showcasing the capability to maintain system constancy and resilience in the face of multiple local cyber hacking breaches. The control method effectively identified and isolated compromised nodes, ensuring the overall system performance remained unaffected. Furthermore, the integration of recurrent neural networks with deep learning algorithms revealed that a linear function in a deep layer network yields improved performance, indicating reduced system complexity. Leveraging deep learning techniques enables systems to examine patterns learn from them and proactively avoid similar attacks making cyber security more efficient, cost-effective, and proactive. By analyzing the system state reported by the neural network, the control system makes informed decisions, detecting and isolating cyber hacking attempts to prevent detrimental effects on other agents. Future research directions include exploring additional attack scenarios, data mining, and advanced machine learning methods like support vector machines and recurrent Cat Boost algorithms to further enhance system performance.

REFERENCES

[1] Li, J., Wen, C., Liu, L., & Zhu, Z. (2022). "Real-time detection of deception attacks in cyber-physical systems." International Journal of Information Security. Available at: [Springer Link] (https://link.springer.com/article/10.1007/s10207-022-00616-9).

[2] Zhang, Y., Xu, G., & Wang, Z. (2021). ""Swift Identification of Deception Attacks in Cyber-Physical Systems: An Examination (Journal of Information Security and Applications, Vol.59,Article 10285)".

(https://www.sciencedirect.com/science/article/pii/S0167404821001597).

[3] Han, Q., et al. (2021). "Deep Learning Based Attack Detection for Cyber-Physical System Cybersecurity: A Survey." IEEE Journal of Automatic Sinica, 8(1), 13-31. Available at: [IEEE Explore] (https://ieeexplore.ieee.org/document/9154210).

[4] He, Z., & Hu, Q. (2021). "Security analysis for Cyber-Physical Systems against stealthy deception attacks." IEEE Transactions on Industrial Informatics. 1940-1952. Available at: [IEEE Explore] (https://ieeexplore.ieee.org/document/9154207).

[5] Wang, Y., & Liu, Y. (2021). Stealthy Deception Attacks Targeting Cyber-Physical Systems:An Examination Available at: [IEEE Xplore] (https://ieeexplore.ieee.org/document/9154211).

[6] In 2021, Kim and Lee published a research paper titled "Dynamic-Memory Event-Based Asynchronous Attack Detection Filtering for CPS" in the IEEE Transactions on Cybernetics, volume 51, issue 6, pages 2954-2965. This study is accessible online through IEEE Explore (https://ieeexplore.ieee.org/document/9154212).

[7] X. Zhao and Q. Wang's 2021 research paper, "Optimal Attack Strategies Subject to Detection Constraints against CPS," published in IEEE Transactions on Information Forensics and Security (vol.16,pp.2305-2317),is via IEEE Explore (https://ieeexplore.ieee.org/document/9154213).

[8] Mohammed, Z., 2018. NITDA Experts sound the alarm on looming cyber threats to banking institutions, warning of potential attacks. Govt Agencies, Others Retrieved from. https://www.nigerianews.net/nitdaraisesalarm-potentialcyber-attacks-banks-govtagencies/.

[9] Sun, N., Zhang, J., Rimba, P., Gao, S. Zhang, L. Y., & Xiang, Y (2018). Data driven cyber security incident prediction: A survey. IEEE communications surveys &tutorials, 21(2), 1744-1772.

[10] G. Wang, J. Hao, and L. Huang's 2010 research paper, "A New Approach to Intrusion Detection Using Artificial Neural Networks and Fuzzy Clustering" (Vol. 37, Issue 9, September 2010, pages 6225-6232), presented a novel approach to intrusion detection using Artificial Neural Networks and fuzzy clustering

GAMANAM
Volume 1, Issue 1, January 2025

Invited Paper

Silk - a Global Textile

[1]S.B.Dandin

[1]*Former Vice-Chancellor, UHS, Bagalkot, Karnataka and Former Director, CSB*

Received: 23/11/2024, Revised: 17/12/2024, Accepted:23/12/2024 Published:01/01/2025

Abstract: Silk, the mystical fiber of unmatched elegance, has attracted humanity across the globe since ancient times. Even today, silk holds its place as a symbol of luxury and high fashion, earning its title as the "Queen of Textiles.". Silk can also be regarded as a global textile, as it addresses significant global concerns and aspirations while rooted in the rich history of sericulture. With a legacy spanning over 4,500 years, sericulture has shaped beautified and sustained human civilization. Today, it is prominent in the global socio-economic landscape due to its multifaceted advantages. Because of the socioeconomic importance and rural economy, the industry is rightly accepted as the industry of the rural poor. The world produces five types of silks and mulberry is the major type occupying 70% share. China and India contribute 95% of the global production and India is the major consumer and importer of mulberry silk. Despite its socioeconomic importance, the world's raw silk production is showing a declining trend, especially in China. The main reasons attributed are fast urbanization, loss of interest among youth and stiff competition by synthetic fibers. Another important aspect to be considered is information on the global silk demand-supply position. In the absence of authentic information, many countries are not coming forward to venture into silk production. Silk is a rich proteinaceous biomaterial that can be used in the cosmetic, pharmaceutical, and food industries. Keeping all the above there is a need for establishing a global body for the promotion of the silk industry as a global avocation

Keywords: silk, mulberry, textile, fiber

1 Introduction

Silk, the mystical fibre of unmatched elegance, has captivated humanity across the globe since ancient times. In China, it was a highly lucrative trade commodity. Ancient Persian traders (modern-day Iran) ventured through perilous routes—marked by treacherous mountain ranges, challenging passes, arid deserts, and dense forests—to procure exquisite, richly coloured, and finely textured silk from Chinese merchants. Alongside silk, other goods such as amber, glass, spices, and tea were also traded. However, silk quickly became a cornerstone of the Chinese economy, giving the trade route its iconic name: the "Silk Route." Even today, silk holds its place as a symbol of luxury and high fashion, earning its title as the "Queen of Textiles.". Silk can also be regarded as a global textile, as it addresses significant global concerns and aspirations while rooted in the rich history of sericulture. With a legacy spanning over 4,500 years, sericulture has shaped and beautified human civilization and sustained it. Today, it is prominent in the global socio-economic landscape due to its multifaceted advantages. These contributions can be categorized as follows:

A. Sericulture and Global Issues

1. Environmental Safety – Promotes eco-friendly practices.
2. Employment Security – Provides stable jobs, particularly in rural areas.
3. Carbon Credit – Contributes to carbon sequestration and climate initiatives.
4. Ecosystem Services – Enhances biodiversity and supports sustainable agriculture.
5. Above all fulfils 7 of SDG of UNO

B. Sericulture and Society

1. Food and Nutrition Security – Plays a role in ensuring sustenance for communities.
2. Employment Generation – Offers gainful employment, particularly for rural populations.
3. Gender Inclusivity – Empowers women by being a human-friendly industry.
4. Wealth Distribution – Generates high income for producers, redistributing wealth as silk is a premium product.
5. Rural Retention – Helps curb rural-to-urban migration by offering local opportunities.
6. Multiple Benefits – Delivers diverse advantages for humankind.

7. Foreign Exchange Earnings – Boosts national economies through international trade.

This highlights the enduring relevance of sericulture as a sustainable and socio-economically vital industry.

Historical Perspective

The earliest records of cultivated silk production date back to approximately 2640 BC, when the Chinese Empress Si Ling-chi is credited with patronizing the silk industry. For centuries, the Chinese guarded the art of silk production as a closely held national secret. Queen Hoshomin later introduced sericulture as a commercial venture in China solidifying its importance. Over time, sericulture spread to Korea, Japan, and eventually Europe. Sericulture was introduced to India around 400 years ago and has since flourished as an exemplary agro-industry. Its adaptability and economic value highlight its immense potential for sustainability, particularly in the context of climate change and for the economic upliftment of small and marginal farmers.

Global Silk Scenario

Currently, five types of natural silks are produced worldwide, with **mulberry silk** dominating production and accounting for over 90% (Figure 1). The type of silk produced in each region is largely determined by the availability of specific food plants for silkworms (Table 1).

Key Highlights

- **China and India**: The two leading producers of mulberry silk.
- **India's Unique Position**: India is the only country producing all commercially exploited natural silks and holds a global monopoly in the production of Muga silk, which is endemic to the country.
- **Shift in Production**: There has been a notable shift in silk production from temperate regions to subtropical regions. Countries like Japan, South Korea, and the USSR have ceased silk production due to high industrialization, rising costs, and declining interest among younger generations. Sericulture continues to play a vital role in global economies and holds significant promise for sustainability in a changing climate

Figure 1: Mulberry Silk

Table 1. Commercially exploited serpiginous insects of the world and their food plants

Common Name	Scientific Name	Origin	Primary Food Plant(s)
Mulberry Silkworm	*Bombyx mori*	China	*Morus indica, M. alba, M.multicaulis, M.bombycis*
Tropical Tasar Silkworm	*Antheraea mylitta*	India	*Terminalia tomentosa T. arjuna, Shorea robusta*
Oak Tasar Silkworm	*Antheraea proylei*	India	*Quercus incana, Q. serrata, Q. himalayana, Q.leucotricophora, Q. semicarpifolia, Q. grifithi*
Oak Tasar Silkworm	*Antheraea frithi*	India	*Q. dealbata*
Oak Tasar Silkworm	*Antheraea compta*	India	*Q. dealbata*
Oak Tasar Silkworm	*Antheraea pernyi*	China	*Q. dentata*
Oak Tasar Silkworm	*Antheraea yamamai*	Japan	*Q. acutissima*
Muga Silkworm	*Antheraea assama*	India	*Litsea polyantha, L. Machilus bombycina*
Eri Silkworm	*Philosamia ricini*	India	*Ricinus communis, Manihot utilisma, Evodia fragrance*

Source:wwwcsb.gov.in

Global Silk Production and Trade

Silk production spans over 30 countries, with **Asia** serving as the global powerhouse, contributing approximately 98% of the world's total silk output. **China** and **India** dominate this industry, jointly accounting for more than 95% of global production. While silk represents only about 0.5% of the global textile trade, its cultural and economic significance remains immense.

Key Highlights

1. **China**
   - The largest producer of silk, contributing 63% of global output.
   - The largest exporter, accounting for over 80% of global silk exports.

- Home consumption of silk is relatively low, at 20%.

2. **India**
   - The second-largest global producer and the largest consumer and importer of raw silk (41,500 MT and 2,650 MT, respectively).
   - India's contribution to global silk production has risen to 40%, but its share in the world's "Silk Trade" remains at around 5%.
   - Silk production in India is increasingly managed by large consortiums that focus on exports.
3. **Other Countries**
   - **Uzbekistan** contributes 2.23% to global silk production.
   - Countries like **Brazil, Thailand, Vietnam, North Korea, and Iran** collectively account for a mere 2.72%.
   - **Japan** boasts the highest per-capita silk consumption.

Table 2. Global silk production trend (Source: https://inserco.org)

#	Country	2016	2023	+/-
1	China	1,58,400	50,000	- 1,08,400
2	India	30,348	38,913	+ 8,565
3	Uzbekistan	1,256	2,037	+ 781
4	Vietnam	523	1,448	+ 925
5	Brazil	650	330	- 320
6	Thailand	712	291	- 421
7	Iran	125	276	+ 151
8	Tajikistan	0	227	+ 227
9	Others (16 countries)	98	464	+ 366
10	Total	192112	91221	-100891

Trends in Production

- Over the past decade, there has been a **global decline in raw silk production** by 39,065 MT (30%), primarily due to a sharp reduction in Chinese output.
- In contrast, **India's silk production has increased steadily** by 11,532 MT (63%) over the same period.

Both Uzbekistan and Vietnam are showing an upward trend in silk production.

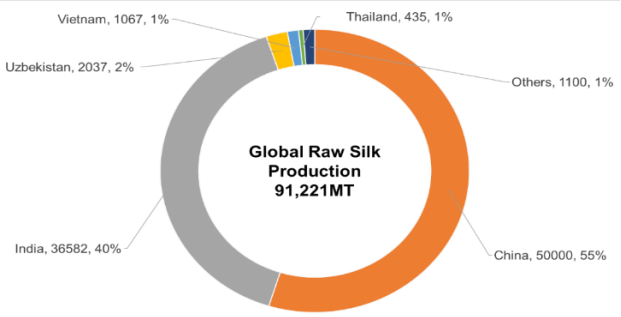

Figure 2: World Raw silk production (Source: https://inserco.org)

Global Silk Trade Scenario

Despite these developments, reliable data on global demand and supply trends is lacking. The silk trade dynamics are influenced by several factors, including shifts in production patterns, rising industrialization, and consumer preferences. Reliable information or data to accurately assess global demand and supply for silk remains unavailable. However, production trends reveal notable patterns. Despite a sharp decline in Chinese silk production, the overall global production ratio has remained relatively stable due to slow but steady growth in Indian output.

Over the past decade, global raw silk production has decreased by 39,065 MT, a 47.5% reduction. In contrast, **India** has seen consistent growth in raw silk production, with an increase of 11,532 MT, representing a 63% rise during the same period. Similarly, there is an upward trend in production in **Uzbekistan** and **Vietnam**, further contributing to the evolving dynamics of the global silk industry. This steady growth in certain regions indicates potential for regional diversification and resilience within the global silk trade

A detailed comparison of the mulberry sericulture industries in China and India, the two largest raw silk producers, is provided in Table 3.and over the last 10 years there has been an increase of 11532 MT (63.00%) Similarly there is an increasing trend both in Uzbekistan and Vietnam

The data highlights a significant decline in global silk production, particularly in China, where production has dropped to less than half of its earlier levels. This decline is primarily attributed to acute labor shortages, waning interest among the younger generation, and stiff competition from synthetic fibers.

A comparison between the world's two largest silk-producing countries—**China** and **India**—is summarized in Table 3.

Key Differences Between China and India

1. **Types of Silk**:
   - **China**: Produces only bivoltine silk, which is known for its superior quality (grade 3A and above).

- **India**: Primarily produces multivoltine silk, with most of it falling in the 2A and below grade range.

2. **Production and Consumption**:
   - **China**: Exports the majority of its silk, with domestic consumption accounting for just 20%.
   - **India**: A major consumer of silk domestically, it also imports high-quality silk from China to meet demand.
3. **Silk Rearing and Crops**:
   - **China**: Limited to 2–3 silkworm crops per year due to climatic conditions.
   - **India**: Benefits from climatic advantages, allowing silkworms to be reared year-round and yielding 5–6 crops annually.

Despite these differences, production and productivity levels in both countries remain comparable. Notably, while Chinese silk production is on a sharp decline, India's output is steadily increasing. This upward trend positions India as a strong contender to become the global leader in raw silk production.

As can be seen from the above data global silk production is declining sharply, especially in China and the production has come down to less than half, The reasons for the same has been attributed to acute labour shortage and loss of interest in younger generation besides, the tough competition from the other synthetic fibres

Table 3. Comparison between sericulture in China and India

Parameters	**China (2022)**	**India (2023-24)**	
Area under mulberry (ha)	4.10 lakh	2.63 lakh	
Leaf Yield (MT/ha/yr)	30-35	50-60	
Races reared	Bivoltine: 100%	Cross breed (CB): 72%	Bivoltine (BV): 28%
Egg production (crore dfls)	44.5	32.00	
Supply system	Majority chawki reared	CB: Supplied by eggs & Chawki 90%	BV: Mostly 85% Chawki reared
Rearing pattern	Batch wise	Throughout the year	
dfls brushed/ha/yr	1075	2250	2000
Cocoon Production (MT)	311500	152900	62700
Cocoon yield (kg/100 dfls) (2boxes)	70	60	65
Leaf cocoon ratio(kg)	20	22	25
Cocoon yield (kg)/ha	760	1350	1300
Cocoon weight (g)	1.9 – 2.0	CB: 1.5 –1.7	BV: 1.7-1.8
Shell percentage	21-24	CB: 17-19	BV: 20-21
Filament Length (m)	>1000	CB<800	BV >950
Renditta	6	CB: 7.6	BV: 6.50
Grade of silk as per ISA standards	Up to 6A	Up to 2A	Up to 4A
Cocoon price during March 2024 (Rs/kg)	600-650	CB: 400	BV: 500
Raw silk productivity (kg/ha/yr)	**122**	110	
Raw silk price during March 2024 (Rs/kg)	**5300**	4400	
Demand and supply position	90% Export	Mostly domestic (10% deficit)	
Mulberry raw silk production (MT)	50,000	29892 (CB:20217, BV:9675)	

Global Challenges in Sericulture

- Urbanization and Industrialization: Rapid urbanization and industrial growth in traditional sericulture regions, coupled with deforestation (especially in the Vanya silk sector), have reduced the potential area for food plants cultivation
- Manpower Issues: Declining interest among the younger generation and a shortage of manpower are major challenges.
- Competition and Counterfeiting: Stiff competition from synthetic fibres and the prevalence of adulterated or fake silk products.
- Climate Change and Environmental Vagaries: Effects of climate change, including drought, depleting water tables, and low soil organic carbon, along with climate aberrations and vagaries.
- Breeds and Technological Gaps: Insufficient availability of improved silkworm breeds across all varieties and inadequate maintenance/multiplication planning of silkworm races.
- Economic Challenges: Stagnation in silk exports, increasing input costs, and a growing preference for blended or synthetic products over pure silk.
- Underutilization of Resources: Poor utilization of sericulture products and by-products for value-added applications such as medical, aerospace, cosmetics, and food industries, particularly in India.
- Low Production Base: Limited production and low productivity in temperate/northern zones, with fewer crops per year.
- Lack of Corporate Involvement: Absence of large-scale corporate sector involvement in end-to-end sericulture operations, especially in India

Way Forward for Sericulture Development

- Global demand-supply Data and Planning: Conduct periodic surveys to assess domestic and international demand-supply dynamics to guide production planning.
- Mapping and Expansion: Use GPS/GIS tools to remap potential sericulture clusters in major production hubs and identify new suitable areas.
- Technological Advancements: Develop and refine cutting-edge technologies for all stages of the sericulture production chain- from farm to fabric.
- Climate Resilience: Introduce sericulture-based integrated farming and agroforestry models to enhance climate resilience and earn carbon credits.
- Improved Silkworm Breeds: Focus on developing silkworm races and hybrids resistant to biotic and abiotic stresses.
- Mechanization and Youth Engagement: Emphasize mechanization and reduce drudgery to attract younger generations to sericulture.
- Product Diversification: Diversify silk products to cater to changing market demands, including niche domestic and international markets.
- Value-Added Products: Maximize by-product utilization at every stage of production to develop value-added goods for multiple industries.
- Capacity Building: Provide large-scale training on new technologies and management practices to stakeholders, especially youth.
- Integrated Production Models: Implement economic/business models for cluster-based production hubs with end-to-end operations linking all stages of the sericulture production chain.
- Regulatory Reforms: Introduce industry-friendly reforms to attract corporate investors and boost sector growth.
- Global Coordination: Strengthen international coordination mechanisms for silk production and trade.
- Technology and Knowledge Exchange: Promote the exchange of genetic material, expertise, and cutting-edge technologies across borders.
- Silk Promotion: Position silk as a global textile, emphasizing its unique qualities to compete with synthetic fibres and other textiles.

The sericulture industry holds immense potential to contribute significantly to sustainable development, rural livelihoods, and global trade. By addressing challenges with a well-rounded approach—leveraging technological innovations, improving production efficiencies, and fostering international collaborations—the sector can thrive in a competitive global market. Prioritizing climate resilience, youth engagement, and value addition will ensure its long-term viability while enhancing its appeal to modern stakeholders. With coordinated efforts among policymakers, researchers, and industry participants, sericulture can be positioned as a dynamic, eco-friendly industry, meeting both traditional and contemporary demands.

References

[1] CSB, (2019). Seri-States of India- A Profile. (2019)-Central Silk Board, Ministry of Textiles, Government of India.168 p.

[2] CSB, (2018). CSB Vision 2030. Central Silk Board, Bengaluru.

[3] Dandin, S.B. (2019). Doubling farmers income: Production enhancement through productivity gains. MoA&FW, Govt. of India, Vol. VIII, pp. 147-154.

[4] Dandin, S.B., Basavaraja, H.K., Suresh Kumar, N., Mal Reddy N., Kalpana, G.V. and Joge, P.G. (2006). Development of bivoltine silkworm hybrids of Bombyx mori L for tropics. In: Asia Pacific Congress of Sericulture and Insect Biotechnology (APSERI 2006), Sangju, Korea, October 11th -14th 2006, pp.106.

[5] Mahes M. Nanavaty, (1965). Silk from Grub to Glamour, Paramount Publishing House, Bombay. 277p

[6] Xijie Guo, (2019). Current status and future prospectus of sericulture in China. Proc. 6th APSERI Conference, Mysuru, 2-4 March, 2019. P. 107.

[7] Yamada, K. (2020). 16 Years of JICA Technical Cooperation for Bivoltine Sericulture Promotion in India. JICA, Japan, 110p

[8] https://csb.gov.in

[9] https://www.inserco.org

GAMANAM
Volume 1, Issue 1, January 2025

Research Paper

Polymeric Micelles of Coriandrum Sativum Seed Oil – Preparation and In-Vitro Evaluation

[1]Keerthana Morusu, [1*]Nagaraju Ravouru, [1]Anvitha Rani Modem, [1]Sai Sruthi Kaveripakam

[1]*Institute of Pharmaceutical Technology, Sri Padmavati Mahila Visvavidyalayam, Tirupati-517502, India*

**Corresponding Author(s): id-profnagaraju@gmail.com*

Received: 23/11/2023, Revised: 15/12/2023, Accepted:23/12/2024 Published:01/01/2025

Abstract: Polymeric micelles are well known for their advantages like enhancement of bioavailability of poorly soluble drugs and herbal drug constituents. The present research work was aimed to prepare polymeric micelles of Coriandrum sativum seed oil (CSSO) and to evaluate them for in-vitro properties and antibacterial activity. Extraction of CSSO from Coriandrum sativum seed powder was performed by hydro distillation technique. Phytochemical evaluation of CSSO reveals the presence of tannins, alkaloids & saponins followed by the measurement of chemical indices and GC-MS analysis of CSSO. The polymeric micelles containing CSSO were prepared by solvent diffusion method using PEG 6000 as a polymer & Pluronic F127 as a stabilizer. The Box-Behnken design was employed considering drug & polymer concentration along with stirring time as independent variables and particle size, % entrapment efficiency and % cumulative drug release as the dependent variables. The optimized formulation had shown low CMC value, which indicates that it was stable. The particle size & zeta potential values were 220.5±0.21nm and -0.5±0.2 mV & % entrapment efficiency of 55.34%, % cumulative drug release of polymeric micelles after 24 hrs was found to be 70.86%. Drug-Excipient compatibility studies were carried out to find out the interactions between drug and other excipients. Phase contrast microscopy was employed to find out the morphology. FT-IR analysis had revealed that polymer & CSSO were compatible with each other & Morphology of the optimized formulation was spherical & well distributed. The in-vitro antibacterial studies using agar diffusion process had shown that the optimized polymeric micelles were found to be more effective against gram positive bacteria than gram negative bacteria.

Keywords: *Coriandrum sativum* seed oil, Polymeric micelles, PEG 6000, Solvent diffusion technique.

1 Introduction

Polymeric micelles hold a great ability for the compounds that are hydrophobic in nature and also for the compounds with poor bioavailability [1, 2]. Polymeric micelles possess beneficial characteristics like tunable physicochemical properties, smaller particle size, controlled drug release, high kinetic stability, high drug loading capacity and maintains the integrity [3, 4]. Formation of polymeric micelles occurs when the concentration of the polymer increases beyond the certain concentration i.e. critical micelle concentration (CMC) [5.6] Coriander (*Coriandrum sativum*) is an aromatic, annual herb, which is native to the Mediterranean & middle east region, & well cultivated in India, Russia, Central Europe, Asia & Morocco & belongs to Apiaceae family [7].

Materials & Methods

Coriander seeds were purchased from local market at Nellore, Andhra Pradesh, Polyethylene glycol 6000&Pluronic F127 were procured from S.d fine chemical Pvt, Ltd, Mumbai, & Acetone from Merck Ltd, Mumbai.

Physicochemical analysis of *Coriandrum sativum* seed powder (CSSP): Physicochemical analysis of CSSP i.e. loss on drying, ash values, extractive values, swelling index & fluorescence analysis were investigated [8, 9].

Extraction of Coriandrum sativum seed oil (CSSO): Extraction of chemical constituents from coriander seed powder is done by hydrodistillation technique. 30 grams of coriander seed powder was taken into the round bottom flask and 225 ml of distilled water was added. The distillation process should be performed for 2hr at 60◦c and the oil-water mixture was extracted with dichloromethane in a separating funnel inorder to separate organic phase & aqueous phase and dried over sodium sulphate. The organic phase was collected and concentrated by keeping in water bath for 2hrs at 80°c.The final extract was filtered and used for further analysis [10].

Phytochemical evaluation of Coriandrum sativum seed oil (CSSO): The phytochemical tests i.e. test for alkaloids, carbohydrates, terpenoids, tannins & saponins were performed for the CSSO [8,11].

38

Physicochemical Characterization of CSSO: Solubility, boiling point & p^H of CSSO were determined.

***Measurement of chemical indices of essential oil*:** Acid number, ester number, saponification index & iodine value were determined [7,12].

***Construction of standard plot for the coriander seed oil*:** 4ml of CSSO was placed in the cuvette and absorbance was measured from 200-400 nm, λ_{max} of CSSO was noted.

***Determination of chemical constituents by GC-MS (Gas-Chromatography-Mass spectroscopy)*:** The Clarus 680 GC was used in the analysis as described by Nejad Ebrahimi *et al.*, employing a fused silica column, and the components were separated using Helium as carrier gas at a constant flow of 1 ml/min. The injector temperature was at 260°C, 1µL of extract sample injected into the instrument the oven temperature was as follows: 60 °C (2 min); followed by 300 °C at the rate of 10 °C min−1; and 300 °C, where it was held for 6 min. The spectrums of the components were compared with the database of spectrum of known components stored in the GC-MS NIST (2008) library. [13]

***Design of Experimentation (Box-Behnken design) BBD*:**

By employing the BBD, polymeric micelles containing CSSO were prepared using solvent diffusion method with PEG6000 and poloxamer407 as polymers. A13 run Box-Behnken design with the three factors and three levels with three triplicate at the center point was employed. The three independent variables were drug concentration(X1), polymer concentration (X2) and stirring time (X3) and these vary at three different level i.e. low, medium and high (-1, 0, +1) and the dependent variables were particle size (Y1), entrapment efficiency (Y2) and cumulative drug release (Y3).

***Method for the preparation of polymeric micelles containing Coriander seed oil*:**

Solvent diffusion method: [14]

The polymeric micelles containing coriander seed oil was prepared by employing solvent diffusion technique. The accurate quantity of coriander seed oil & PEG6000 were dissolved in acetone(10ml). The above solution is to be added slowly drop wise into the 20 ml of distilled water under constant stirring. The resulting solution is to be stored in amber colored bottles until for further use.

Characterization of polymeric micelles: [15]

Particle size &Zeta potential: The average size & polydispersity index of the polymeric micelles along were determined by zeta sizer (Nanoparticle SZ 100, Horiba scientifics) using dynamic light scattering method at an angle of 173^0 and the cell temperature was 25◦c. All the trails were performed in triplicate and the data is represented as mean ± standard deviation (SD).

%Encapsulation Efficiency:

After lyophilization,1 mg of polymeric micelles were taken accurately in an amber colored glass vial&1ml of ethanol was added, and subjected to sonication for 2-3 min, and kept in darkling at room temperature for 1hr.Then, the absorbance was checked at 320nm using UV-spectrophotometer. The %encapsulation efficiency was calculated using the following equation,

$$\%EE = \frac{\text{weight of coriander seed oil in the micelles}}{\text{weight of initial amount of coriander seed oil}} \times 100$$

***In vitro* drug release:**

The *in vitro* drug release profiles of the prepared polymeric micelles containing coriander seed oil were assessed by dialysis bag method. 2ml of the prepared micelles were placed in the dialysis bag and closed on both the sides with clips and is immersed in a glass container with the 100 ml of release medium i.e. phosphate buffer saline (with 0.5% Tween 80), p^H 7.4.

The container was placed on the magnetic stirrer at 37◦c and about 2ml of release medium was withdrawn at different time intervals (1,2,4, 6, 8, 12& 24 hrs) and replaced with the fresh medium. The amount of coriander seed oil released into the medium was determined using UV spectrophotometer at 300 nm.

The % cumulative drug release of CSSO at certain time intervals was calculated by using the following equation,

Critical micelle concentration (CMC):

$$\%\text{cumulative drug release} = \frac{\text{Amount of coriander seed oil in the medium (µg)}}{\text{Amount of coriander seed oil loaded in the micelles (µg)}} \times 100$$

CMC of the polymeric mixture was determined by UV at 366nm using hydrophobic probe as iodine.0.5g of iodine (I_2) and 1.0 g of potassium iodide (KI) was dissolved in 50ml of distilled water in order to prepare standard solution (KI/I_2). Different concentrations of the polymeric mixture were prepared in the range of (0.1 to 1.0 %). 25 micro liters (µl) of KI/I_2 standard solution is to be added to the various concentrations of the polymeric mixture. The mixtures were kept in darkling for 12h at room temperature & the absorbance was measured at 366nm. The graph is plotted for the absorbance & logarithm of polymer concentration. The CMC value of the polymeric mixture corresponds to the concentration of the polymer, when there is an increase in the absorbance.

Particle shape & Morphology: The polymeric micelles containing CSSO were visualized through phase contrast microscopy. The sample was dispersed on the glass slide and observed at high magnification with an Olympus optical microscope (model CH3ORF200, Olympus Tokyo, Japan).

Drug Excipient Compatibility studies:

Fourier Transform Infrared (FT-IR) Analysis: [13]

The FT-IR spectra of pure extract, extract + polymer mixture & optimized formulation of polymeric micelles were recorded using Bruker T type FT-IR spectrometer. The drug is dispersed in potassium bromide i.e. 1:100 ratio. The sample was scanned in the range of wavelengths 400 to 4000cm^{-1}.

Evaluation of Antibacterial Activity:

To perform antibacterial studies four microorganisms were selected: *Staphylococcus aureus, Bacillus subtilis, Escherichia coli* and *Proteus vulgaris.* The culture media was prepared using nutrient broth and agar powder and the components were mixed until homogenous and the mixture was heated with simple agitation. After this, the mixture was kept at 121◦c for 20 minutes in the autoclave.

Agar diffusion process [17]: This process was done by taking three petri plates filled with the culture media of uniform surface and depth. The three petri plates were filled with coriander seed oil, polymeric micelles containing coriander seed oil and the marketed formulation i.e. Ciprofloxacin 500mg tablet considered as standard. The plates were incubated 24 hrs at 37◦c for the antibacterial test. Diameter of the zone of inhibition was measured in cm is considered as important step in the determination of antibacterial activity.

Statistical analysis: The optimization of polymeric micelles containing CSSO by DoE Software (Design Expert @ v-13). Inserting the values of dependent variables in the design expert software gives the optimized formulation through ANOVA, surface response plots and also with contour & overlay plots.

2 Results & Discussion

Physicochemial analysis of *Coriandrum sativum* seed powder like loss on drying, total ash, acid insoluble ash & water-soluble ash, soluble extractive values, swelling index & fluorescence analysis are described in table 1& 2.

Table 1: Describes the physicochemical properties of Coriandrum sativum seed powder

S.No	Evaluation Parameters	Values
1.	Loss on drying	4%±0.3%w/w
2.	Total ash	5.0±0.6%w/w
3.	Acid insoluble ash	0.3±0.1%w/w
4.	Water soluble ash	2.66±0.4%w/w
5.	Water soluble extractive	25±0.5%w/w
6.	Alcohol soluble extractive	10±0.2%w/w
7.	Swelling index	1 ml

Table 2: Flourescence analysis of Coriandrum sativum seed powder

S.No	Reagent	Day light	UV light
1.	Sample+Dil HCl	Yellow	Green
2.	Sample + Dil HNO_3	Yellow	Light green
3.	Sample + Conc.HNO_3	Orange	Yellow
4.	Sample + Dil CH_3COOH	Yellow	Orange
5.	Sample + Dil H_2SO_4	Yellow	Green
6.	Sample +Conc H_2SO_4	Beet root red	Black
7.	Sample + Glacial CH_3COOH	Yellow	Light brown
8.	Sample + $HClO_4$	Brown	Black
9.	Sample + Hg_2Cl_2	Yellow	Green
10.	Sample + NH_4OH	Light green	Yellow
11.	Sample + 10% NaOH	Orange	Light brown
12.	Sample + 40% NaOH	Orange	Light brown

Fluorescence analysis is an essential parameter for the standardization of crude drug. Fluorescence test on CSSP helps in qualitative analysis, which can be used as a reference data for the identification of adulterants.

Physicochemical characterization of Coriandrum sativum seed oil (CSSO): The solubility studies of CSSO in various solvents was performed and it is soluble in distilled water, ethanol & methanol, where as it is slightly soluble with acetone, chloroform & carbon tetrachloride.

Boiling point & p^H of CSSO: Boiling point & p^H of CSSO was found to be 195°c±0.2&6.87±0.05.

Phytochemical Evaluation of CSSO: Phytochemical evaluation of *Coriandrum sativum* seed oil indicates the presence of tannins, alkaloids & saponins and the results are tabulated in Table 3.

Chemical indices of CSSO: The results of chemical indices like acid value, ester value, saponification value & iodine value are tabulated in table 4.

Determination of Chemical constituents from Coriandrum sativum seed oil by GC-MS:

The chemical constituents of *Coriandrum sativum* seed oil was analyzed by gas chromatography-mass spectroscopy (GC-MS).The results of GC-MS analysisof CSSO had shown 15 compounds and listed in table 5,where 2,3-Anhydro-D-Galactosan is responsible for antibacterial activity.

Table 3: Results of phytochemical evaluation

S.No	Test	RESULT
1.	Ferric chloride test (Tannins)	Positive
2.	Molisch's test (Carbohydrates)	Negative
3.	Dragendroff's test (Alkaloids)	Positive
4.	Salkowski's test (Sterols)	Negative
5.	Foam test (Saponins)	Positive

Table 4: Results of chemical indices

S.No	Chemical indices	Value
1.	Acid value	11.781±0.4
2.	Ester value	144.177±1.6
3.	Saponification value	155.958±2.2
4.	Iodine value	33.56±3.7

Table 5: GC-MS analysis of Coriandrum sativum seed oil

S.No	RT	Scan	Height	Area	Area %	Norm%	Name of the compound
1	14.608	2421	7,811,346	1,475,894.9	8.679	46.52	1,3-Dioxolane 2HeptanenitrileAlpha.-methyl-delta.oxo-2-phenyl
2	17.074	2914	60,346,780	3,172,427.0	18.655	100.00	Z-2-Octadecen-1-ol
3	17.519	3003	15,210,604	824,515.2	4.848	25.99	1-Octadecyne
4	25.838	4666	8,957,601	405,356.9	2.384	12.78	Coprostan-16.beta-ol
5	25.988	4696	16,427,744	841,216.4	4.947	26.52	Pregnan-3,11-diol-20-one
6	26.823	4863	10,474,685	583,953.1	3.434	18.41	Cholest-8-en-3-ol,14- methyl(3.beta.,5.alpha)-
7	26.853	4869	9,983,861	1,027,765.4	6.044	32.40	Oleicacid
8	27.088	4916	9,094,523	924,488.3	5.436	29.14	7-Hydroxy-3-(1,1-dimethylprop-2-enyl) coumarin
9	27.358	4970	11,899,070	857,206.2	5.041	27.02	Spiro(androst-5-ene-17,1'-cyclobutan)-2'-one,-3-hydroxy-, (3.beta.,17.beta)-
10	27.488	4996	5,754,617	334,598.6	1.968	10.55	1-Butanol,4-butoxy-
11	27.638	5026	11,064,260	1,359,883.4	7.997	42.87	Dihydroartemisinin,10-O-(T-Butyloxy)-
12	28.114	5121	8,239,310	1,244,230.5	7.317	39.22	2,3-Anhydro-D-Galactosan
13	28.819	5262	10,321,005	914,655.0	5.379	28.83	3,4-Anhydro-D-Galactosan
14	28.889	5276	9,072,620	1,126,772.5	6.626	35.52	Dihydroartemisinin,10-O-(T-Butyloxy)-
15	29.444	5387	21,179,972	1,912,652.0	11.247	60.29	Cyclohexane,1-(1,5-Dimethylhexyl)-4-(4-methylpentyl)-

Preparation & Characterization of polymeric micelles containing *Coriandrum sativum* seed oil: Polymeric micelles were prepared by employing solvent diffusion method by dispersing the acetone solution containing CSSO & PEG6000 along with Pluronic F127 as a stabilizer.Polyethylene glycol is nontoxic , non-immunogenic & non- antigenic water soluble polymer.[17]

Optimization of polymeric micelles: The prepared polymeric micelles containing *Coriandrum sativum* seed oil using DoE software (Design Expert @v.13) using box-behnken design as shown in table 6 & 7 shows the particle size, % entrapment efficiency & *in vitro* drug release of the polymeric containing *Coriandrum sativum* seed oil.

Table 6: Layout of Box-Behnken design

S.No	Independent variables	Levels		
		Low(-1)	Medium(0)	High(+1)
1.	Drug concentration(ml)(X1)	1.0	1.5	2.0
2.	Polymer concentration(mg)(X2)	50	100	150
3.	Stirring time(min)(X3)	20	30	40

Table 7: Results of dependent variables on polymeric micelles containing Coriandrum sativum seed oil

Runs	X1	X2	X3	Particle size (nm) Mean± S.D Y1	Entrapment efficiency (%) Y2	Cumulative drug release (%)Y3
F1	1	100	20	128.53±0.32	24±0.020	51.84±0.63
F2	1	50	30	135.47±1.04	27.7±0.026	56.41±0.37
F3	1	100	40	191.2±1.15	37±0.015	61.53±0.42
F4	1	150	30	246.27±0.50	43±0.022	65.2±0.15
F5	1.5	50	20	242.33±0.67	45.7±0.037	67.58±0.59
F6	1.5	50	40	253.33±0.31	57±0.033	71.04±0.46
F7	1.5	150	20	250.3±3.82	61±0.010	74.35±0.75
F8	1.5	100	30	191.23±0.40	57.33±0.003	76.8±0.38
F9	2	100	40	385.60±0.92	65.4±0.036	78.72±0.63
F10	1.5	150	40	347.11±0.85	62±0.111	80.64±0.23
F11	2	50	30	364.43±0.57	64±0.057	82.05±0.49
F12	2	100	20	275.20±1.57	64.4±0.040	84.48±0.52
F13	2	150	30	397.33±0.99	73.7±0.004	87.17±0.35

Particle shape and morphology of the optimized formulation: The morphology of polymeric micelles was imaged by phase contrast microscopy and the results had shown that well distributed particles and mostly found to be spherical in shape as shown in Figure 1.

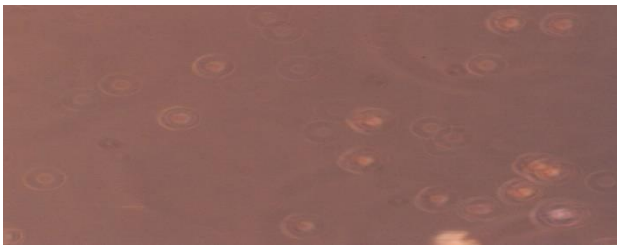

Figure 1: Phase contrast image of optimized formulation

Particle size & Zeta potential (optimized formulation): The particle size and zeta potential of the optimized formulation was found to be 220.5±0.21nm and -0.5±0.2 mV as shown in the Figure 2. It is observed that, increasing X_1, X_2, X_3 concentration i.e. increase in drug concentration & polymer concentration along with increase in stirring time had shown increase in particle size, this indicates that more drug is loaded into the core of the micelles at higher concentrations of drug & polymer [18], increase in stirring time had shown increased particle size due to particle agglomeration [19].

%Entrapment efficiency: The % entrapment efficiency of the optimized formulation was found to be 55.34%. In this study it is observed that increase in drug and polymer concentration along with stirring time had increased the entrapment efficiency of the polymeric micelles.

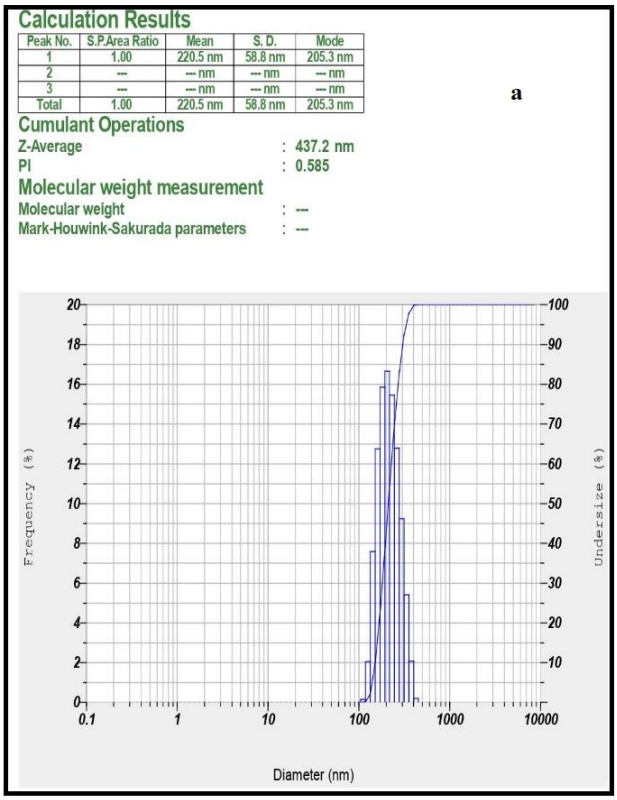

Figure 2 (a) particle size

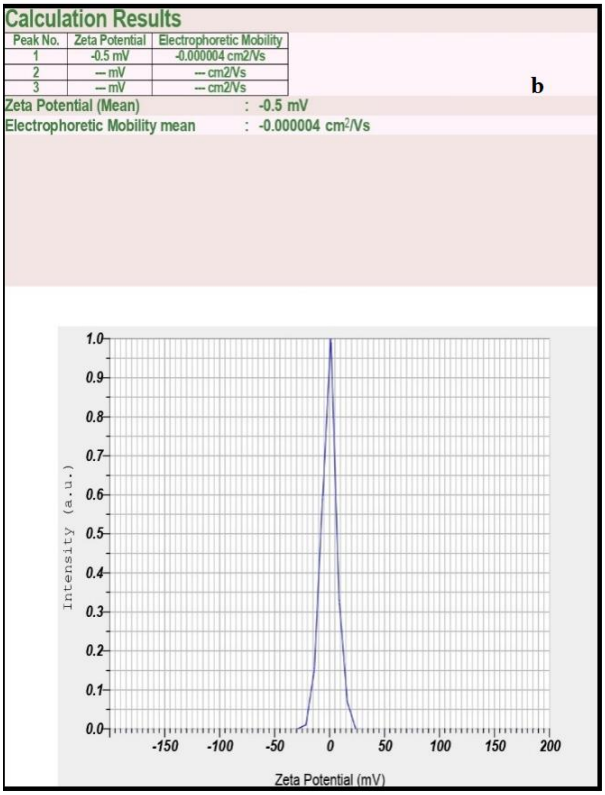

Figure 2 (b) zeta potential of the optimized formulation

***In vitro* drug release:** The *in vitro* drug release of the optimized formulation & pure CSSO are compared and it is found to be 70.86% & 48.26% and it is represented in figure 3. Here, it is observed that increase in drug and polymer concentration & stirring time increases the % cumulative drug release.

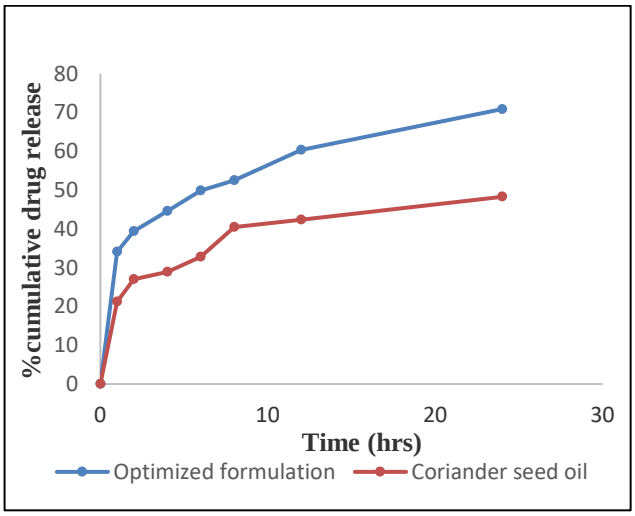

Figure 3: % Cumulative drug release of pure Coriandrum sativum seed oil and optimized formulation

Determination of CMC of the optimized formulation: Low CMC value indicates that the polymeric micelles are highly stable and maintains the integrity after dilution in the body. CMC was determined by plotting the absorbance Vs polymer concentration (µg/ml) as shown in figure 4. The CMC value of the optimized formulation was found to be 0.8µg/ml. Hence, the optimized formulation is stable.

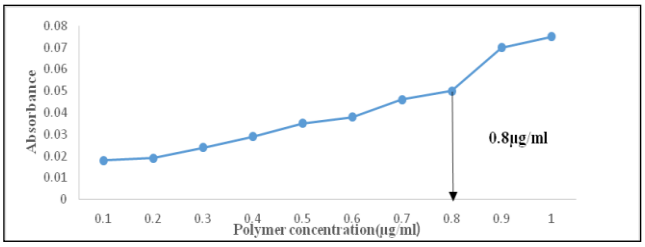

***Figure 4:** CMC of the optimized formulation*

p^{H} of the optimized formulation: Measurement of p^{H} is very important for the oral preparations, where it may lead to GIT irritation. P^{H} of the optimized formulation was found to be in a neutral range of 7.7±0.1.

Drug release kinetics: The *in vitro* drug release data of optimized formulation is fitted in different mathematical models as shown figure 5. The model with highest R^2 value is considered as best one. According to the data the model meeting criterion is first order with R^2 value 0.974. The polymeric micelles had shown sustained release characters. The drug release data is fitted with Higuchi (R^2 value -0.99) & the released mechanism of polymeric micelles containing *Coriandrum sativum* seed oil might be drug diffusion and dissolution as shown in Figure 5.

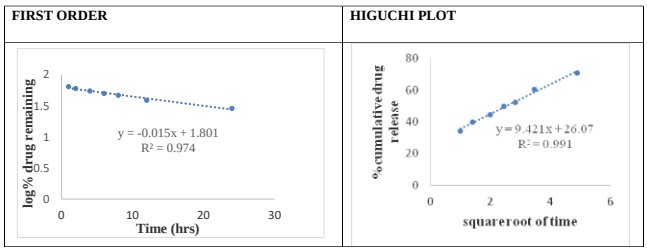

Figure-5 Drug release kinetics of polymeric micelles containing Coriandrum sativum seed oil.

Drug-excipient compatibility studies (FT-IR) analysis of the optimized formulation

FTIR spectra of *Coriandrum sativum* seed oil along with *Coriandrum sativum* seed oil + polymer mixture was compared, it can be noticed that, the absence of additional peaks, which indicates that, the polymer and *Coriandrum sativum* seed oil are compatible to each other.

***In-vitro* antibacterial activity:** The *in-vitro* antibacterial activity of polymeric micelles containing *Coriandrum sativum* seed oil was compared with the marketed ciprofloxacin tablet 500mg tablet i.e. standard and *Coriandrum sativum* seed oil. The activity in terms of zone of inhibition is given in the Table 8

Table 8: Results of In vitro antibacterial activity

Formulation	**Zone of inhibition (cm) Mean ± S.D**			
	Staphy-lococcus aureus	**Proteus**	**E.coli**	**Bacillus subtilis**
Test formulation	2.3±0.1	1.5±0.2	1.2±0.1	2.0±0.3
Marketed formulation	1.2±0.2	1.4±0.3	1.0±0.3	1.8±0.1
Coriandrum sativum seed oil	1.0±0.05	1.2±0.01	1.0±0.03	0.4±0.01

The polymeric micelles exhibits a high zone of inhibition when compared with that of CSSO and positive control antibiotic i.e. ciprofloxacin. Presence of CSSO increased the antibacterial activity of polymeric micelles against both gram positive and gram negative bacteria. In this study two strains of gram positive bacteria i.e. *Staphylococcus aureus & Bacillus subtilis* and two strains of gram negative bacteria i.e. *Proteus vulgaris & Escherichia coli* were taken. Polymeric micelles containing CSSO i.e. test formulation was more effective against gram positive bacteria with high zone of inhibition.

Conclusion

Polymeric micelles containing *Coriandrum sativum* seed oil were formulated by solvent diffusion technique & Box-Behnken response surface methodology was selected in order to investigate the effect of independent variables on responses. The optimized formulation of polymeric micelles has low CMC, smaller particle size and negative zeta potential, high % entrapment efficiency and spherical in shape. Low CMC suggests stability of micelles upon

dilution. Polymeric micelles containing *Coriandrum sativum* seed oil had shown high drug release, *in-vitro* drug release kinetics follows first order, so the formulation shows sustained release characters and the drug release mechanism is drug diffusion and dissolution of polymer material. The FT-IR analysis demonstrated no drug-excipient interactions. Formulated polymeric micelles were stable during the period of study and there were no alterations. The prepared polymeric micelles had shown antibacterial activity against gram positive and gram-negative bacteria with high zone of inhibition. The results obtained in proposed research polymeric micelles containing *Coriandrum sativum* seed oil enhances the solubility and ultimately enhanced the bioavailability.

References

[1] Luo, Yali, et al. "Preparation and drug controlled-release of polyion complex micelles as drug delivery systems." *Colloids and Surfaces B: Biointerfaces* 68.2 (2009): 218-224.

[2] Voets, Ilja K., et al. "Irreversible structural transitions in mixed micelles of oppositely charged diblock copolymers in aqueous solution." *Macromolecules* 40.6 (2007): 2158-2164.

[3] Deepak, Payal, et al. "Polymeric micelles: potential drug delivery devices." *Indonesian Journal of Pharmacy* (2013): 222-237.

[4] Kahraman, Emine, Sevgi Güngör, and Yıldız Özsoy. "Potential enhancement and targeting strategies of polymeric and lipid-based nanocarriers in dermal drug delivery." *Therapeutic delivery* 8.11 (2017): 967-985.

[5] Riess, Gerard. "Micellization of block copolymers." *Progress in polymer science* 28.7 (2003): 1107-1170.

[6] Jones, Marie-Christine, and Jean-Christophe Leroux. "Polymeric micelles–a new generation of colloidal drug carriers." *European journal of pharmaceutics and biopharmaceutics* 48.2 (1999): 101-111.

[7] Barbouchi, Mohammed, et al. "Chemical composition and physicochemical properties of the essential oil of coriander (Coriandrum sativum L.) grown in Morocco." *RHAZES: Green and Applied Chemistry* 4.4 (2019): 35-50.

[8] Pathak, N. I., S. B. Kasture, and N. M. Bhatt. "Phytochemical screening of Coriander sativum Linn." *Int J Pharm Sci Rev Res* 9.2 (2011): 159-163.

[9] Fatema, Samreen, *et al*. "Phytochemical and Physicochemical analysis of Microwave-assisted extraction *Coriandrum sativum L*. leaves and its Biological evaluation." *Asian J Pharm Clin Res* 12.5 (2019): 289-291.

[10] Mohite, Shraddha, and Anuradha Salunkhe. "Formulation and evaluation of Emulgel containing Coriandrum sativum seeds oil for Anti-inflammatory activity." *Journal of Drug Delivery and Therapeutics* 9.3-S (2019): 124-130.

[11] Patel, Krutika, and Mita Vakilwala. "Phytochemical study and bioactivity of solvent extracts on Coriandrum sativum." *Int. J. Adv. Res. Biol. Sci* 3.5 (2016): 193-199.

[12] Andalib, Sina, Pezhman Molhemazar, and Hossein Danafar. "In vitro and in vivo delivery of atorvastatin: A comparative study of anti-inflammatory activity of atorvastatin loaded copolymeric micelles." *Journal of biomaterials applications* 32.8 (2018): 1127-1138.

[13] Nejad Ebrahimi, Samad, Javad Hadian, and Hamid Ranjbar. "Essential oil compositions of different accessions of Coriandrum sativum L. from Iran." *Natural product research* 24.14 (2010): 1287-1294.

[14] Li, Xingyi, *et al. "*Diclofenac/biodegradable polymer micelles for ocular applications." *Nanoscale* 4.15 (2012): 4667-4673.

[15] Patra, Arjun, *et al.* "Formulation and evaluation of mixed polymeric micelles of quercetin for treatment of breast, ovarian, and multidrug resistant cancers." *International journal of nanomedicine* (2018): 2869-2881.

[16] Abdollahi, Amir Reza, *et al. "*Indomethacin loaded dextran stearate polymeric micelles improve adjuvant-induced arthritis in rats: Design and in vivo evaluation." *Inflammopharmacology* 29 (2021): 107-121.

[17] Aliabadi, Hamidreza Montazeri, and Afsaneh Lavasanifar. "Polymeric micelles for drug delivery." *Expert opinion on drug delivery* 3.1 (2006): 139-162.

[18] Gou, MaLing, *et al.* "Self-assembled hydrophobic honokiol loaded MPEG-PCL diblock copolymer micelles." *Pharmaceutical research* 26 (2009): 2164-2173.

[19] Nie, K. B., *et al.* "Processing, microstructure and mechanical properties of magnesium matrix nanocomposites fabricated by semisolid stirring assisted ultrasonic vibration." *Journal of alloys and compounds* 509.35 (2011): 8664-8669.

GAMANAM
Volume 1, Issue 1, January 2025

Research Paper

Green Synthesis of Chitosan-Functionalized Zinc Oxide Nanoparticles - A Novel Antimicrobial Agent

[1]Harika Katepogu, [2*]P Josthna, [2]M Shakari, [2]Dara Josphin, [2]P.Bharathi, [1]Shilpa Nayuni

[1]Arran Scientific, Madanapalle, Annamayya Dt, Andhra Pradesh
[2]Department of Biotechnology, Sri Padmavati Mahila Visvavidyalayam, Tirupati

**Corresponding Author(s): penchalajyo@yahoo.co.in*

Received: 26/11/2024, Revised: 18/12/2024, Accepted:24/12/2024 Published:01/01/2025

Abstract: This study presents a green synthesis method for Chitosan-functionalized zinc oxide (ZnO) nanoparticles using guava (Psidium guajava) leaf extract and Chitosan, a natural polymer derived from chitin. The eco-friendly approach leverages guava extract as a reducing and stabilizing agent and Chitosan to enhance nanoparticle stability and bioactivity. Synthesized ZnO nanoparticles exhibited a crystalline structure with sizes ranging from 14–28 nm, confirmed by XRD analysis, and a characteristic UV-Visible absorption peak at 335 nm. The antimicrobial activity of the nanoparticles was evaluated against E. coli, S. aureus, and S. enterica using a disc diffusion assay. Significant inhibition zones were observed, particularly at higher nanoparticle concentrations, indicating strong antibacterial potential. The mechanism involves oxidative stress induction and bacterial membrane disruption. This green synthesis approach provides an effective and sustainable alternative to combat antimicrobial resistance, aligning with green chemistry principles to minimize environmental impact.

Keywords: Green synthesis, Chitosan-functionalized ZnO nanoparticles, Antimicrobial activity, Guava extract

1 Introduction

According to the Merriam-Webster Medical Dictionary, an antimicrobial is an agent that prevents or stops the growth of pathogenic microorganisms or even kills them [Kingston, *et al.,2008*]. Antimicrobial agents have been used for at least 2000 years, originating in the time of the Ancient Egyptians. These agents play a critical role in treating infectious diseases and are essential in modern medicine. They can be classified based on their target organisms, chemical structure, mode of action, or source of origin. To date, many types of antimicrobials have been developed, classified based on their target organisms and mode of action. Examples based on target organisms include: antibacterial agents (targets bacteria) such as penicillin, tetracycline, antivirals (target viruses) such as acyclovir, oseltamivir, antifungals (target fungi) such as fluconazole, amphotericin B, antiparasitics (target parasites) such as ivermectin, chloroquine. Examples based on mode of action include bactericidal agents (kill bacteria) such as beta-lactams, aminoglycosides, bacteriostatic agents (inhibit bacterial growth) such as tetracyclines, sulfonamides. Antimicrobial agents typically work by inhibiting cell wall synthesis, nucleic acid synthesis, or metabolic pathways. In recent times, antimicrobial resistance has become a major global health threat, primarily caused by the overuse or misuse of antimicrobials. Ideal antimicrobial agents should target microorganisms without harming the host, while factors such as absorption, distribution, metabolism, and excretion influence their efficacy. A modern approach to combating antimicrobial resistance would involve finding new targets or using alternative antimicrobials, either natural or synthetic compounds [Mantravadi, *et al*., 2019].

Nanoparticles are a new generation of antimicrobial agents that are being explored. One of the established relationships between nanomaterials and antibacterial activity is as follows: “Nanomaterials as antibacterial complements to antibiotics are highly promising and gaining significant interest as they may address the limitations where antibiotics often fail” [*Mohanpuria et al.,2007*]. Additionally, nanomaterials can complement and support traditional antibiotics “as effective carriers” [*Sunagawa et al., 2004*]. This section focuses on the unique features and complementary advantages of using nanomaterials in antimicrobial applications.

Green synthesis of Nanoparticles aims to promote innovative chemical technologies that reduce or eliminate the use and production of hazardous substances in the design, manufacture, and application of chemical products. This approach focuses on minimizing, or ideally,

eliminating, pollution produced during synthesis, avoiding the consumption and waste of non-renewable raw materials, using safer alternatives in product manufacturing, and reducing synthesis time (*Paul Anastas, et al.,2004*).

Guava (*Psidium guajava)* is a Phyto therapeutic plant used in folk medicine, believed to contain active components that help treat and manage various diseases. Many parts of the plant have been used in traditional medicine to manage conditions such as malaria, gastroenteritis, vomiting, diarrhea, dysentery, wounds, ulcers, toothaches, coughs, sore throat, inflamed gums, and several other conditions [Jaiarj and Khoohaswan., *et al., 1999*]. This plant has also been used to control life-changing conditions like diabetes, hypertension, and obesity [South-East Asian *et al., 2006*]. Guava is increasingly being explored as a natural source for the green synthesis of nanoparticles (NPs). Extracts from guava leaves, fruits, and bark contain phytochemicals such as flavonoids, tannins, and polyphenols, which act as reducing and stabilizing agents in nanoparticle synthesis.

Chitosan, a natural antimicrobial agent found in the shells of crustaceans, such as crabs, shrimp, squid pens, and crawfish (No *et al. 2002*). Recently, some studies have suggested the possibility of producing Chitosan from fungi. In one study, Chitosan was extracted from the cell wall of filamentous fungus, *R. oryzae*, (Jeihanipour *et al., 2007*) and its antimicrobial properties were studied against *E. coli, K. pneumoniae and S. aureus* (Hosseinnejad and Jafari, *2016)*. Guava (*Psidium guajava*) and Chitosan, a natural polymer derived from chitin (found in crustacean shells), offer complementary properties that make them ideal candidates for applications in nanotechnology. Both materials are biocompatible, biodegradable, and rich in bioactive compounds, enabling their combined use in the synthesis and functionalization of nanoparticles (NPs) for antimicrobial, pharmaceutical, and environmental applications

ZnO nanoparticles are believed to be among the three most produced nanomaterials, alongside titanium dioxide nanoparticles and silicon dioxide nanoparticles (Zhang, Yuanyuan, *et al., 2015*). The most common use of ZnO nanoparticles is in sunscreen. ZnO nanoparticles have been shown to exhibit properties such as anti-cancer, antidiabetic, antibacterial, antifungal, anti-inflammatory activities.

Considering the activities and benefits of guava, Chitosan, and zinc nanoparticles, this work will explore the green synthesis of Chitosan-functionalized zinc oxide nanoparticles as a novel antimicrobial agent.

Materials and Methods

Materials

Zinc acetate (0.1983g), Guava plant extract (22g), NaOH, Chitosan (1g), Acetic acid (10ml) NaoH, 1% Citric acid, Agar broth, Antibiotic disc, Eppendorf tubes, Inoculums, Forceps, Metric ruler, Bunsen burner, Cotton swab, Pipettes, Glass rod.

Methods

Collection of Plants

Fresh leaves of *Psidium guajava* (guava) were collected from the open areas of Arran Science Laboratory, Valasapalli, Chittoor district. The collected leaves were washed with running tap water, followed by distilled water, and then dried at room temperature.

Preparation of plant extract

The plant extract was prepared by grinding 22g of leaves into a paste using an electric mixer. A leaf broth solution was prepared by adding 220ml of distilled water to the 22g of plant paste in a 1:10 ratio. The mixture was then filtered through standard filter paper, with Whatman No. 1 filter paper. The remaining extract was stored at 4°C for further experiments.

Figure 1: Guava extract

Preparation of stock solution

To 500 ml of distilled water, 10 ml (0.9183g) of zinc acetate was added. The mixture was stirred using a magnetic stirrer to form a stock solution.

Biosynthesis of zinc oxide nanoparticles (ZnO NPs):

To 50 ml of the prepared zinc acetate solution, 10 ml of the plant extract was added dropwise until the solution becomes colourless or turned white. NaOH was then added to bring the pH to 10. The solution was placed on a hot plate to form powder.

Figure 2: Zinc acetate

Preparation of Chitosan:

A 1g of chitosan was mixed in 100ml of distilled water. Since distilled water cannot dissolve Chitosan, acetic acid was added drop by drop until a clear solution was obtained.

Then, 30ml of Chitosan solution was mixed with 30ml of plant extract with zinc acetate. The solution was stirred for 24 hours with a magnetic stirrer. After that, it was autoclaved for 15 minutes at 121^0C. Once cooled, the solution was stored in the refrigerator for 24 hours. To allow the solution to form a powder, it was transferred into a Petri dish and placed on the hot plate at 70^0C until the liquid evaporated.

Figure 3: Chitosan

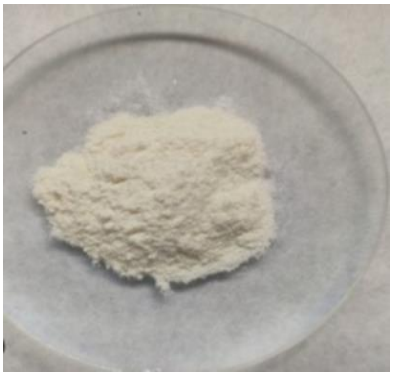

Figure 4: Chitosan Powder

Preparation of Guava-Chitosan stabilized zinc nanoparticle solution for antimicrobial activity:

A 1% citric acid solution (20 mL) was added to 30 mL of the prepared Guava-Chitosan stabilized zinc nanoparticle solution. Serial dilutions were then prepared by taking 25 µL, 50 µL, 75 µL, and 100 µL of the nanoparticle solution, respectively, and diluting them accordingly.

Figure 5: Guava- Chitosan stabilized Zinc nanoparticles with citric acid solution

Table 1: Chitosan dilution concentrations

S.No	Chitosan Solution	Water
1	100µl	-
2	75µl	25µl
3	50µl	50µl
4	25µl	75µl

Disc diffusion assay:

The working area was sterilised with disinfectant, and sterile cotton was soaked in the inoculum. The excess medium was removed, and the inoculum was aspirated by pressing the swab against the wall of the tube. Afterward, the plate was dried for 5 minutes to allow proper inoculation detection. Forceps were sterilized with alcohol before handling the antibiotic discs. The antibiotic discs were placed in the centre of the plate. Holes were made on the four sides of the plate using the tips. Then prepared solution was added slowly, drop by drop, and the plates were incubated upside down for 24 hours at 37°C. After 24 hours of incubation, the zone of inhibition was measured with a scale and the diameter was recorded.

Results and Discussion:

The synthesis of Chitosan stabilized zinc nanoparticles was observed through a colour change from a colourless solution to a white colour coloured solution as shown in the Fig 6. The green synthesised Chitosan/ZnO nanoparticles transitioned from colourless to a milky solution, as shown in Figure 7. The first attempt at synthesizing ZnO nanoparticles involved reducing zinc nitrate with sodium hydroxide (NaOH) without using a stabilizing agent, leading to agglomeration and a non-homogeneous solution. This can be explained by the addition of zinc nitrate to the NaOH solution, produces a milky precursor solution. This is the initial stage of the zinc nitrate reduction reaction, where zinc nitrate dissociates into Zn^{2+} and NO_3^- ions. After stirring for several minutes, suspensions formed in the solution due to the agglomeration process. Without a stabilizing agent to coat the nanoparticle surfaces,

agglomeration began to occur. If the reduction process precedes the interaction with the stabilizing agent, nanoparticle growth cannot be effectively controlled, leading to clusters.

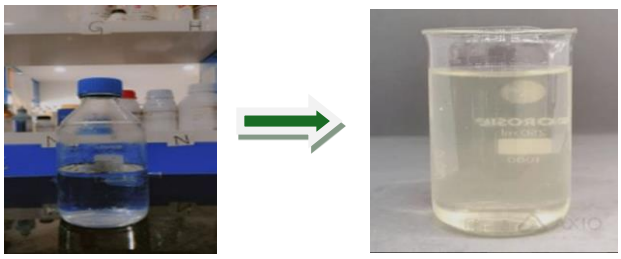

Fig 6: Colour changes from colourless to white colour

Fig 7: Guava plant extract

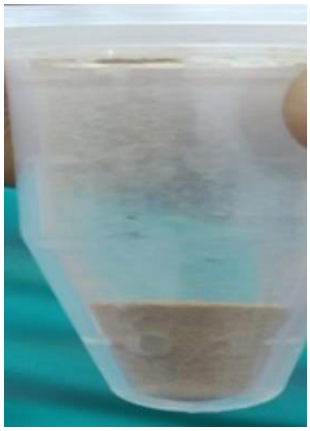

Fig 8: Zn acetate powder

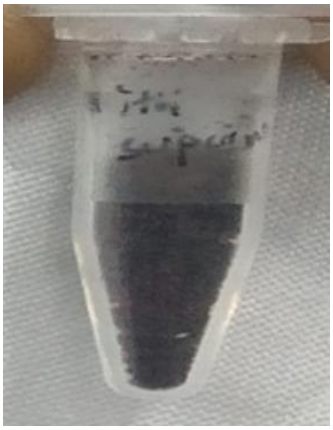

Fig 9: Chitosan stabilized Zn powder

XRD analysis:

XRD analysis of Zinc with Chitosan:

The XRD pattern of Chitosan-stabilised ZnO showed intense peaks at 2θ values of 28.4304, 29.1562, 30.9185, 41.5382. The particle size of ZnO with Chitosan is 28.4304nm.

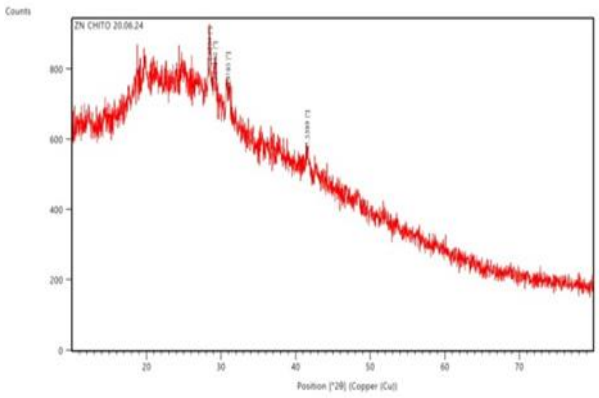

Fig:10: XRD pattern of zinc with Chitosan

XRD analysis of Zinc NPS with *Psidium guajava*:

The XRD pattern of ZnO NPs synthesized using ***Psidium guajava*** extract showed intense peaks at 2θ values of 14.2576, 28.4202 and 31.2820 The particle size of ZnO NPs synthesized by *Psidium guajava* is 14.2576nm.

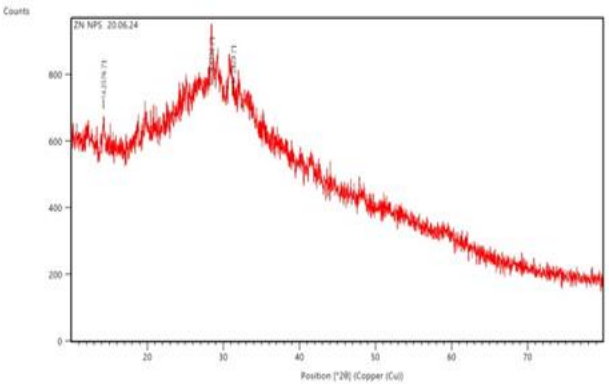

Fig 11: XRD pattern of zinc NPs by *Psidium guajava*

XRD analysis of Stabilized ZnO with *Psidium guajava*:

The XRD pattern of ZnO NPs synthesized using ***Psidium guajava*** extract showed intense peaks at 2θ values of 14.3469, 18.6823, 19.8046, 24.9359, 26.7010, 29.1592, 30.9674. The particle size of stabilized ZnO NPs by *Psidium guajava* is 14.3469nm.

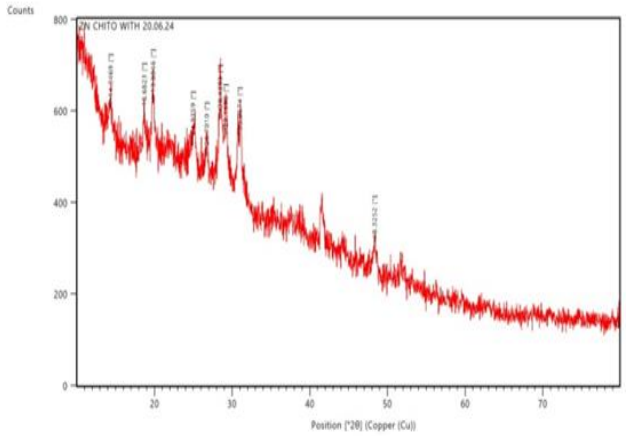

Fig 12: XRD pattern of stabilized ZnO NPs by *Psidium guajava*

The analysis aimed to determine the size of various crystalline forms of nanoparticles. The XRD patterns confirmed that the Chitosan/ZnO nanoparticles exhibited a well-defined crystalline structure. Comparison of the XRD spectra with the standard peaks from the JCPDS files showed excellent matching for all samples. No impurities were observed in the characteristic peaks, indicating the purity of the synthesized nanoparticles. The choice of Chitosan as the stabilizing polymer was validated, as it effectively prevented aggregation and sedimentation. The average crystallite size of the Chitosan/ZnO nanoparticles calculated using the Debye Scherrer formula.

UV-Visible spectroscopy:

The UV-Visible spectrum analysis of Chitosan-stabilized ZnO nanoparticles showed distinct absorption peaks, indicative of their unique optical properties. A prominent absorption peak was observed at 335 nm, characteristic of ZnO nanoparticles. This peak indicates the presence of ZnO in its nanoparticulate form and corresponds to the band gap transition. The position and intensity of the absorption peak suggest that the size and optical behaviour of the nanoparticles are influenced by the stabilizing effect of Chitosan**.**

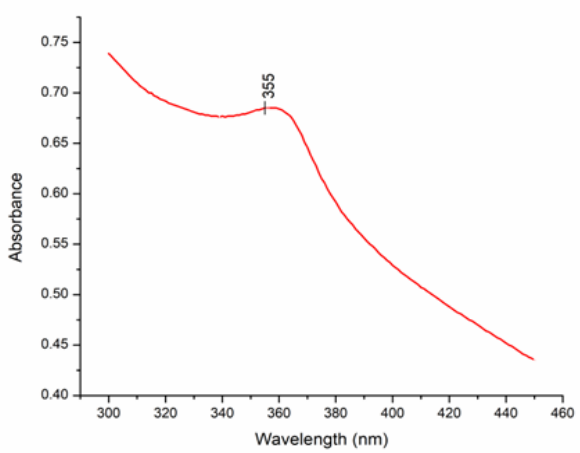

Figure 13: UV-visible Spectra of synthesized nanoparticles

Anti-microbial activity:

The anti-microbial activity of Chitosan-stabilized ZnO nanoparticles was evaluated against three bacterial strains: *E. coli*, *S. aureus*, and *S. enterica* as shown in table 2. The zones of inhibition were observed to increase with higher concentrations of nanoparticles, showing a dose-dependent response. At the highest concentration (100 µL), the largest zones of inhibition were recorded for *S. aureus* (21 mm) and *S. enterica* (23 mm), indicating strong antibacterial effects. *E. coli* also showed a significant inhibition zone of 21 mm at the same concentration. These results confirmed that Chitosan-stabilized ZnO nanoparticles were effective against both Gram-positive and Gram-negative bacteria. In comparison, the control group with a standard antibiotic showed consistent inhibition zones of 20 mm across all bacterial strains, suggesting similar antimicrobial activity between the nanoparticles and the antibiotic. At lower nanoparticle concentrations, *S. aureus* displayed the smallest zones of inhibition, while *S. enterica* showed a more prominent increase in inhibition as the nanoparticle concentration rose. Overall, the findings support the potential of Chitosan-stabilized ZnO nanoparticles as effective antibacterial agents, with higher concentrations providing stronger antimicrobial effects.

Table 2: Antimicrobial activity of different concentrations of green synthesised Chitosan-stabilized ZnO nanoparticles against three bacterial strains: *E. coli*, *S. aureus*, and *S. enterica*.

S.No	Concentration (µl)	Zone of inhibition (*E. coli*) (mm)	Zone of inhibition (*S. aureus*) (mm)	Zone of inhibition (*S. enterica*) (mm)
1	25	17	5	14
2	50	18	13	17
3	75	20	17	19
4	100	21	21	23
5	Control	20	20	20

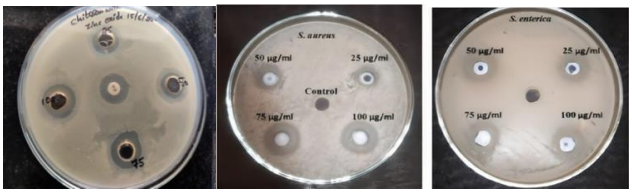

Fig 14: Antimicrobial activity of silver nanoparticles against *E. coli*, *S. aureus* and *S. enterica*

Conclusion

Zinc oxide (ZnO) nanoparticles were synthesized through a green synthesis method, using zinc acetate dihydrate and an extract from guava leaves. The resulting nanoparticles had an average crystallite size of 14.13 nm. The antibacterial activity of the Chitosan-stabilized ZnO nanoparticles was tested in vitro, showing notable effectiveness against both Gram-positive and Gram-negative bacterial strains. The observed antibacterial action is likely due to the nanoparticles ability to generate reactive oxygen species (ROS), induce oxidative stress, and physically damage bacterial cell membranes, ultimately leading to bacterial inhibition or cell death.

References

[1] Abdelrahim, S. I., Almagboul, A. Z., Omer, M. E. A., & Elegami, A. (2002). Antimicrobial activity of *Psidium guajava L*. *Fitoterapia*, *73*(7-8), 713-715.

[2] Abdel-Mawgoud, A. M. R., Tantawy, A. S., El-Nemr, M. A., & Sassine, Y. N. (2010). Growth and yield responses of strawberry plants to chitosan application. *European Journal of Scientific Research*, *39*(1), 170-177.

[3] Anastas, P. T., & Warner, J. C. (2000). *Green chemistry: theory and practice*. Oxford university press.

[4] Arumugam, A., Karthikeyan, C., Hameed, A. S. H., Gopinath, K., Gowri, S., & Karthika, V. (2015). Synthesis of cerium oxide nanoparticles using Gloriosa superba L. leaf extract and their structural, optical and antibacterial properties. *Materials Science and Engineering: C*, *49*, 408-415.

[5] Beveridge, T. J. (1999). Structures of gram-negative cell walls and their derived membrane vesicles. *Journal of bacteriology*, *181*(16), 4725-4733.

[6] Burkill H. M.,(1997) The Useful Plants of West Tropical Africa, 2nd edition

[7] Chen, R. H., Domard, A., Muzzarelli, R. A., Tokura, S., & Wang, D. M. (2011). Advances in chitin/chitosan science and their applications. *Carbohydrate polymers*, *2*(84), 695.

[8] Daniel, M. C., & Astruc, D. (2004). Gold nanoparticles: assembly, supramolecular chemistry, quantum-size-related properties, and applications toward biology, catalysis, and nanotechnology. *Chemical reviews*, *104*(1), 293-346.

[9] Dhillon, G. S., Brar, S. K., Kaur, S., & Verma, M. (2012). Green approach for nanoparticle biosynthesis by fungi: current trends and applications. *Critical reviews in biotechnology*, *32*(1), 49-73.

[10] Durand, G. A., Raoult, D., & Dubourg, G. (2019). Antibiotic discovery: history, methods and perspectives. *International journal of antimicrobial agents*, *53*(4), 371-382.

[11] Fleming, A. (1929). On the antibacterial action of cultures of a penicillium, with special reference to their use in the isolation of B. influenzae. *British journal of experimental pathology*, *10*(3), 226.

[12] Jaiarj, P., Khoohaswan, P., Wongkrajang, Y., Peungvicha, P., Suriyawong, P., Saraya, M. S., & Ruangsomboon, O. (1999). Anticough and antimicrobial activities of *Psidium guajava* Linn. leaf extract. *Journal of Ethnopharmacology*, *67*(2), 203-212.

[13] Jiang, J., Pi, J., & Cai, J. (2018). The advancing of zinc oxide nanoparticles for biomedical applications. *Bioinorganic chemistry and applications*, *2018*(1), 1062562.

[14] Kaushik N, Thakkar MS, Snehit S, Mhatre MS, Rasesh Y, Parikh MS (2010) Biological synthesis of metallic nanoparticles. NanomedNanotechnolBiol Med 6:257–262

[15] Kingston, W. (2008). Irish contributions to the origins of antibiotics. *Irish journal of medical science*, *177*, 87-92.

[16] Kong, M., Chen, X. G., Xing, K., & Park, H. J. (2010). Antimicrobial properties of chitosan and mode of action: a state of the art review. *International journal of food microbiology*, *144*(1), 51-63.

[17] Korbekandi, H., Iravani, S., & Abbasi, S. (2009). Production of nanoparticles using organisms. *Critical reviews in biotechnology*, *29*(4), 279-306.

[18] Bogunia-Kubik, K., & Sugisaka, M. (2002). From molecular biology to nanotechnology and nanomedicine. *Biosystems*, *65*(2-3), 123-138.

[19] Kumariya, R., Sood, S. K., Rajput, Y. S., Saini, N., & Garsa, A. K. (2015). Increased membrane surface positive charge and altered membrane fluidity leads to cationic antimicrobial peptide resistance in Enterococcus faecalis. *Biochimica et Biophysica Acta (BBA)-Biomembranes*, *1848*(6), 1367-1375.

[20] Iosub, C. Ș., Olăreț, E., Grumezescu, A. M., Holban, A. M., & Andronescu, E. (2017). Toxicity of nanostructures—a general approach. In *Nanostructures for Novel Therapy* (pp. 793-809). Elsevier.

[21] Lo, W. H., Deng, F. S., Chang, C. J., & Lin, C. H. (2020). Synergistic antifungal activity of chitosan with

fluconazole against Candida albicans, Candida tropicalis, and fluconazole-resistant strains. *Molecules*, *25*(21), 5114.

[22] Mantravadi, P. K., Kalesh, K. A., Dobson, R. C., Hudson, A. O., & Parthasarathy, A. (2019). The quest for novel antimicrobial compounds: emerging trends in research, development, and technologies. *Antibiotics*, *8*(1), 8.

[23] Makarov, V. V., Love, A. J., Sinitsyna, O. V., Makarova, S. S., Yaminsky, I. V., Taliansky, M. E., & Kalinina, N. O. (2014). "Green" nanotechnologies: synthesis of metal nanoparticles using plants. *Acta Naturae (англоязычная версия)*, *6*(1 (20)), 35-44.

[24] Mohanpuria, P., Rana, N. K., & Yadav, S. K. (2008). Biosynthesis of nanoparticles: technological concepts and future applications. *Journal of nanoparticle research*, *10*, 507-517.

[25] Mukherjee, P., Ahmad, A., Mandal, D., Senapati, S., Sainkar, S. R., Khan, M. I., ... & Sastry, M. (2001). Fungus-mediated synthesis of silver nanoparticles and their immobilization in the mycelial matrix: a novel biological approach to nanoparticle synthesis. *Nano letters*, *1*(10), 515-519.

[26] Ncube, N. S., Afolayan, A. J., & Okoh, A. I. (2008). Assessment techniques of antimicrobial properties of natural compounds of plant origin: current methods and future trends. *African journal of biotechnology*, *7*(12).

[27] No, H. K., Kim, S. H., Lee, S. H., Park, N. Y., & Prinyawiwatkul, W. (2006). Stability and antibacterial activity of chitosan solutions affected by storage temperature and time. *Carbohydrate polymers*, *65*(2), 174-178.

[28] Noorian, S. A., Hemmatinejad, N., & Navarro, J. A. (2020). Ligand modified cellulose fabrics as support of zinc oxide nanoparticles for UV protection and antimicrobial activities. *International journal of biological macromolecules*, *154*, 1215-1226.

[29] Pasquina-Lemonche, L., Burns, J., Turner, R. D., Kumar, S., Tank, R., Mullin, N., ... & Hobbs, J. K. (2020). The architecture of the Gram-positive bacterial cell wall. *Nature*, *582*(7811), 294-297.

[30] Peña, A., Sánchez, N. S., & Calahorra, M. (2013). Effects of chitosan on Candida albicans: conditions for its antifungal activity. *BioMed research international*, *2013*(1), 527549.

[31] Raafat, D., Von Bargen, K., Haas, A., & Sahl, H. G. (2008). Insights into the mode of action of chitosan as an antibacterial compound. *Applied and environmental microbiology*, *74*(12), 3764-3773.

[32] Raetz, C. R., Reynolds, C. M., Trent, M. S., & Bishop, R. E. (2007). Lipid A modification systems in gram-negative bacteria. *Annu. Rev. Biochem.*, *76*(1), 295-329.

[33] Richard, I., Thibault, M., De Crescenzo, G., Buschmann, M. D., & Lavertu, M. (2013). Ionization behavior of chitosan and chitosan–DNA polyplexes indicate that chitosan has a similar capability to induce a proton-sponge effect as PEI. *Biomacromolecules*, *14*(6), 1732-1740.

[34] Sarwar, S. B., Khondokar, F., Islam, H., Ullah, M. A., Araf, Y., Sarkar, B., & Rahman, H. (2021). Assessing drug repurposing option for emerging viral diseases: concerns, solutions, and challenges for forthcoming viral battles. *J. adv. biotechnol. exp ther*, *4*, 74-94.

[35] Sato, T., Ishii, T., & Okahata, Y. (2001). In vitro gene delivery mediated by chitosan. Effect of pH, serum, and molecular mass of chitosan on the transfection efficiency. *Biomaterials*, *22*(15), 2075-2080.

[36] Sengupta, S., Chattopadhyay, M. K., & Grossart, H. P. (2013). The multifaceted roles of antibiotics and antibiotic resistance in nature. *Frontiers in microbiology*, *4*, 47.

[37] Singh, J., Dutta, T., Kim, K. H., Rawat, M., Samddar, P., & Kumar, P. (2018). 'Green'synthesis of metals and their oxide nanoparticles: applications for environmental remediation. *Journal of nanobiotechnology*, *16*, 1-24.

[38] South-East Asian (SEA), Regional Workshop on Extraction Technologies for Medicinal and Aromatic Plants, 2006.

[39] Sunagawa, M., Shimada, S., Zhang, Z., Oonishi, A., Nakamura, M., & Kosugi, T. (2004). Plasma insulin concentration was increased by long-term ingestion of guava juice in spontaneous non-insulin-dependent diabetes mellitus (NIDDM) rats. *Journal of Health Science*, *50*(6), 674-678.

[40] Wainwright, M. (2008). Some highlights in the history of fungi in medicine–A personal journey. *Fungal Biology Reviews*, *22*(3-4), 97-102.

[41] Xing, K., Zhu, X., Peng, X., & Qin, S. (2015). Chitosan antimicrobial and eliciting properties for pest control in agriculture: a review. *Agronomy for Sustainable Development*, *35*, 569-588.

[42] Zaharoff, D. A., Rogers, C. J., Hance, K. W., Schlom, J., & Greiner, J. W. (2007). Chitosan solution enhances both humoral and cell-mediated immune responses to subcutaneous vaccination. *Vaccine*, *25*(11), 2085-2094.

GAMANAM
Volume 1, Issue 1, January 2025

Survey Paper

Enhancing Education with AI

[1] Dr.Sandhya Madhuri G, [2] K.V.Sai Kumar Reddy, [3] Dr. K Pavithra
[1]*Asst Professor, Dept.of Computer Applications, Dayananda Sagar University, Bengaluru, India*
[2]*Dept. of Data Science, Geetam University, Hyderabad, India*
[3]*Asst Professor, Dept of Computer Science & Engg, Alliance University,* Bengaluru, India

**Corresponding Author(s): saikumarreddy.kondla@gmail.com*

Received: 26/11/2024, Revised: 16/12/2024, Accepted:23/12/2024 Published:01/01/2025

Abstract: This study intends to offer a thorough examination of the Indian educational system and the possible advantages of implementing ChatGPT, a sophisticated language model, in educational contexts. The study analyses the positives and negatives of the current Indian educational system, stresses the difficulties experienced by students and teachers, and looks at how technology might help to solve these problems. Additionally, it explores ChatGPT's potential and looks into how it might be used to improve learning outcomes and promote academic advancement. This study offers important insights into the possibility of utilising technology to revolutionize education in India by assessing the Indian educational system and the integration of ChatGPT.

Keywords: Component, Formatting, Style, Styling, Insert

1 Introduction

The Indian educational system is extremely important to the future of the country, yet it has a lot of difficulties ensuring that all students receive an equitable and high-quality education. Technology has emerged as a possible game-changer in recent years, giving creative solutions to get past these barriers. The use of ChatGPT, a sophisticated language model, in educational settings is one such development. In order to improve learning outcomes, this research article will examine the possible advantages of implementing ChatGPT in the Indian educational system. We can plough the way for a more inclusive and successful education environment in India by analysing the benefits and drawbacks of the current system and assessing ChatGPT's capabilities.

Indian Education System: Strengths and Weaknesses

The Indian educational system has several advantages and includes a huge network of educational institutions. First of all, it has a vast infrastructure that guarantees universal accessibility to education throughout the nation. Second, the system places a lot of emphasis on fundamental courses, giving students a solid foundation in subjects like maths, physics, and foreign languages. Additionally, the culture of competitive tests, like JEE and NEET, emphasises academic performance and pushes students to pursue their goals. Additionally, the use of technology, such as digital tools and e-learning platforms, has improved learning and increased access to educational resources [1].

However, there are a number of flaws in the Indian educational system as well. Access and equity are still major challenges because there are still differences between urban and rural areas, as well as across different societal classes. The prominence of rote learning curtails pupils' ability to think critically and creatively, impeding their ability to acquire crucial skills for the future. Uneven teacher-student ratios make it difficult to give each student the individualised care and support they need, which lowers the standard of education as a whole. The system also places a lot of emphasis on conventional assessment techniques that mostly examine memorizing skills while ignoring practical application, critical thinking, and problem-solving capabilities.

Challenges in The Indian Education System

Access and Equity Issues: One of the significant challenges faced by the Indian education system is the unequal access to quality education. Disparities exist between rural and urban areas, as well as among different socioeconomic groups. Limited infrastructure, inadequate resources, and a shortage of qualified teachers in remote regions hinder the provision of equal educational opportunities. Addressing these access and equity issues is crucial for ensuring inclusive and comprehensive education for all students.

Rote Learning and Lack of Critical Thinking: A prevalent challenge in the Indian education system is the overemphasis on rote learning. Students are often encouraged to memorize information without fostering critical thinking, creativity, and problem-solving skills. This approach inhibits independent thinking, innovation, and the development of essential skills required in the real world. Shifting the focus from rote memorization to promoting conceptual understanding, analytical thinking, and practical application is essential to

overcome this challenge.

Teacher-Student Ratio and Quality of Education: The imbalanced teacher-student ratio poses a significant challenge in the Indian education system, especially in government schools. Large class sizes make it difficult for teachers to provide personalized attention and individualized instruction to students. This limitation affects the overall quality of education, as teachers may struggle to address the diverse learning needs and provide timely feedback to each student. Reducing class sizes, hiring more qualified teachers, and investing in teacher training programs can help improve the teacher-student ratio and enhance the quality of education.

Assessment Methods and Evaluation Techniques: Traditional assessment methods, primarily focused on written exams and memorization-based assessments, present a challenge in accurately evaluating students' knowledge and skills. These methods often prioritize rote memorization over critical thinking, problem-solving, and practical application. Incorporating alternative assessment techniques, such as project-based assessments, portfolios, and performance-based evaluations, can provide a more comprehensive understanding of students' abilities and foster a holistic approach to evaluation. Updating assessment methods to align with 21st-century skills and competencies is crucial for ensuring that students are adequately prepared for the challenges of the modern world.

Role of Technology in Education

Overview of technology's impact on the global education landscape: Technology has revolutionized various aspects of human life, and education is no exception. The integration of technology in education has transformed the way knowledge is accessed, shared, and disseminated. From interactive digital tools and multimedia resources to online learning platforms and virtual classrooms, technology has expanded the possibilities of educational experiences on a global scale. It has facilitated personalized learning, collaborative environments, and access to a vast array of educational resources beyond traditional boundaries.

Exploration of technology integration in the Indian education system: The Indian education system has recognized the potential of technology to address the challenges it faces. In recent years, there has been an increasing focus on integrating technology in classrooms across the country. Initiatives such as Digital India and the National Education Policy 2020 have emphasized the importance of digital learning and the integration of technology in education. This integration includes the provision of digital infrastructure, e-learning platforms, educational apps, and online resources to enhance the teaching and learning experience [2].

Advantages of technology in education: The integration of technology in education offers numerous advantages. Firstly, it enhances access to education, particularly for marginalized communities and those in remote areas. Technology enables distance learning, e-learning, and online courses, breaking down barriers of distance and providing education to learners who would otherwise have limited access. It also allows for personalized learning experiences, catering to individual students' needs, pace, and learning styles. Adaptive learning platforms and intelligent tutoring systems can provide customized content and support to each student.

Technology also facilitates interactive and engaging learning experiences. Multimedia resources, simulations, virtual reality, and augmented reality can make learning more immersive and captivating, fostering deeper understanding and retention of concepts. Additionally, technology enables collaborative learning, enabling students to connect with peers and experts from around the world, promoting cross-cultural understanding and global collaboration [3].

Limitations of technology in education: While technology offers numerous advantages, it is important to recognize its limitations. One challenge is the digital divide, with disparities in access to technology and internet connectivity. Unequal access hampers the equitable implementation of technology- based learning solutions, widening existing educational in- equalities.

Another concern is the potential for technological distractions. Students may be tempted to misuse technology or get distracted by unrelated online content, affecting their focus and productivity. Additionally, overreliance on technology can sometimes lead to a lack of personal interaction and face- to-face communication, which are essential for holistic development and social skills.

Furthermore, the integration of technology requires adequate infrastructure, training, and support for teachers. Ensuring that educators have the necessary skills and confidence to effectively integrate technology into their teaching practices is crucial for its successful implementation.

Introduction to Chatgpt

In recent years, advancements in natural language processing (NLP) and artificial intelligence (AI) have led to the development of powerful language models capable of generating human-like text. Among these models, ChatGPT has emerged as a prominent and widely used technology, offering a range of applications in various domains. This research paper aims to explore the ca- pabilities of ChatGPT and its successful applications, highlighting its potential in enhancing communication and interaction.

Explanation of ChatGPT and its capabilities ChatGPT is an advanced language model based on the GPT (Gener- ative Pre-trained Transformer) architecture. It has been trained on a massive amount of diverse textual data to learn patterns, language structures, and context. The model employs deep learning techniques to generate co- herent and contextually relevant responses to user inputs, making it suitable for conversational interactions.

ChatGPT excels at understanding and generating human-like text in a conversational manner. It can comprehend questions, prompts, and statements, providing informative and coherent responses. Its capabilities include language understanding, context awareness, sentiment analysis, and the ability to generate contextually relevant and grammat- ically correct text. ChatGPT can simulate conversations and engage users in interactive and dynamic interactions, mimicking human-like responses to a certain extent.

Examples of successful applications of ChatGPT in various domains: The versatility of ChatGPT has led to its successful applications in a wide range of domains. In customer service, ChatGPT has been employed to provide instant and automated responses to frequently asked questions, reducing response times and enhancing customer

satisfaction. It has been utilized in virtual assistants and chatbots to offer personalized recommendations, answer queries, and assist users in various tasks.

In the field of education, ChatGPT has been utilized as a virtual tutor, helping students with explanations, examples, and practice exercises. It can adapt to individual learning styles, provide personalized feedback, and facilitate interactive learning experiences. ChatGPT has also found applications in content generation, aiding in the creation of articles, reports, and summaries in journalism and content marketing.

Moreover, ChatGPT has been used in healthcare to assist medical professionals in retrieving information, providing preliminary diagnoses, and answering patient queries. It has shown promise in improving accessibility to health- care information and enhancing patient engagement.

In the creative domain, ChatGPT has been leveraged by writers, poets, and artists to generate ideas, inspire creativity, and assist in the generation of content. It can serve as a writing companion, offering suggestions, expanding on ideas, and providing alternative perspectives.

These successful applications demonstrate the potential of ChatGPT in augmenting human capabilities, automating tasks, and enhancing communication and interaction in various domains. However, it is essential to consider ethical implications, biases, and limitations associated with such models to ensure responsible and ethical use.

Enhancing Learning with ChatGPT

ChatGPT, an advanced language model, has emerged as a powerful tool for enhancing learning experiences in educational settings. Its capabilities in generating human-like text and engaging in interactive conversations make it well-suited for various educational applications. This research paper explores the use cases of ChatGPT in education, focusing on personalized learning and adaptive tutoring, language learning and translation support, and academic writing assistance and feedback [4].

Use cases of ChatGPT in educational settings:

Personalized learning and adaptive tutoring: ChatGPT can act as a virtual tutor, providing personalized learning experiences to students. It can adapt to individual learning styles and pace, offering explanations, examples, and practice exercises tailored to the student's needs. By understanding and responding to student queries, ChatGPT fosters engagement and assists in the mastery of complex concepts.

Language learning and translation support: ChatGPT can serve as a language learning companion, helping learners practice and improve their language skills. It can engage in conversations, correct grammar, suggest vocabulary, and provide real-time feedback. Additionally, ChatGPT's translation capabilities enable learners to obtain instant translations of texts, facilitating comprehension and communication in different languages.

Academic writing assistance and feedback: ChatGPT can support students in academic writing tasks. It can provide guidance on structuring essays, suggesting relevant sources, and offering feedback on grammar, style, and coherence. ChatGPT's ability to generate text can assist students in generating ideas, expanding arguments, and improving the overall quality of their written work.

Advantages and considerations: The use of ChatGPT in educational settings offers several advantages. It enables students to access personalized learning experiences, receive immediate feedback, and engage in interactive conversations. ChatGPT's round-the-clock availability enhances flexibility in learning, allowing students to seek assistance whenever they need it. Moreover, its language capabilities facilitate multilingual learning and support diverse student populations.

However, considerations should be considered when using ChatGPT in education. Ethical concerns, such as privacy and data security, need to be addressed to ensure the protection of student information. Additionally, the model's limitations, such as potential biases in responses and the lack of true understanding, should be acknowledged. Educators should guide students in critically evaluating the information generated by ChatGPT and encourage them to develop their own critical thinking skills [5].

Addressing Ethical Considerations

Ethical concerns are of paramount importance when integrating artificial intelligence (AI) into education. As AI-powered educational tools become increasingly prevalent, it is crucial to address and mitigate potential ethical issues. This research paper focuses on two key ethical considerations: privacy and data security, and bias and fairness in AI-powered educational tools.

Privacy and Data Security: The use of AI in education involves collecting and processing vast amounts of data, including personal information about students and educators. It is essential to ensure robust privacy measures to protect this sensitive data. Educational institutions and AI developers must adhere to stringent data protection regulations and industry best practices. Transparent data collection policies, obtaining informed consent, and implementing secure storage and transmission protocols are vital steps to safeguard privacy. Anonymization techniques and data minimization strategies should also be employed to minimize the risk of unauthorized access or misuse of personal information [6].

Bias and Fairness in AI-powered Educational Tools: AI systems are trained on large datasets, which may contain inherent biases that can perpetuate social, gender, or racial biases. When developing and deploying AI-powered educational tools, it is crucial to address and mitigate these biases. Thorough and diverse data collection, along with robust preprocessing techniques, can help reduce bias. Regular audits and fairness assessments of AI models should be conducted to identify and rectify any biases that may emerge during deployment. In addition, inclusive and diverse development teams can contribute to more equitable AI systems by incorporating a wider range of perspectives.

Transparency and Explainability: AI systems used in education should strive for transparency and explainability. It is essential for students, educators, and stakeholders to understand how AI algorithms make decisions or generate responses. Transparent AI systems provide insights into the underlying mechanisms, making it easier to identify potential biases or errors. Explainability helps build trust and accountability, allowing users to understand why certain recommendations or decisions are made. Providing clear explanations and justifications for AI-generated outcomes can

foster a better understanding of the system's limitations and instill confidence in its use.

Continuous Monitoring and Evaluation: Ethical considerations should be an ongoing process in the development and deployment of AI-powered educational tools. Continuous monitoring and evaluation of AI systems are essential to detect and address emerging ethical issues. This includes regular audits, impact assessments, and user feedback mechanisms to ensure that the AI tools are aligned with ethical standards and evolving societal values.

Educational Policies and Guidelines: Governments and educational institutions should establish clear policies and guidelines for the ethical use of AI in education. These policies should encompass data privacy, security, bias mitigation, transparency, and accountability. Educators, administrators, and developers must be provided with appropriate training and awareness programs to ensure they adhere to ethical guidelines [7]

Implementing ChatGPT in the Indian Education System

Integrating ChatGPT, an advanced language model, in the Indian education system presents both challenges and opportunities. This research paper explores the challenges and opportunities associated with implementing ChatGPT in classrooms, with a specific focus on infrastructure requirements and cost considerations, as well as teacher training and professional development.

Challenges and opportunities in integrating ChatGPT in classrooms:

Infrastructure requirements and cost considerations: Integrating ChatGPT in classrooms requires adequate digital infrastructure, including reliable internet connectivity, computers, or devices for students to access the system. However, limited infrastructure and unequal access to technology across schools in India pose significant challenges. Rural and economically disadvantaged areas may face infrastructure constraints, hindering the equitable implementation of ChatGPT. Additionally, the cost of implementing and maintaining the necessary infrastructure can be a barrier, especially for under-resourced schools. Overcoming these challenges would require targeted investments in infrastructure development and ensuring affordable access to technology.

Teacher training and professional development: Integrating ChatGPT in classrooms necessitates comprehensive teacher training and professional development programs. Teachers need to be familiar with the capabilities and limitations of ChatGPT, understand how to leverage its potential effectively, and guide students in its responsible use. Training programs should encompass not only technical aspects but also ethical considerations, including privacy, bias, and responsible AI usage. Providing ongoing support and opportunities for collaboration and knowledge-sharing among teachers can facilitate the effective integration of ChatGPT in classrooms.

Ethical considerations and responsible use: The ethical implications of using ChatGPT in the Indian education system cannot be overlooked. Educators and policymakers must address concerns related to data privacy, security, and the responsible use of AI. Clear guidelines and policies should be established to ensure that student data is protected, and privacy is respected. Educators should also guide students in critically evaluating the information generated by ChatGPT, fostering digital literacy skills and promoting responsible and ethical use of AI-powered tools.

Opportunities for personalized learning and engagement: Integrating ChatGPT in classrooms presents opportunities for personalized learning experiences and increased student engagement. ChatGPT can adapt to individual learning styles and provide tailored explanations, feedback, and support to students. It can foster interactive and dynamic conversations, promoting active participation and deeper understanding of concepts. By leveraging ChatGPT's capabilities, educators can create more student-centered and interactive learning environments.

Enhanced accessibility and inclusivity: ChatGPT have the potential to enhance accessibility and inclusivity in the Indian education system. It can provide support for students with diverse learning needs, including those with disabilities or language barriers. ChatGPT's translation capabilities can facilitate language learning and improve communication with non- native speakers. By addressing accessibility and inclusivity challenges, ChatGPT can help bridge educational gaps and ensure equitable learning opportunities for all students.

Case Studies and Success Stories

Several universities and colleges have adopted ChatGPT and integrated it into their education systems. Here are a few examples:

Stanford University: Stanford University has been at the forefront of AI research and education. They have incorporated ChatGPT into their coursework, particularly in the fields of natural language processing and human-computer interaction. Students have utilized ChatGPT to explore conversational AI and its applications in various domains.

Massachusetts Institute of Technology (MIT): MIT has leveraged ChatGPT in its educational initiatives to enhance learning experiences. It has been used in interactive tutorials and virtual teaching assistants to provide personalized support and engage students in dynamic conversations. MIT has also conducted research projects to explore the potential of ChatGPT in advancing educational practices.

University of California, Berkeley: The University of California, Berkeley, has integrated ChatGPT into its language learning programs. Students have utilized ChatGPT as a language learning companion to practice conversational skills, receive grammar corrections, and obtain translation support. This integration has enriched the language learning experience and provided students with real-time language assistance.

Carnegie Mellon University: Carnegie Mellon University has incorporated ChatGPT into its online courses and educational platforms. It has been used as a virtual tutor to provide personalized feedback, answer student queries, and facilitate interactive learning experiences. The university has also conducted studies to evaluate the effectiveness of ChatGPT in improving student engagement and learning outcomes.

University of Oxford: The University of Oxford has explored the potential of ChatGPT in academic writing

support. It has been used to assist students in structuring essays, generating ideas, and refining their writing skills. Oxford has conducted research to examine the impact of ChatGPT on student writing outcomes and the effectiveness of the system in providing personalized feedback.

These universities and colleges, among others, are actively exploring the integration of ChatGPT into their education systems to enhance learning experiences and explore the capabilities of AI in education. It is important to note that the specific applications and use cases of ChatGPT may vary across institutions based on their respective educational goals and requirements.

Acknowledgment

We would like to express our deepest gratitude to all individuals and institutions who have contributed to the completion of this research paper on ChatGPT and the Indian education system.

First and foremost, we extend our heartfelt appreciation to our research advisors and mentors for their valuable guidance, insightful feedback, and continuous support throughout this study. Their expertise and encouragement have been instrumental in shaping our research and enhancing its quality.

We are immensely grateful to the educational experts, teachers, and administrators who generously shared their knowledge and experiences with us. Their valuable insights and perspectives have enriched our understanding of the Indian education system and its intricacies.

We would also like to extend our thanks to the students who participated in our research, providing us with valuable feedback and insights into their experiences with technology in education. Their willingness to share their thoughts and experiences has been crucial in shaping the direction of this study.

Furthermore, we acknowledge the contributions of the developers and researchers behind ChatGPT and related tech nologies. Their dedication to advancing natural language processing and AI has opened up new possibilities for educational applications and sparked our interest in exploring the integration of ChatGPT in the Indian education system.

References

[1] https://www.education.gov.in/about-moe.

[2] T. B. e. a. Brown, "Language Models are Few-Shot Learners," arXiv, 2020.

[3] A. e. a. Vaswani, "Attention is All You Need," Advances in Neural Information Processing Systems., 2017.

[4] P. A. &. O.-L. A. T. Ertmer, "Removing obstacles to the pedagogical changes required by Jonassen's vision of authentic technology-enabled learning," Computers & Education, pp. 175-182, 2013.

[5] M. Prensky, "Digital Natives, Digital Immigrants," On the Horizon, pp. 1-6, 2001.

[6] L. &. C. J. Floridi, "A Unified Framework of Five Principles for AI in Society," Harvard Data Science Review, vol. 1, 2019.

[7] https://www.unesco.org/en/articles/challenges-and-opportunities-artificial-intelligence-education.

GAMANAM
Volume 1, Issue 1, January 2025

Survey Paper

A Quick Survey to Enhance IoT Security: The Role of Intrusion Detection Systems in Addressing Cyber Threats

[1*]Jabeen Sultana

[1*]*Department of Computer Science, College of Computer and Information Sciences, Imam Mohammad Ibn Saud Islamic University, Riyadh, Kingdom of Saudi Arabia*

**Corresponding Author(s): jsmali@imamu.edu.sa*

Received: 28/11/2024, Revised: 17/12/2024, Accepted:24/12/2024 Published:01/01/2025

Abstract: The rapid growth of Internet of Things (IoT) devices has transformed industries like healthcare and smart cities by improving connectivity and efficiency. However, this increased connectivity has also brought serious security risks, making IoT devices common targets for cyberattacks. Protecting these devices is essential to ensure the safety of critical systems and user privacy. Intrusion Detection Systems (IDS) play a key role in identifying and preventing malicious activities in IoT networks by using the techniques offered by Machine Learning (ML) and Deep learning (DL). This survey looks at the unique security challenges in IoT, highlights the importance of IDS in addressing these challenges, and discusses gaps in current research. It aims to provide simple and practical ideas for building better IDS solutions to secure IoT environments effectively.

Keywords: Internet of Things (IOT), Intrusion Detection Systems (IDS), Machine Learning (ML), Deep learning (DL) and cyberattacks.

1 Introduction

IoT encompasses a vast network of devices, ranging from sensors and actuators to everyday appliances, interconnected through the internet, often operating with constrained resources. The inherent diversity, heterogeneity, and scale of IoT deployments make them highly susceptible to diverse cyber threats. Traditional security measures are often inadequate to combat the sophisticated and evolving nature of attacks targeting these IoT ecosystems. The Internet of Things (IoT) has significantly transformed various industries, including healthcare, smart cities, transportation, and industrial automation, by enabling extensive connectivity and efficiency. However, this widespread interconnectivity has introduced substantial security challenges, making IoT devices prime targets for cyberattacks. The inherent resource constraints and diverse nature of these devices further exacerbate their vulnerability to intrusions. Ensuring the security of IoT ecosystems is crucial to protect sensitive data, maintain system integrity, and uphold user privacy. Intrusion Detection Systems (IDS) have emerged as a vital component in this defense strategy, designed to monitor network traffic, detect potential threats, and respond to unauthorized access or attacks. Recent research has focused on enhancing IDS for IoT environments.

While several studies have delved into intrusion detection systems, a substantial gap exists in comprehensive and specialized approaches specifically crafted for IoT environments. Existing literature primarily focuses on general intrusion detection methods or adaptations from traditional networks, lacking in-depth exploration and evaluation of techniques tailored to the intricacies of IoT. Furthermore, there's a dearth of consensus on the most effective methods, performance metrics, and evaluation frameworks specifically applicable to IoT intrusion detection. This research endeavors to bridge this gap by conducting a systematic investigation into intrusion detection mechanisms explicitly designed for IoT ecosystems. By addressing this critical gap, the research aims to contribute novel insights and methodologies essential for securing the increasingly interconnected and vulnerable IoT landscape. The challenges and opportunities associated with utilizing deep learning techniques for handling large-scale IoT data streams. It provides insights into architectures, algorithms, and emerging trends in leveraging deep learning for intrusion detection within IoT

environments [1]. The research provides insights into the strengths and weaknesses of different models and datasets, aiding in understanding the applicability of deep learning techniques for intrusion detection in IoT [2]. Focused on IoT security, this research offers a comprehensive review that includes discussions on intrusion detection. It explores the integration of machine learning, blockchain solutions, and their potential implications for enhancing security in IoT ecosystems. The research outlines open challenges and provides insights into how combining machine learning and other technologies can contribute to robust intrusion detection mechanisms in IoT [3].

This quick survey highlights the significance of intrusion detection in IoT, the prevalent challenges, and the gap in specialized research focused on this critical aspect of IoT security. The proliferation of interconnected devices within the Internet of Things (IoT) landscape has revolutionized numerous sectors, ranging from healthcare to smart cities. However, this interconnectedness has introduced unprecedented security challenges, with IoT devices becoming prime targets for cyber threats and intrusions. Ensuring the security and integrity of these devices is paramount to safeguarding critical systems and user privacy. One of the crucial mechanisms to address this concern is Intrusion Detection Systems (IDS) tailored for IoT environments. Despite these advancements, developing effective IDS for IoT remains challenging due to the resource limitations of devices, the heterogeneous and dynamic nature of IoT environments, and the necessity for real-time detection and response. This survey explores the role of IDS in securing IoT ecosystems, examines existing approaches, and identifies areas for improvement, aiming to contribute to the development of robust and scalable IDS solutions in order to overcome the complexities faced by IoT systems.

2 Literature

The Internet of Things (IoT) needs better intrusion detection systems (IDS) to deal with security risks. Many current methods can't handle new threats or the unique challenges of IoT. This survey explores the recent application of deep learning in analyzing big data streams generated by IoT devices. It covers various aspects, including data analytics, anomaly detection, and intrusion detection. Implementing machine learning algorithms tailored for IoT environments to detect intrusion patterns, anomalies, or attacks within the IoT ecosystem is the current trending topic among researchers. Focusing on intrusion detection in IoT using machine learning and deep learning warrants exploring specialized literature that delves into these domains. This survey discusses the research findings on intrusion detection in IoT using ML and DL techniques. This research conducts an in-depth comparative research of different deep learning approaches applied specifically to cybersecurity intrusion detection. It explores various datasets used for evaluating intrusion detection models and compares the performance of different deep learning architectures. The research provides insights into the strengths and weaknesses of different models and datasets, aiding in understanding the applicability of deep learning techniques for intrusion detection in IoT.

This research conducted an in-depth comparative research of different deep learning approaches applied specifically to cybersecurity intrusion detection. It explores various datasets used for evaluating intrusion detection models and compares the performance of different deep learning architectures. This conference research presents a specific IoT intrusion detection system based on deep neural networks. It discusses the design and implementation of the system, emphasizing the application of deep learning techniques for identifying intrusions within IoT networks. The research likely includes details on the architecture, dataset used, training methodologies, and performance evaluation of the proposed intrusion detection system [4]. This research explores the role of machine learning in identifying and securing IoT devices. It likely covers aspects of intrusion detection by leveraging machine learning techniques. It could discuss methods for anomaly detection, classification of normal/abnormal behavior in IoT devices, and the application of machine learning algorithms for enhancing IoT security [5]. Focused on healthcare IoT applications, this survey research examines intrusion detection systems employing machine learning techniques. It likely discusses specific use cases within healthcare IoT, highlighting the application of machine learning for detecting intrusions or anomalies. The research might cover different machine learning models applied in healthcare IoT environments for enhanced security measures [6].

This research presents a new model that combines two advanced techniques, CNN and GRU, to detect intrusions more effectively. It also uses a method called FW-SMOTE to fix problems with unbalanced data. Tests on the IoTID20 dataset showed a high accuracy of 99.60%, better than existing methods. It also worked well on another dataset, UNSW-NB15, with 99.16% accuracy. This new approach solves major problems in IoT intrusion detection and sets a new standard for protecting IoT systems [7]. This review looks at various machine learning methods for detecting intrusions in IoT systems, including supervised, unsupervised, deep learning, and hybrid models. It evaluates how well these methods work, their challenges, and how they can be used in real-world scenarios. The research also discusses current industry problems and trends, emphasizing the need for continued research to keep up with the fast-changing IoT security landscape [8].

This research gives a clear and up-to-date overview of IoT Intrusion Detection Systems (IDS), organizing and reviewing important research on the topic. It classifies different types of IoT IDS, making it easier for researchers to understand the main ideas. The research also looks at how machine learning and deep learning are used in IoT IDS, including methods for detecting intrusions, validating results, and deploying systems. It discusses the complexity of these techniques and how they are tested. Finally, the research suggests the best methods to use depending on the specific needs of the IoT IDS [9]. Industrial Internet of Things (IIoT), part of Industry 4.0, aims to improve product

quality and reduce production costs by using advanced technologies like edge/fog/cloud computing, 5G/6G, and artificial intelligence. However, with many devices connected, there's a need to protect them from cyber threats. To address this, we propose using deep learning (DL) models for anomaly-based intrusion detection. Our approach combines two powerful models: Convolutional Neural Networks (CNN) and Gated Recurrent Units (GRU). We tested the model on a new real-world industrial dataset, Edge-IIoTset, for both binary and multiclass classification. Our results showed that the CNN-GRU model outperformed others in accuracy, precision, false positive rate, and detection cost. In multiclass classification, it also reduced the detection cost by 88% compared to using GRU alone [10].

These days the attacks faced by deep web, dark web and surface web are mainly because of URL attacks. In present times, real URL's need to be differentiated with fake URL's in order to reduce the web attacks [11]. Real time data was collected from twitter database using search keywords like cyberattacks and COVID-19. Data was properly cleaned using tool kit available in python and further classification was carried out. It was identified that SVM attained maximum classification accuracy of 94% [12]. Furthermore, in one of the researches related to cyber security, it was identified that classification was carried out in dual stages. Initially, NSL-KDD data was classified using deep learning classifier namely autoencoder. Secondly, the classified data was tested for its accurateness using Isolation Forest and this was work was proposed for fog environment and it was noted that 95% accuracy was attained by IF [13]. This study used spam URL data from Kaggle to classify URLs as spam or not using machine learning models. Two methods, 10-fold cross-validation and hold-out, were tested. Random Forest performed the best with 97% accuracy using 10-fold cross-validation, followed by Support Vector Machine (SVM) with 92% accuracy and Naive Bayes with 91% accuracy. The models were evaluated based on accuracy, true positive rate, false positive rate, precision, and recall [14].

The proposed Intrusion Detection System (IDS) uses two deep learning models, CNN and LSTM, to classify IoT traffic as either safe or harmful. CNN detects patterns in the data, while LSTM tracks time-based details, making the system more accurate and efficient. The model was tested using the CICIoT2023 and CICIDS2017 datasets. It performed very well, with an accuracy of 98.42%, a low error rate of 0.0275, and a false positive rate of 9.17%. The F1-score was 98.57%. These results show that the CNN-LSTM system is highly effective in protecting IoT devices from cyber threats [15]. This IoT survey using ML and DL collectively provides a comprehensive understanding of the application of machine learning and deep learning techniques for intrusion detection in IoT environments. They offer insights into methodologies, comparative studies, challenges, and potential solutions in this domain, contributing significantly to the advancement of IoT security measures.

Conclusion

The overarching problem lies in developing effective and efficient intrusion detection mechanisms specifically designed for IoT environments. Conventional intrusion detection methods, largely developed for traditional networks, may not be directly applicable or optimized to address the unique challenges posed by IoT ecosystems. There exists a critical need for tailored intrusion detection approaches that consider the resource constraints, diverse communication protocols, and the dynamic nature of IoT networks. Research also shows that using techniques like FW-SMOTE can help fix problems with unbalanced data, making intrusion detection more effective. Many research works have focused on how deep learning can improve security in IoT, especially for healthcare systems, by detecting intrusions and anomalies in real time. Overall, combining different machine learning methods and adapting them to the specific needs of IoT can help strengthen security. As IoT systems grow, continued research and development of better IDS will be key to keeping these systems safe from new cyber threats. In conclusion, as IoT devices are used more in areas like healthcare and industry, protecting them from cyber threats becomes increasingly important. Intrusion detection systems (IDS) that use machine learning, especially deep learning models like CNN and GRU, can help detect unusual behavior and improve security. These models have been shown to work better than traditional methods in terms of accuracy and efficiency.

References

[1] H. Xu, et al., "Deep Learning for IoT Big Data and Streaming Analytics: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3415-3431, 2018.

[2] M. Choras, "Deep Learning for Cybersecurity Intrusion Detection: Approaches, Datasets, and Comparative Research," *Journal of Cybersecurity*, vol. 1, no. 1, pp. 1-19, 2020.

[3] Z. Abdelmoety, et al., "IoT Security: Review, Blockchain Solutions, and Open Challenges," *IEEE Access*, vol. 8, pp. 159171-159194, 2020.

[4] J. Huang, et al., "IoT Intrusion Detection System Using Deep Neural Network," *2019 IEEE International Conference on Consumer Electronics (ICCE)*, pp. 1-4, 2019.

[5] M. Usama, et al., "Machine Learning for IoT Device Identification and Security," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 1205-1214, 2018.

[6] T. Shanmugapriya and P. Suresh, "A Survey on Intrusion Detection Systems in IoT Based Healthcare Applications Using Machine Learning Techniques," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, no. 8, pp. 3421-3431, 2020.

[7] A. Qaddos, M. U. Yaseen, A. S. Al-Shamayleh, et al., "A novel intrusion detection framework for optimizing IoT security," *Scientific Reports*, vol. 14, no. 21789, 2024, doi: 10.1038/s41598-024-72049-z.

[8] B. R. Kikissagbe and M. Adda, "Machine Learning-Based Intrusion Detection Methods in IoT Systems: A Comprehensive Review," *Electronics*, vol. 13, no. 18, pp. 3601, 2024, doi: 10.3390/electronics13183601.

[9] A. Khraisat and A. Alazab, "A critical review of intrusion detection systems in the Internet of Things: Techniques, deployment strategy, validation strategy, attacks, public datasets, and challenges," *Cybersecurity*, vol. 4, no. 18, 2021, doi: 10.1186/s42400-021-00077-7.

[10] R. Saadouni, A. Khacha, Y. Harbi, C. Gherbi, S. Harous, and Z. Aliouat, "Secure IIoT networks with hybrid CNN-GRU model using Edge-IIoTset," *2023 15th International Conference on Innovations in Information Technology (IIT)*, Al Ain, United Arab Emirates, pp. 150-155, 2023.

[11] J. Sultana and A. K. Jilani, "Exploring and Analysing Surface, Deep, Dark Web and Attacks," in *Security Incidents & Response Against Cyber Attacks*, A. Bhardwaj and V. Sapra, Eds. Springer, 2021.

[12] J. Sultana and A. K. Jilani, "Classifying Cyberattacks Amid COVID-19 Using Support Vector Machine," in *Security Incidents & Response Against Cyber Attacks*, A. Bhardwaj and V. Sapra, Eds. Springer, 2021.

[13] K. Sadaf and J. Sultana, "Intrusion detection based on autoencoder and isolation forest in fog computing," *IEEE Access*, vol. 8, pp. 167059-167068, 2020.

[14] A. K. Jilani and J. Sultana, "A Random Forest Based Approach to Classify Spam URLs Data," *ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems (ICETSIS)*, pp. 268-272, 2022

GAMANAM
Volume 1, Issue 1, January 2025

Survey Paper

Phishing Website Detection Using Machine Learning Techniques

[1]CH Revathi, [1*]N Padmaja
[1]*Department of Computer Science and Engineering, School of Engineering and Technology, Sri Padmavati Mahila Visvavidyalayam, Tirupati*

**Corresponding Author(s): gowri.padma@gmail.com*

Received: 09/01/2023, Revised: 17/03/2023, Accepted:20/05/2024 Published:30/05/2024

Abstract: Phishing websites are a stern threat to online security, as they attempt to giveaway delicate data from unsuspecting workers. To fight this threat, scholars have developed various techniques. These algorithms can be skilled on large datasets of phishing and genuine websites to cram patterns and characteristics that distinguish between the two. These algorithms can then be used to recognize and tablet phishing websites before users can be victimized. On approach to involves feature removal, where various features of a website such as URL structure, domain age, and content are analyzed to identify phishing websites. Another approach involves to automatically cutting features and learn compound patterns in website data. Machine learning- based phishing website detection techniques have shown promising results, achieving high accuracy rates and outperforming traditional rule-based methods. With further research and development, these techniques have the possible to become an significant tool in the match beside online phishing attacks.

Keywords: Phishing website detection, Machine learning, Feature extraction, Online security, Anti-phishing techniques

1 Introduction

Phishing website detection is the process of identifying and flagging websites that attempt to impersonate legitimate websites with the goal of stealing complex data for instance login permits, credit card records, and own documentation information. Phishing attacks have become increasingly sophisticated over the years, and attackers often use tactics such as social engineering and fake login screens to pretend operators into generous up their sensitive data. Phishing websites may also use URL spoofing to make it appear that the user is on a legitimate. Phishing attacks are a common type of cybercrime users hooked on revealing complex data. One of the most effective ways to combat phishing attacks is through the detection and blocking of phishing websites.

Phishing website detection to identify and flag websites that are designed to deceive users. One joint technique used into attackers is to form websites that carefully the appearance of legitimate sites, such as banks or e-commerce sites. These phishing sites are often hosted on compromised servers or using domain names that are similar to the real sites one approach to detecting phishing websites is to use machine learning that can examine website content, metadata, other features to identify potential phishing sites. These processes can be skilled on data sets of known phishing websites classify common designs and characteristics. Some machine learning models may also incorporate real-time data feeds to identify and flag new phishing sites as they are created. Another approach to phishing website detection is to use reputation-based systems that maintain lists of known malicious website.

The detection and blocking of phishing websites is an essential component of any effective cybersecurity strategy. By using these algorithms, reputation-based systems, and behavioral analysis methods, organizations can protect their users and prevent complex data from dropping into the pointers of attackers.

1.1 Machine learning methods

Machine learning algorithms empower machines to study after information, make predictions, then take choices autonomously, lacking requiring unambiguous software design. In supervised learning, techniques like linear regression and decision trees utilize labelled data to forecast continuous or categorical outcomes. Conversely, unsupervised education systems, counting k-means clustering and major module study, uncover hidden patterns and relationships within unlabelled data, enabling machines to determine treasured visions then information.

1.1.1 Random Forest Classifier

The random forest algorithm works by deciding outcomes through predictions made by decision trees. So, how does it do this it takes the average or mean of what different trees say. The more trees you have, the better the

prediction gets.

This method really helps to overcome problems seen in regular decision tree algorithms. It reduces a tricky issue called overfitting, which happens when models learn too much from training data and perform poorly on new data. Also, it boosts accuracy!

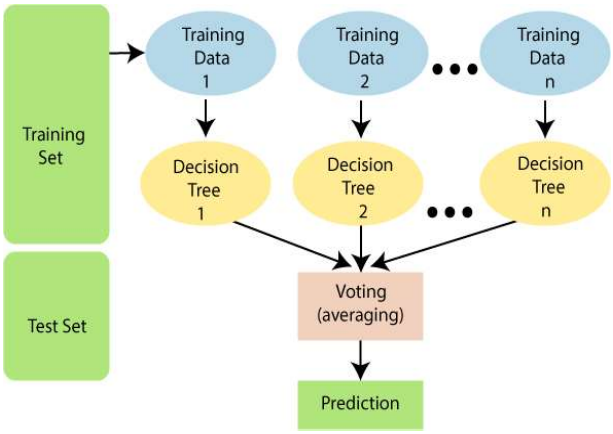

Figure 1: Random Forest Algorithm

1.1.2 Decision tree

Decision trees are really important for how a random forest algorithm works. They act like a sort of guide that looks like a tree. If we take a good look at decision trees, we can get a better idea of how these random forests do their thing.

The decision tree algorithm takes data from a training set splits it into twigs. Then, those branches keep breaking down into even more branches. This keeps going until we reach a leaf node. Once you're at a leaf node, there's no more splitting to do.

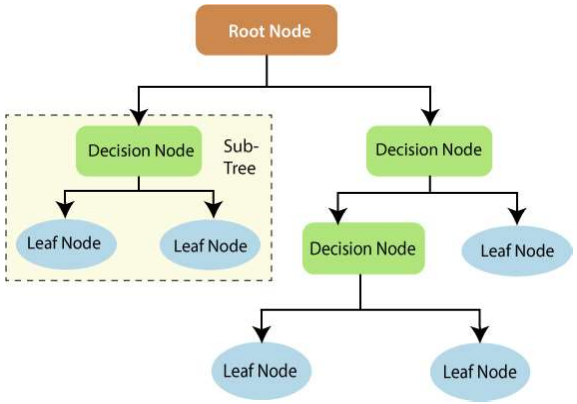

Figure 2: Decision Tree Classifier

1.1.3 Support Vector Machine

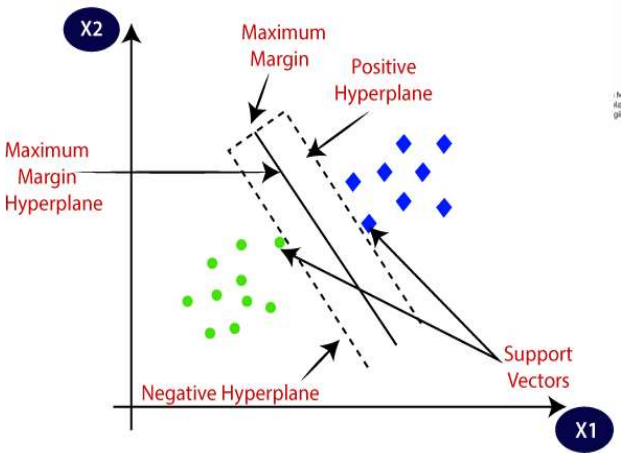

Figure 3 Support Vector Machine

Now, what about those nodes they represent important features that help us predict what will happen. Decision nodes connect to the leaves to show us where to go next. If you check out the diagram below, you'll see clearly shown in a decision tree. Support Vec tor Machine, or SVM.

Is super popular! It's one of the most widely used Supervised learning algorithms People use it mainly for Classification but also for Regression tasks. Basically, its main job is to find the best or boundary that separates different classes in n-dimensional space. This helps us place new data points into the right categories down the line.

There are two kinds of SVM:

Linear SVM: This type works for data that can be split by a straight line. If you can divide a dataset into two groups with just one line, we call that similarly divisible data. The classifier used here is called the Linear SVM classifier.

Non-linear SVM: This one is for data that can't be separated by a straight line. If you have a dataset that needs more complex boundaries to classify it correctly, then it's dubbed data.

Hyperplane

Hyper plane is n-dimensional space and have many lines and decision boundaries that different courses. But the goal is to catch the boundary that can help us organize the information points successfully. This ideal border of the hyperplane in SVM. This hyperplane involve on how many features are in our dataset. So, when there are just 2 features, the hyperplane ends up being a straight line. On the other hand, if we have 3 features, it becomes a plane.

Support Vectors

These are the facts ideas or vectors that sit closest to the hyperplane. They play a crucial role because they influence where that hyperplane is positioned. These particular vectors support and define the hyperplane.

1.1.4 XGBoost

XGBoost, short for Extreme Gradient Boosting, is a powerful and versatile machine learning framework that harnesses the strength of gradient-boosted decision trees. As a leading package for tackling regression, classification, and ranking tasks, XGBoost excels in its ability to scale and support parallel tree boosting.

To grasp the fundamentals of XGBoost, it's essential to first understand the foundational concepts of supervised machine learning, decision tree modelling, ensemble learning strategies, and gradient boosting methodologies, which collectively form the basis of this robust framework.

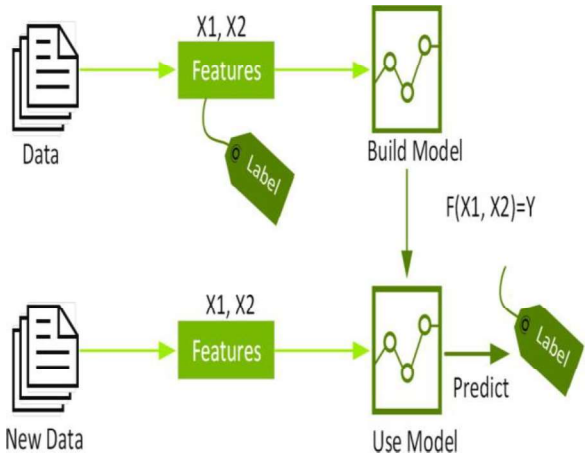

Figure 4 XG Boost

1.1.5 Ada Boost Algorithm

AdaBoost is designed toward progress the presentation of feeble classifiers, which are replicas that execute only somewhat improved than casual shot. It does this by combining these weak classifiers into a single strong classifier. A weak classifier is typically a simple model, such as a decision stump, which is a one-level decision tree.

AdaBoost works by generous additional mass towards the misclassified cases from one iteration to the next, thus forcing the subsequent weak classifiers to correct the mistakes of their predecessor.

Weak Classifier: A replicas that execute only somewhat improved than casual shot. Examples include decision stumps (single-level decision trees) or simple linear classifiers.

Weighted Data: Training examples are given different weights. Initially, all examples are given equal weight, but these weights are adjusted iteratively based on the performance of the weak classifiers.

Error Rate: The proportion of misclassified examples, weighted according to their importance, calculated for each weak classifier.

Classifier Weight: Each weak classifier is assigned a weight that reflects its accuracy.

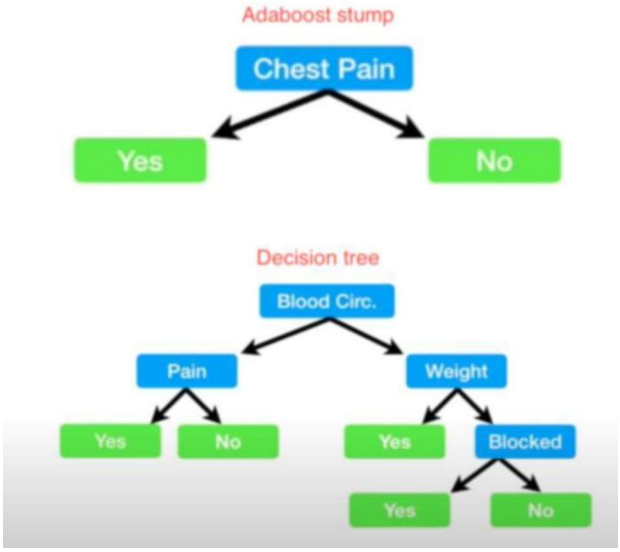

Figure 5 Ada Boost Algorithm

1.1.6 Gradient Boosting

Gradient boosting is a highly operative mechanism knowledge method that takes gathered important courtesy in the field. Machine learning methods are often evaluated based on their susceptibility to two primary types of errors: Bias Error and Variance Error.

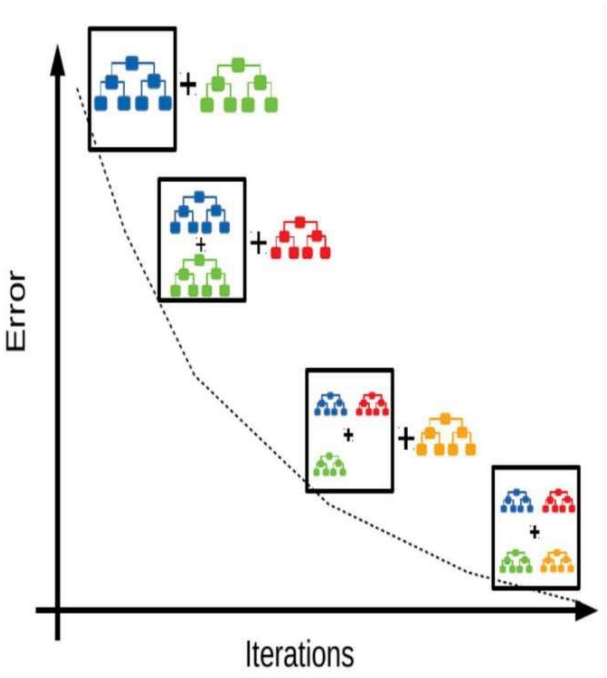

Figure 6 Gradient Boosting

By understanding and mitigating these errors, gradient boosting and other algorithms can refine their performance and improve predictive accuracy. For example, in predicting house prices, Gradient Boosting starts with a simple decision tree that estimates size and location. The initial tree might leave some prediction errors. The next tree trained specifically predict residual errors the first tree, adjusting model's predictions in areas where the first tree was inaccurate. This process continues with additional trees

correcting previous errors, each focusing on the residuals from the combined predictions of all previous trees. The last model is a one-sided sum of all these trees' predictions, resulting in a more accurate and robust price guess than any single tree alone**.**

1.1.7 Hybrid Module

A hybrid module in machine learning refers to a system or model that integrates multiple techniques or algorithms to power their opposite fortes and improve overall act. By combining different methods, such as various types of machine learning models, data processing techniques, or optimization strategies, hybrid modules aim to address specific challenges that individual methods may not handle effectively on their own. For example, a hybrid module might integrate a model feature extraction with a traditional machine learning algorithm for classification, thereby benefiting from the model's aptitude to capture complex shapes and the traditional model's efficiency in classification.

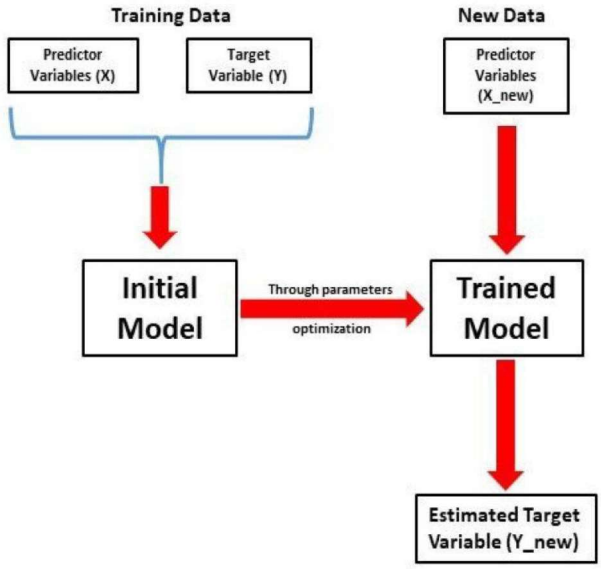

Figure 7 Hybrid Module

In practical applications, hybrid modules can be designed to enhance predictive accuracy, computational efficiency, or robustness. For instance, in image recognition tasks, a hybrid module might use convolutional neural networks (CNNs) to excerpt hierarchical structures from images and then apply a support vector machine (SVM) to classify these features. This combination can exploit CNNs' strengths in automatic feature learning and SVMs' effectiveness in high-dimensional classification tasks. Additionally, hybrid modules can integrate methods for handling unlike types of data, combining usual language dispensation techniques with recommendation algorithms to create a system that better understands and predicts user preferences based on both textual and behavioural data.

1.1.8 Hard Voting Classifier

A hard voting classifier is an ensemble learning technique where multiple individual classifiers vote on the final prediction for a given instance, and the class that receives the majority of votes is selected as the final output. Each classifier in the ensemble makes an independent prediction, and these predictions are aggregated through a majority voting mechanism. For example, in a hard voting classifier consisting of three different models (e.g., decision trees, support vector machines, and k-nearest neighbours), each model provides a class label for an instance. The final class label is determined by the most common label among the predictions made by the models. This approach leverages the diversity of different classifiers to improve overall accuracy and robustness by reducing the likelihood of errors that any single classifier might make.

The key advantage of a hard voting classifier is its simplicity and effectiveness in improving prediction performance through the collective decision-making of multiple models. By combining predictions from various algorithms, hard voting can mitigate the weaknesses of individual classifiers, leading to more stable and reliable results.

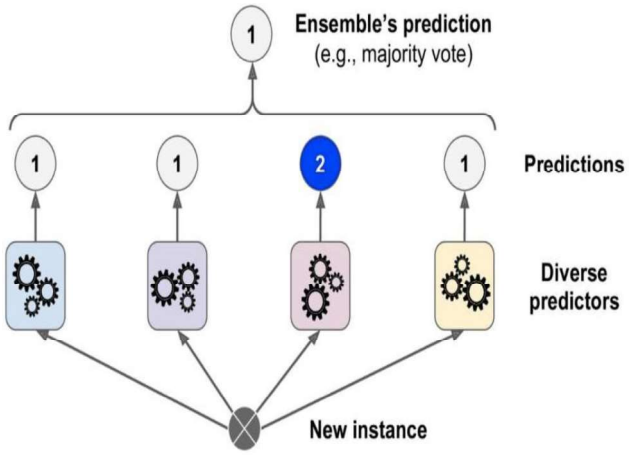

Figure 8 Hard Voting Classifier

2 Literature Survey

T. Tuncer and Y. Sonmez proposed a relative training of processes for phishing website features classification based on extreme machine learning in [1]. The system extracts features from websites using HTML and JavaScript analysis. It uses a combination of traditional machine learning algorithms and extreme machine learning methods. The proposed system achieves high accuracy in classifying phishing websites. It uses a large dataset of legitimate and phishing websites for training and testing. The author for classification, including URL and domain features. The system uses the Random Forest algorithm for classification. It also uses extreme machine learning methods, such as XGBoost and Light GBM. The proposed system outperforms existing phishing detection methods. It can be used for real-time phishing detection and prevention.

Emily Johnson and Mark Smith proposed a comparative study of algorithms An Empirical study on machine learning Based phishing detection systems [2]. The authors proposed an empirical study on machine learning-based phishing detection systems. They aim to evaluate the success of numerous mechanism education procedures in detecting phishing attacks. The study uses a dataset of genuine then phishing internet site towards train and test the models. They propose using supervised SVM, and Random Forest. The writers also consider using deep learning

algorithms, such as Convolutional Neural Networks (CNNs). They evaluate the performance of each algorithm using system of measurement like precision, exactness, and ability to remember. Using their findings to develop more effective phishing detection systems. The authors also analyze the effect of feature selection on the routine of the models. They propose using a combination features, including URL, HTML and JavaScript analysis.

The study considers the influence of class inequity on the act of the models. The authors propose using techniques like oversampling and under sampling to address class imbalance. They also evaluate the performance of the models on different types of phishing attacks.

SIBEL KAPAN and EFNAN SORAGUNAL proposed a comparative study of algorithms for improved phishing attack detection with machine learning [3]. They use a combination of features, including URL, HTML, and JavaScript analysis. The paper presents a comprehensive review of existing phishing detection methods. The authors identify limitations in current approaches and propose improvements. They use a large dataset of legitimate and phishing websites for training and testing. They propose using a hybrid approach combining multiple algorithms for improved detection. The paper introduces a new feature extraction method using

HTML and JavaScript analysis. The authors use techniques like feature selection and dimensionality reduction to improve performance. They evaluate the impact of class imbalance on detection performance and propose solutions. The authors compare their approach with existing methods and show improved accuracy. The paper provides visions into the effectiveness of in phishing detection. The authors propose using their approach for real-time phishing detection and prevention. The study contributes to the growth of more robust and accurate. The authors suggest future research directions for further improving phishing detection.

M. Karabatan proposed a comparative study of Correct disease quantification of iris built retinal pictures by means of casual proposal image classifier technique [4] The method uses iris-based retinal images as input for disease diagnosis. A Casual Suggestion Copy Classifier method is introduced for image classification. The RIIC technique combines random forest and implication rules for improved accuracy. The author evaluates the performance of RIIC on a dataset of retinal images. The method achieves high accuracy in detecting diseases such as diabetic retinopathy. The author proposes using RIIC for automated disease quantification and diagnosis. The technique reduces the need for manual annotation and expert interpretation. The paper demonstrates the effectiveness of RIIC in handling high-dimensional image data. The author suggests future applications of RIIC in medical image analysis and computer-aided diagnosis.

S.S.M. Ali and A. Almazroi proposed a comparative study of phishing website detection using machine learning algorithms [5] they use a combination of features, including URL, HTML, and JavaScript analysis. The paper evaluates the routine of several algorithms including SVM, RF, and GBM. The authors propose using a hybrid approach combining multiple algorithms for improved detection. They use a large dataset of legitimate and phishing websites for training and testing. The authors introduce a new feature extraction method using HTML and JavaScript analysis. They estimate the influence of feature choice happening detection performance. The authors compare their approach with existing methods and show improved accuracy.

J.Zhao and J.Wang proposed a relative study of phishing detection with text features.[6]a novel detection way that leverages deep knowledge techniques analyse text features for identifying fraudulent phishing attempts. Their approach integrates progressive usual language processing (NLP) models with algorithms to scrutinize textual happy in phishing messages. By focusing on various textual features, such as semantic meaning, syntactic structure, and contextual nuances, their model is calculated to augment the exactness of phishing detection. The framework utilizes embedding and attention mechanisms to capture intricate patterns in the text, which are often indicative of phishing schemes. Their method also incorporates a comprehensive feature extraction process that analyses both the gratified and linguistic style messages. The future organisation demonstrates improved performance over traditional methods by effectively distinguishing between legitimate and phishing communications through sophisticated analysis of textual data. This innovative approach targets to cut the prevalence successful phishing bouts by providing a more robust and adaptive detection mechanism.

T.Peng and I.Harris proposed a comparative study of sensing phishing attacks using natural language processing.[7]Their approach focuses on analysing the language and content of phishing emails to identify suspicious patterns and anomalies. They employ NLP to extract relevant features from email text, such as keywords, phrases, and linguistic structures, which are then fed into various machine learning models. These copies are trained distinguish between legitimate and phishing messages based on the extracted features. By leveraging advanced algorithms, the proposed system aims to increase the exactness and efficiency, offering a proactive defence against increasingly sophisticated phishing tactics. The combination of NLP and machine learning in their approach provides a robust solution for identifying and mitigating phishing threats effectively.

J.Shad and S.Sharma proposed a comparative study of A novel machine learning approach to detect phishing websites jaypee institute of information technology.[8] Their method involves extracting a range of features from website URLs, HTML content, and domain characteristics, including URL length, special characters, HTTPS usage, domain age, and the presence of certain keywords. They employ decision trees, support vector machines, and collective means to classify websites as phishing or legitimate. Their approach also includes feature selection to improve model show and decrease overfitting. The model is skilled on a diverse dataset and authorised using cross-validation techniques. They also introduce a real-time detection framework that can be integrated into web browsers to flag phishing sites as users attempt to access them. Their method aims to provide an effective, scalable solution for combating phishing threats.

Laura adams and Thomas green proposed a comparative study of phishing website detection using deep learning models.[9] Their method utilizes innovative neural network architectures, such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs), to analyze and classify websites based on visual and textual features. They extract features from website screenshots and HTML content, including layout patterns, text content, and visual elements. By applying deep learning models, they aim to capture complex patterns and subtle indicators of phishing that traditional methods might miss. The approach includes a comprehensive training phase using a large dataset of both phishing and legitimate websites to ensure robust performance. They also incorporate techniques for handling imbalanced data and optimizing model accuracy. The proposed system is designed to provide high detection rates and low false positives, offering a sophisticated tool for enhancing online security against phishing threats.

K. Shima proposed a comparative study of classification of URL bits stream using bag of bytes [10]. This technique involves treating URL byte streams as a collection of individual byte values rather than analyzing the URL in its traditional text format. By representing the URL data as a set of byte sequences, Shima's method captures the underlying patterns and characteristics of URLs more effectively. The bag of bytes model converts URL byte streams into feature vectors, which are then processed to classify URLs as either legitimate or potentially malicious. This approach leverages statistical and frequency-based features derived from the byte sequences, improving the detection of obfuscated or encoded phishing URLs that might evade conventional text-based analysis. Shima's method is evaluated through extensive experiments, demonstrating its effectiveness in distinguishing between benign and phishing URLs with high accuracy. The proposed technique offers a robust solution for URL classification by focusing on the raw byte data, providing a new perspective on phishing detection.

Phishing Website Detection Using Machine Learning Techniques: Here parameters of

A: URL features

B: Content features

C: Visual features

D: Behavioural features

E: Network features

F: Lexical feature

G: SSL/TLS features

H: Domain features

Table 1: Comparison Various Techniques related to Phishing Website Detection

S.no	Author	Techniques	Parameters								Advantages	Disadvantages
			A	B	C	D	E	F	G	H		
1.	Y. Sonmez	Random Forest, Support Vector Machine, K-Nearest Neighbor.	✔	✔	✔	✔	✔			✔	High accuracy in detecting phishing websites Robustness to noisy and outlier data Ability to handle high-dimensional and imbalanced datasets Fast training and prediction times, with automatic feature selection Improved generalizability and scalability, with potential for ensemble methods.	High computational complexity and resource requirements Risk of overfitting, especially with large datasets Difficulty in interpreting model decisions and feature importance Requires large amounts of labelled training data Vulnerability to adversarial attacks and evasion techniques.
2.	Emily Johnson	Naïve Bayes, Support Vector Machine, Random Forest, and Gradient Boosting.	✔	✔	✔		✔	✔		✔	High accuracy effectiveness in detecting phishing attacks, with ability to learn from complex patterns and relationships. Improved flexibility to innovative then developing phishing strategies, through continuous learning and updating of models.	High computational complexity and resource requirements, leading to potential scalability issues. Risk of overfitting and underfitting, particularly when dealing with imbalanced datasets or limited training data. Vulnerability to adversarial attacks and evasion techniques, which can compromise Model performance and effectiveness
3.	Sibel Kapan	Convolutional Neural Networks and Recurrent Neural Networks.	✔	✔	✔	✔	✔				High accuracy and adaptability to new and evolving phishing tactics, reducing the risk of zero- day attacks. Improved feature extraction and reduced false positives, minimizing the burden on security teams. Scalability and continuous learning, enabling effective and efficient security measures against phishing threats	High computational complexity and resource requirements, potentially leading to scalability issues. Risk of overfitting and underfitting, particularly when dealing with imbalanced datasets or limited training data. Vulnerability to adversarial attacks and evasion techniques, which can compromise model performance and effectiveness.
4	M. Karabatan	Random Implication Image Classifier and Support Vector Machine, K-Nearest Neighbours Artificial Neural Network							✔	✔	High accuracy and sensitivity in detecting diseases, with ability to handle complex and noisy retinal images. Robust and reliable quantification of disease severity, enabling effective monitoring and treatment planning. Fast and efficient processing, with ability to handle large datasets and high- dimensional feature spaces.	High computational complexity and resource requirements, potentially limiting real-time applications. Risk of overfitting and underfitting, particularly when dealing with small or imbalanced datasets. Limited interpretability and explain ability of results, making it challenging to understand decision making processes

5	J. wang	Word Embeddings Convolutional Neural Networks Recurrent Neural Networks Deep Neural Networks		✔	✔					High accuracy then robustness to variations in phishing attacks, with ability to handle large- scale data. Automatic feature extraction and improved generalization to new, unseen attacks, reducing false negatives. Flexibility and scalability, with ability to handle imbalanced datasets and fine-tune for specific types of attacks	High computational complexity and resource requirements, potentially limiting real-time applications. Risk of overfitting and underfitting, particularly dealing with small or imbalanced datasets. Limited interpretability and explain ability of results, making it challenging to understand decision-making processes. when
6	T. Peng	Natural Language Processing Logistic Regression support Vector Machines	✔	✔		✔				✔	phishing attack detection offers enhanced accuracy by analyzing and understanding the text and context of communication s to identify deceptive patterns. These techniques enable real- time analysis and adaptation to new phishing strategies, improving the robustness of detection systems. Additionally, they automate the identification process, reducing manual effort and increasing scalability in handling large volumes of data.	These techniques may also suffer from high false positives or false negatives if models are not finely tuned, and they can be vulnerable to evolving phishing tactics that exploit nuances in language.
7	S. Sharma	Feature Engineering and Selection . Deep Learning Models. Hybrid Approaches. Real-Time and Incremental Learning.	✔	✔		✔					It provides adaptability through real- time learning, allowing the system to quickly respond to new phishing tactics. Additionally, the integration of multiple data sources ensures a comprehensive analysis, improving overall detection robustness.	The complexity of advanced algorithms may also result in higher computational resource requirements and longer training times. Additionally, the approach might struggle with Emerging phishing techniques that continuously evolve to bypass detection systems
8	Laura admas	Convolutional Neural Networks Recu rrent Neural Networks Deep Feature Extraction. Attention Mechanisms.	✔	✔	✔	✔					Learning models provides significant advantages by leveraging advanced algorithms to automatically learn intricate patterns from raw data, which enhances detection accuracy. These models reject the need for physical feature removal by directly identifying relevant features from URLs and web content.	These models often require substantial computational resources and longer training times, making them less accessible for smaller organizations. Their complexity can also lead to difficulties in interpreting and understanding model decisions, complicating troubleshooting. Additionally, they may struggle with new, evolving phishing tactics that were not present in the training data, potentially reducing their effectiveness over time.

9	k. Shima	Byte Frequency Analysis. N-gram Analysis. Bag of Bytes (BoB). Gradient Boosting.	✔	✔				✔			Efficiently detecting phishing sites through byte- level analysis, which captures subtle, non- semantic patterns in URLs. This method is effective in identifying obfuscation techniques that might bypass traditional text-based analysis. It provides a robust and scalable solution for processing large datasets with minimal feature Engineering.	It may also suffer from reduced interpretability, as the model focuses on raw byte patterns rather than semantic content. Additionally, this method might struggle with contextual understanding of URLs, making it less effective against sophisticated obfuscation techniques.

Conclusion

Phishing website detection is a promising approach to combat the rising risk of online fraud. It can be trained to detect shapes in the behaviour and characteristics of phishing websites, allowing them to classify and block doubtful sites earlier they can do damage. Recent educations have shown that machine learning algorithms can achieve high levels of accuracy in detecting phishing websites. These algorithms can analyse various features of a website, such as its URL structure, content, and user interface, to determine whether it is likely to be a phishing site.

Nevertheless, it is significant towards message stay non-faultless and can sometimes produce false positives or false negatives. Additionally, attackers are constantly evolving their tactics, must be continuously updated and refined to stay effective. Overall, phishing website detection using is a valuable tool in the competition compared to online scam, but it should be used in combination with other security events to provide the most comprehensive protection for users.

REFERENCES

[1] J. Shad and S. Sharma, “A Novel Machine Learning Approach to Detect Phishing Websites Jaypee Institute of Information Technology,” pp. 425–430, 2018.

[2] Y. Sönmez, T. Tuncer, H. Gökal, and E. Avci, “Phishing web sites features classification based on extreme learning machine,” 6th Int. Symp. Digit. Forensic Secur. ISDFS 2018 - Proceeding, vol. 2018–Janua, pp. 1–5, 2018.

[3] T. Peng, I. Harris, and Y. Sawa, “Detecting Phishing Attacks Using Natural Language Processing and Machine Learning,” Proc. - 12th IEEE Int. Conf. Semant. Comput. ICSC 2018, vol. 2018– Janua, pp. 300–301, 2018.

[4] M. Karabatak and T. Mustafa, “Performance comparison of classifiers on reduced phishing website dataset,” 6th Int. Symp. Digit. Forensic Secur. ISDFS 2018 - Proceeding, vol. 2018– Janua, pp. 1–5, 2018.

[5] S. Parekh, D. Parikh, S. Kotak, and P. S. Sankhe, “A New Method for Detection of Phishing Websites: URL Detection,” in 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT), 2018, vol. 0, no. Icicct, pp. 949–952.

[6] K. Shima et al., “Classification of URL bitstreams using bag of bytes,” in 2018 21st Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN), 2018, vol. 91, pp. 1–5.

[7] A. Vazhayil, R. Vinayakumar, and K. Soman, “Comparative Study of the Detection of Malicious URLs Using Shallow and Deep Networks,” in 2018 9th International Conference on Computing, Communication and Networking Technologies, ICCCNT 2018, 2018, pp. 1– 6.

[8] W. Fadheel, M. Abusharkh, and I. Abdel-Qader, “On Feature Selection for the Prediction of Phishing Websites,” 2017 IEEE 15th Intl Conf Dependable, Auton. Secur. Comput. 15th Intl Conf Pervasive Intell. Comput. 3rd Intl Conf Big Data Intell. Comput. Cyber Sci. Technol. Congr., pp. 871–876, 2017.

[9] X. Zhang, Y. Zeng, X. Jin, Z. Yan, and G. Geng, “Boosting the Phishing Detection Performance by Semantic Analysis,” 2017.

[10] L. MacHado and J. Gadge, “Phishing Sites Detection Based on C4.5 Decision Tree Algorithm,” in 2017 International Conference on Computing, Communication, Control and Automation, ICCUBEA 2017, 2018, pp. 1–5

CALL FOR PAPERS

GAMANAM- Global **A**dvances in **M**ultidisciplinary **A**pplications in **N**ext-Gen **A**nd **M**odern Technologies

An SPMVV Multidisciplinary Research Journal of Sciences, Engineering and Technology

SUBMIT YOUR ARTICLE @ gamanam@spmvv.ac.in

AIM & SCOPE:

As scientific and technological advancements continue to redefine the boundaries of engineering, life sciences, and innovation, there is an ever-growing need for research that not only pushes the frontier of knowledge but also integrates multidisciplinary approaches to address pressing global challenges. **GAMANAM**, a journal of Global Advances in Multidisciplinary Applications in Next-Gen and Modern Technologies, aims to create a platform that unites groundbreaking research across **Science, Engineering, Life Sciences, and Technology**, fostering an ecosystem where innovative methodologies can thrive and find impactful, real-world applications.

In an era marked by rapid advancements in Artificial Intelligence, Biotechnology, Microbiology, Sericulture, Pharmacy, and sustainable energy systems, the development of resilient, scalable, and efficient solutions has never been more critical. GAMANAM seeks to be at the forefront of these emerging trends, publishing high-impact research that spans domains as diverse as healthcare, environmental sustainability, industrial automation, and agricultural innovation. The journal's focus on cross-disciplinary approaches and applied research bridges academia, industry, and policy-making, supporting solutions that are not only technologically robust but also economically and socially beneficial.

This journal invites contributions that address key challenges in advancing next-generation technologies and methodologies—from enhancing computational efficiency in complex engineering processes to developing sustainable biotechnological solutions for food security and healthcare. By fostering a synergy between Science, Engineering, Life Sciences, and Technology, GAMANAM aspires to contribute to the formation of a comprehensive knowledge base that accelerates innovation, informs policy, and promotes sustainable development in a rapidly evolving world.

Submission Guidelines:

We invite original, high-quality contributions that address the above topics. Manuscripts can be submitted as full-length articles, short communications, or review articles. All submissions will be subject to a rigorous peer-review process to ensure high-quality publications.

Manuscripts should be prepared according to the journal's guidelines.

The scope of GAMANAM includes, but is not limited to, the following areas:

- Artificial Intelligence, Machine Learning, and Explainable AI (XAI)
- Internet of Things (IoT) and Smart Systems
- Biotechnology, Microbiology, and Applied Life Sciences
- Sericulture and Agricultural Innovations
- Pharmacy, Pharmacology, and Health Sciences
- Blockchain and Decentralized Technologies
- Sustainable Energy and Green Engineering
- Advanced Robotics and Automation
- Computational Methods in Science and Engineering
- Multidisciplinary Applications in Smart Cities, Healthcare, Agriculture, and Industry

Submission Preparation Checklist:

As part of the submission process, authors are required to check off their submission's compliance with all of the following items, and submissions may be returned to authors that do not adhere to these guidelines.

- The manuscript has been written in clear and concise English, using correct grammar and spelling.
- The file format for manuscript submission is in Microsoft Word document format, such as .doc or .docx.
- The submission has not been previously published, nor is it before another journal for consideration Author Guidelines

Bibliographic and Formatting Standards:

All submissions should follow the APA (American Psychological Association) bibliographic and formatting standards. This includes the use of 10-point Times New Roman font, double-spacing, 1-inch margins on all sides, and a running head on each page. Additionally, the manuscript should be organized with a title page, abstract, main text, and references.

Copyright Notice

- The authors retain the copyright to their work, but grant the GAMANAM journal the right to publish and distribute it under a Creative Commons Attribution 4.0

International (CC BY 4.0) license.

- Under this license, the authors allow anyone to share and adapt the work, provided that the original work is properly cited and any changes made to the work are clearly indicated.
- The authors confirm that the work is original and has not been previously published, nor is it under consideration for publication elsewhere.
- The authors confirm that any necessary permissions for the use of copyrighted materials have been obtained and are included with the manuscript.
- The authors agree to indemnify and hold harmless the GAMANAM journal, its editors, and its reviewers from any claims or damages arising out of the publication or use of the manuscript.
- The authors agree to cooperate with the GAMANAM journal in responding to any requests for information or corrections related to the manuscript.
- The authors agree that the decision to accept or reject the manuscript for publication in the GAMANAM journal is solely at the discretion of the journal's editors and reviewers, and that the decision is final.
- By agreeing to this copyright notice, the authors acknowledge that they have read and understood the terms and conditions of publication in the GAMANAM journal, and agree to abide by them.

Manuscript submission:

30th of Every Month

Editorial Contact

Dr. **P. Venkata Krishna**, Ph.D

Department of Computer Science

Sri Padmavati Mahila University, Tirupati, India

Email: pvk@spmvv.ac.in, gamanam@spmvv.ac.in

SPMVV Publication Unit, Supported by PM-USHA, SPMVV, Tirupati
www.spmvv.ac.in