JCMM

Journal of Computers, Mechanical and Management

e-ISSN: 3009-075X

Volume 4, Issue 2

2025

AAN PUBLISHING

JCMM Journal of Computers, Mechanical and Management
Journal homepage: www.jcmm.co.in e-ISSN: 3009-075X
AAN PUBLISHING

Editorial Comments Volume 4 Issue 2

Ritesh Bhat* [1,2]

[1]Department of Mechatronics Engineering, Rajalakshmi Engineering College, Thandalam, Tamil Nadu, India 602015

[2]Journal of Computers, Mechanical and Management, AAN Publishing, Kangar Perlis, Malaysia 01000

Volume 4, Issue 2 of the *Journal of Computers, Mechanical, and Management* featured a diverse selection of studies highlighting advancements in intelligent systems, cybersecurity, healthcare technologies, and structural engineering. These contributions reflected the journal's ongoing commitment to interdisciplinary research and the development of data-driven, secure, and scalable solutions. Nikhil Kassetty [1] examined a dual-layered fraud mitigation framework in fintech by combining blockchain's transparency with artificial intelligence's predictive capabilities. The review addressed emerging challenges in digital financial systems and proposed a holistic solution for real-time threat detection. Pandit D. Pradeep and Manoj E. Patil [2] introduced a blockchain-driven software engineering framework that enhanced the scalability and security of IoT ecosystems. By leveraging smart contracts and decentralized control, their framework offered robust applications across domains such as healthcare, industrial automation, and supply chain management. Sonam and Jyoti [3] provided a comprehensive narrative review of data mining algorithms—Apriori, FP-Growth, and ECLAT—for recognizing user behavior. An illustrative walkthrough of Apriori was included to clarify algorithmic complexity, while the study discussed performance trade-offs and practical implications. Abhishek Kumar et al. [4] conducted a comparative evaluation of convolutional neural networks for the classification of upper respiratory infections using chest X-rays. DenseNet demonstrated the highest diagnostic efficiency, while ResNet-50 offered a balanced trade-off between performance and speed. The findings supported the integration of AI in resource-constrained diagnostic settings. Suresh Tiwari [5] surveyed recent mechanical joining techniques for metal–composite hybrid structures, including self-piercing riveting, friction riveting, and form-locked joints developed through additive manufacturing. The review emphasized joint durability, nanofiber reinforcement, and challenges in manufacturability and long-term performance. Shaharkar B. Bharat and Manoj E. Patil [6] proposed a blockchain-integrated framework for secure health monitoring with wearable devices. The study implemented decentralized authentication and smart contract automation to improve data protection, enable anomaly detection, and address vulnerabilities in cloud-based healthcare systems. Collectively, these articles demonstrated the journal's focus on technological convergence and real-world impact. The editorial board expressed appreciation to the authors for their original research and to the reviewers for their constructive evaluations. Readers were encouraged to engage with the findings presented in this issue, which offered valuable insights into the digital, secure, and sustainable future of applied sciences.

*Corresponding Author: Editor-in-Chief (journalmanager@jcmm.co.in)

Received: 01 May 2025; **Revised:** 01 May 2025; **Accepted:** 01 May 2025; **Published:** 01 May 2025

DOI: 10.57159/jcmm.4.2.25216.

References

[1] N. Kassetty, “Blockchain and ai in fintech: A dual approach to fraud mitigation,” *Journal of Computers, Mechanical, and Management*, vol. 4, no. 2, pp. 1–8, 2025.

[2] P. D. Pradeep and M. E. Patil, “Innovative iot development: A blockchain-driven software engineering approach with smart contracts,” *Journal of Computers, Mechanical, and Management*, vol. 4, no. 2, pp. 9–16, 2025.

[3] Sonam and Jyoti, “A narrative review of data mining techniques for user behavior recognition with illustrative application of the apriori algorithm,” *Journal of Computers, Mechanical, and Management*, vol. 4, no. 2, pp. 17–23, 2025.

[4] P. Tiwari, A. Kumar, and R. K. Burman, “Comparative evaluation of ai models for automated classification of upper respiratory infections using chest x-ray imaging,” *Journal of Computers, Mechanical, and Management*, vol. 4, no. 2, pp. 24–29, 2025.

[5] S. Tiwari, “Advances in mechanical joining techniques for metal–composite hybrid structures—a mini review,” *Journal of Computers, Mechanical, and Management*, vol. 4, no. 2, pp. 30–39, 2025.

[6] S. B. Bharat and M. E. Patil, “Blockchain-integrated authentication framework for secure cloud-based health monitoring with wearable devices,” *Journal of Computers, Mechanical, and Management*, vol. 4, no. 2, pp. 40–47, 2025.

JCMM Journal of Computers, Mechanical and Management
Journal homepage: www.jcmm.co.in e-ISSN: 3009-075X
AAN PUBLISHING

Volume 4 Issue 2

Article Number: 25193

Blockchain and AI in Fintech: A Dual Approach to Fraud Mitigation

Nikhil Kassetty*

Senior Software Engineer, Independent Researcher, Atlanta, Georgia, USA

Abstract

This study examines fraud reduction in the fintech industry via the combined use of blockchain and artificial intelligence (AI). The immutable ledger of blockchain enhances transparency and security, reducing the risk of data breaches and unauthorized financial transactions. AI, powered by machine learning algorithms, enables real-time, high-precision fraud detection and prediction. The integration of these technologies in fintech results in efficient, scalable, and cost-effective fraud prevention frameworks. This mini-review evaluates current advancements, highlights operational benefits and challenges, and identifies future research directions for secure, innovative financial services.

Keywords: Fintech Systems; Blockchain Technology; Artificial Intelligence; Fraud Mitigation

1. Introduction

The convergence of artificial intelligence (AI) and blockchain technology has transformed the fintech sector, providing a new paradigm for financial institutions, businesses, and consumers [1]. AI, supported by advanced machine learning algorithms, utilizes predictive analytics and cognitive computing to automate and optimize core financial operations such as risk assessment, fraud detection, investment management, and customer service [2, 3]. Meanwhile, blockchain technology, originating as the backbone of digital currency, has evolved to enable secure, transparent, and efficient financial transactions worldwide [1, 4]. Blockchain systems have revolutionized payments, settlements, and asset management by reducing costs and operational risks [4]. Beyond their strengths, integrating AI and blockchain redefines traditional financial systems by supporting innovations in digital identity, tokenization, decentralized finance (DeFi), and smart contracts [4]. However, this rapid digitization brings new challenges, such as identity theft, data breaches, and evolving fraud techniques [5]. As financial services become more accessible through mobile banking and digital currencies, the need for robust, scalable, and real-time fraud prevention frameworks has intensified. In this technologically advanced landscape, self-executing blockchain protocols and AI-driven digital banking systems present opportunities and vulnerabilities. While decentralized blockchain networks offer scalable security, they may harbor protocol-specific risks. Likewise, AI systems face issues related to algorithmic bias, data privacy, and adaptability to emerging threats [6]. Integrating these technologies must address privacy, ethical, and operational considerations to build reliable fraud detection solutions for fintech. AI and blockchain have emerged as complementary tools for mitigating financial fraud. AI applies advanced data analysis, including deep learning and natural language processing, to identify suspicious patterns more effectively than conventional methods [6]. Blockchain enhances data integrity and transparency through decentralized, immutable ledgers, supporting regulatory compliance and Know Your Customer (KYC) requirements [6, 7]. The synergy between AI's predictive power and blockchain's tamper-proof record-keeping underpins efficient, next-generation fraud prevention systems [8]. Figure 1 illustrates the evolution from a single-tier to a dual-tier model in financial technology, demonstrating the enhanced security, transparency, and operational efficiency achieved through integrating blockchain and financial institution nodes [7]. This mini review critically examines the

*Corresponding Author: Nikhil Kassetty (nikhil.kassetty@email.com)

Received: 19 Jan 2025; **Revised:** 13 Feb 2025; **Accepted:** 29 Apr 2025; **Published:** 30 Apr 2025

DOI: 10.57159/jcmm.4.2.25193.

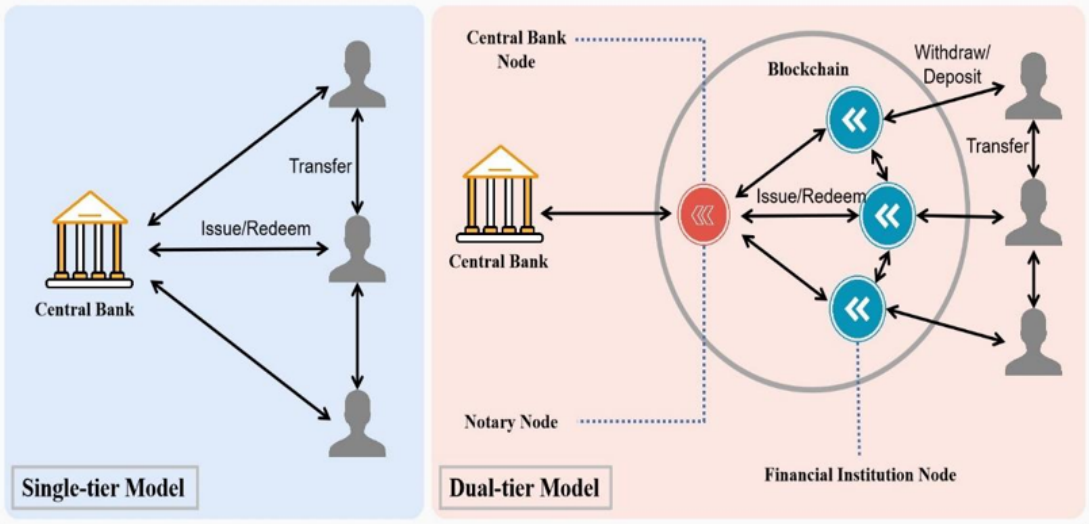

Figure 1: Comparison of single-tier and dual-tier models in fintech, highlighting the integration of blockchain for secure and transparent financial operations [7].

combined application of AI and blockchain for fraud mitigation in fintech. It addresses the need for accurate, scalable, and real-time fraud detection, evaluates current methodologies, and explores practical advice for deploying advanced fraud prevention technologies [3].

The article further highlights research objectives, including analyzing cost reduction, exploring synergies and conflicts in technology integration, and evaluating real-time, scalable fraud detection frameworks [9]. The study also identifies major challenges—such as scalability, interoperability, security, and regulatory compliance—and concludes by outlining future research directions for the secure, innovative advancement of financial services [10, 11].

2. Recent Developments and Challenges in AI–Blockchain Enabled Fintech

Recent advances in financial technology are driven by the integration of artificial intelligence (AI) and blockchain, resulting in enhanced security, efficiency, and innovative financial services. AI supports real-time analytics, fraud detection, risk assessment, and customer service automation, while blockchain provides immutable transaction verification, secure digital identities, and decentralized financial processes [12, 3, 1]. Current implementations show significant improvements in fraud mitigation, operational transparency, and financial product personalization. These technologies are not limited to traditional banking; they are also transforming cloud-based fintech applications, digital asset management, and even carbon market monitoring by leveraging AI's anomaly detection and blockchain's secure record-keeping [13, 14]. The combined use of smart contracts, IoT integration, and data science further automates compliance and boosts reliability in financial reporting and audit [15]. Despite these advantages, several technical and practical challenges remain. Interoperability between AI and blockchain platforms is hindered by the lack of standardized interfaces, making integration complex and costly [12]. High computational requirements, data privacy issues, and algorithmic bias in AI models pose additional barriers. Most existing studies focus on conceptual or small-scale implementations, leaving a gap in large-scale, real-world evaluation and adoption [16, 17]. Furthermore, scaling these solutions raises concerns over energy consumption, especially for blockchain networks. Legal and regulatory uncertainties also persist, as rapid innovation often outpaces the establishment of industry standards.

Achieving compliance and ethical data management is vital for broad adoption and trust in these systems [18, 19]. As a result, future research should prioritize the development of interoperable frameworks, privacy-preserving AI, and regulatory-aligned solutions to realize the full potential of AI–blockchain integration in fintech.

3. AI and Blockchain Applications in Fraud Mitigation

Artificial intelligence (AI) and blockchain technology are reshaping financial fraud prevention by introducing automation, transparency, and predictive accuracy. AI is particularly effective in detecting fraudulent behavior by processing massive datasets in real-time, leveraging algorithms such as decision trees, logistic regression, K-nearest neighbors, naïve Bayes, and random forests [20]. These models identify unusual patterns that may indicate phishing, identity theft, or money laundering. Figure 2 illustrates a complete AI-based fraud detection pipeline—from data collection to model evaluation—highlighting critical stages like preprocessing, feature engineering, and hyperparameter tuning. A simplified decision-making flow in AI fraud systems is shown in Figure 3, where processed data is analyzed to detect malicious behavior and initiate threat mitigation processes.

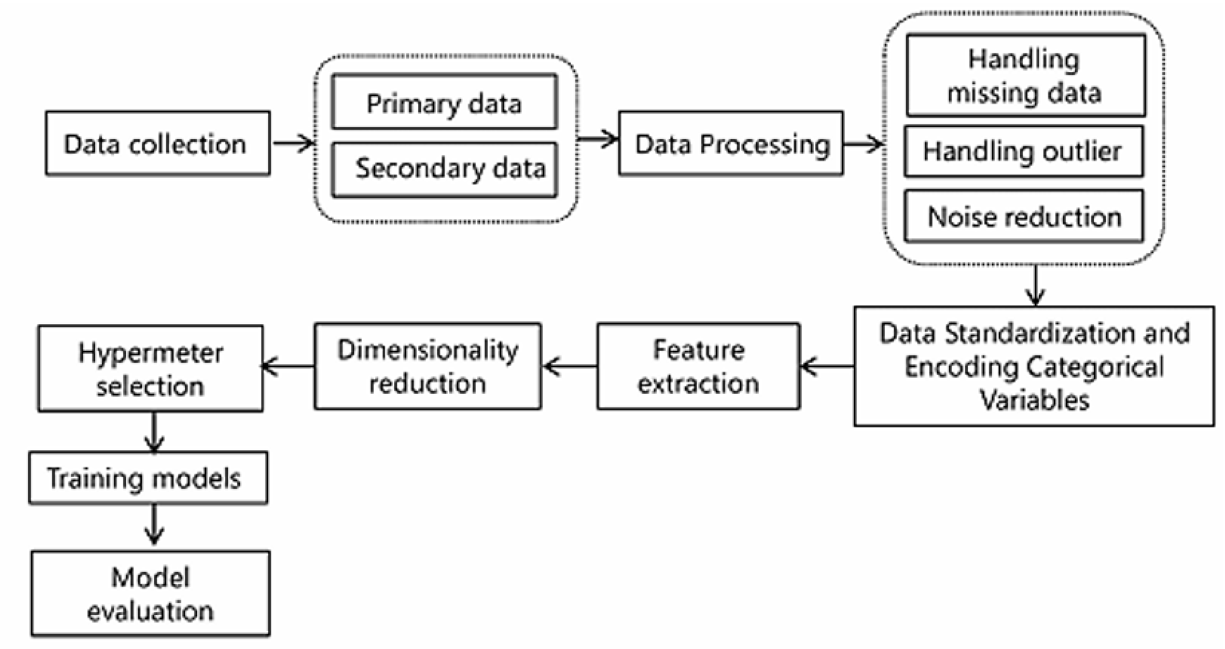

Figure 2: AI fraud detection pipeline: data collection, preprocessing, feature extraction, and model training [20].

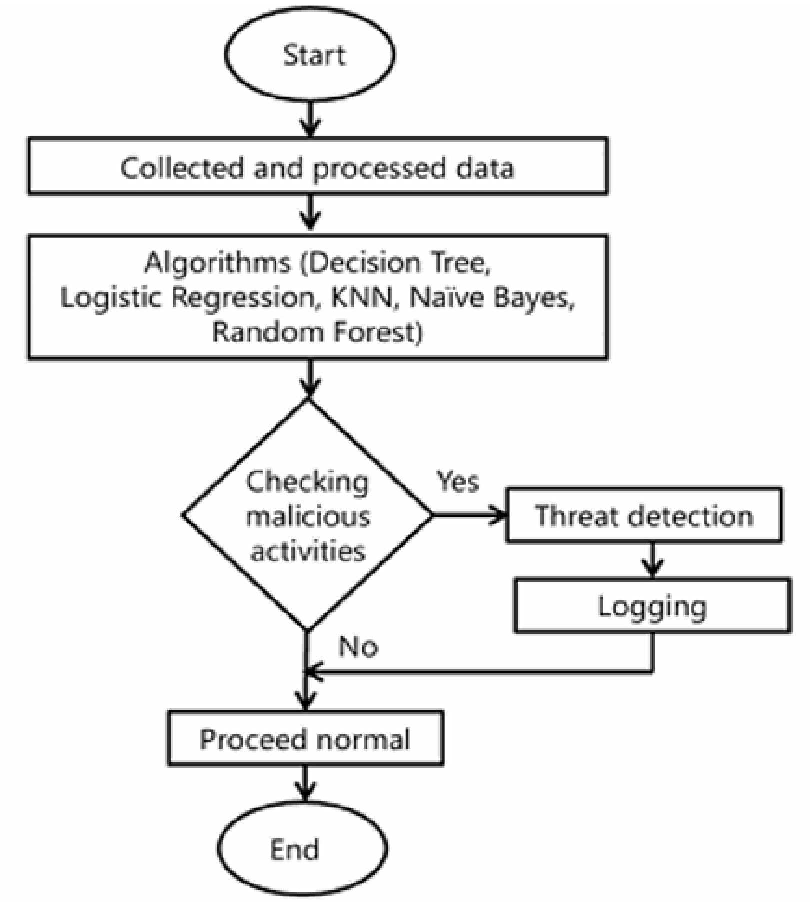
Start
Collected and processed data
Algorithms (Decision Tree, Logistic Regression, KNN, Naïve Bayes, Random Forest)
Checking malicious activities
Yes
Threat detection
Logging
No
Proceed normal
End

Figure 3: AI-based fraud detection decision flow using supervised learning algorithms [20].

Comparative evaluation of fraud detection datasets, their usage frequencies, and performance metrics further supports AI's effectiveness. Figure 4 presents commonly used datasets, with credit card fraud detection leading in application volume. Figure 5 shows accuracy, detection time, and cost comparisons between traditional and AI-based fraud detection systems. AI methods demonstrate superior performance, albeit with higher implementation costs.

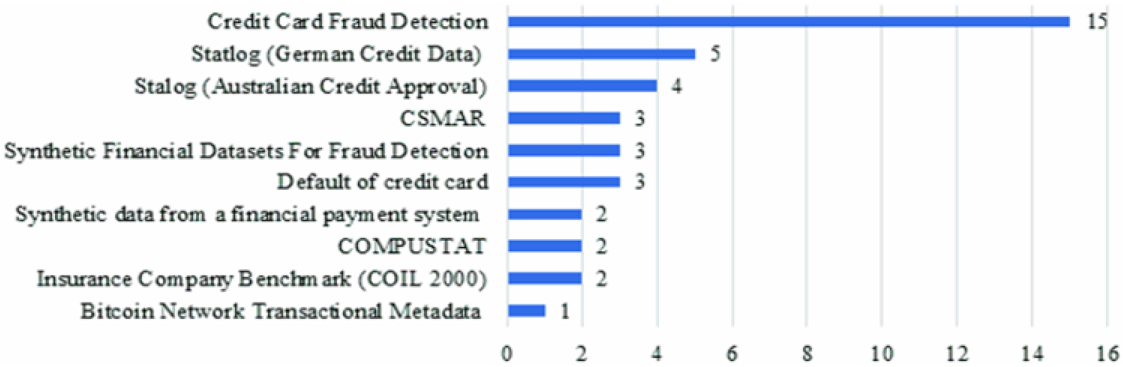

Figure 4: Popular datasets used in financial fraud detection research [21].

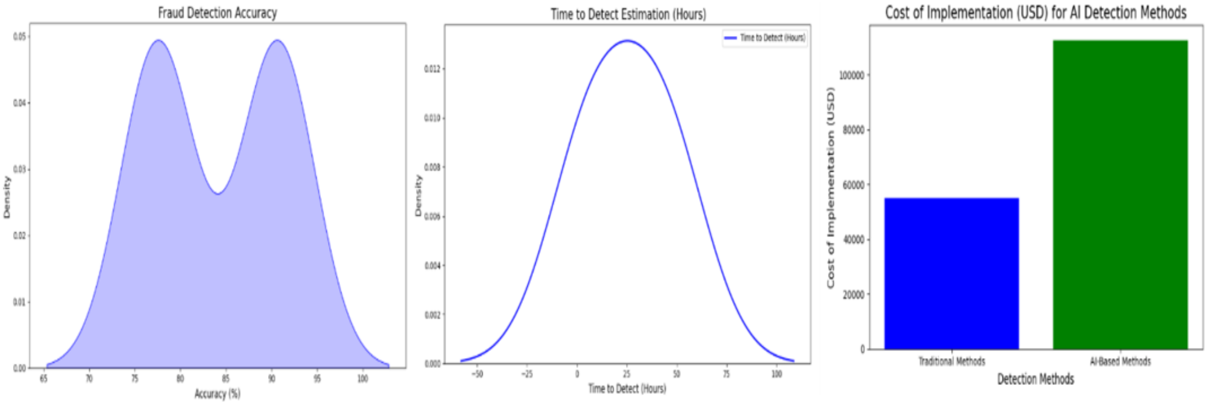

Figure 5: Metrics comparison for AI vs. traditional fraud detection methods: accuracy, detection time, and cost [22].

Blockchain adds an immutable and decentralized layer of security to fintech applications. Its implementation in fraud mitigation involves smart contracts and consensus mechanisms, ensuring transactional transparency and resistance to tampering. Figure 6 shows a proposed layered architecture integrating AI and blockchain for enhanced fraud detection.

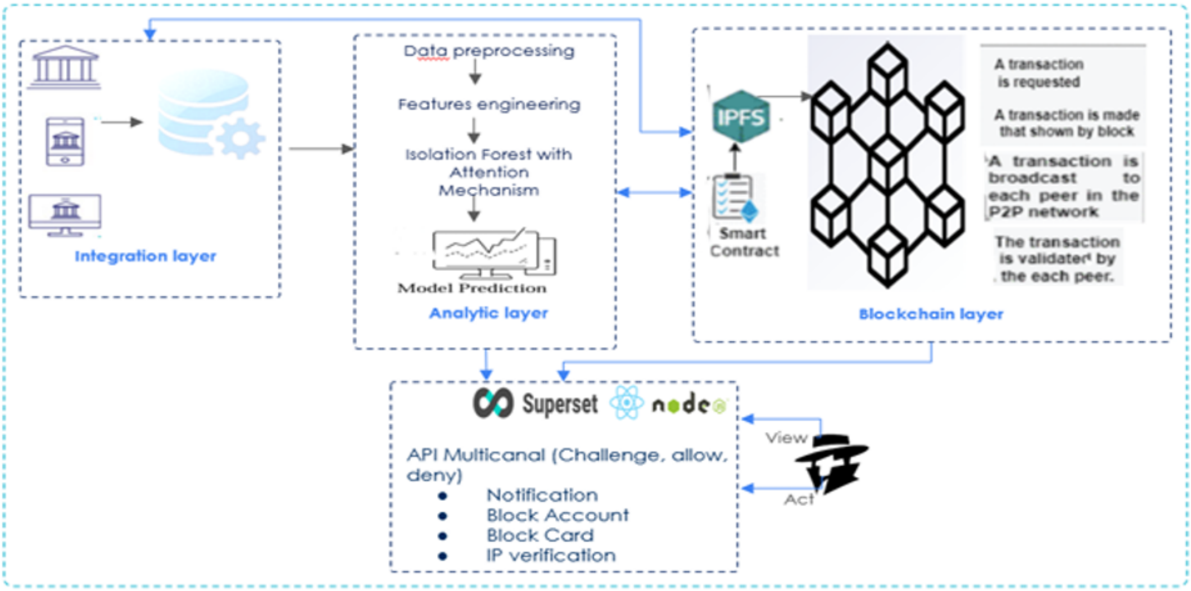
Integration layer
Data preprocessing
Features engineering
Isolation Forest with Attention Mechanism
Model Prediction
Analytic layer
IPFS
Smart Contract
A transaction is requested
A transaction is made that shown by block
A transaction is broadcast to each peer in the P2P network
The transaction is validated by the each peer.
Blockchain layer
Superset
node
API Multicanal (Challenge, allow, deny)
Notification
Block Account
Block Card
IP verification
View
Act

Figure 6: Integrated architecture: AI analytic layer, blockchain smart contracts, and multichannel API for real-time fraud alerts [23].

The superiority of AI-based fraud detection over traditional approaches is quantitatively evident. As shown in Table 1, AI systems provide markedly higher accuracy, reduced detection times, and—while costlier to implement—offer substantial operational benefits in the long run [22]. Table 2 further demonstrates the higher true positive rates and lower false positive rates of AI-enabled detection, underscoring the practical value of AI in modern fintech fraud prevention [22].

Table 1: Comparative Table on AI Fraud Detection (2019–2024) [22].

Detection Method	Accuracy (%)	Time to Detect (Hours)	Cost (USD)
Traditional Methods	77.5	43	$55,000
AI-Based Methods	90.67	7.5	$112,500

Table 2: Fraud Detection: True Positive Rate (TPR) and False Positive Rate (FPR) [22].

Detection Method	True Positive Rate (TPR)	False Positive Rate (FPR)
Traditional Methods	77.5	43
AI-Based Methods	90.67	7.5

Blockchain applications in identity verification, anti-money laundering, and secure settlements have become prevalent in banking. Figure 7 illustrates core blockchain use cases within fintech ecosystems, including trade finance and tokenized payments. Overall, the synergy of AI and blockchain offers real-time detection, tamper-proof recording, and increased customer trust. However, challenges such as energy efficiency, cost, and algorithmic fairness remain critical areas for future research and optimization.

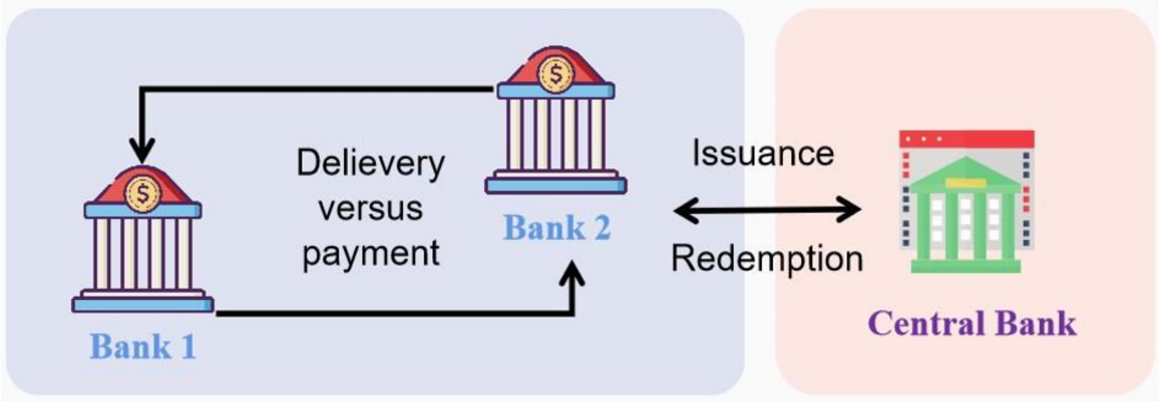

Figure 7: Core blockchain applications in financial services, including digital identity, asset transfer, and fraud prevention [7].

4. Challenges and Research Gaps

Despite the transformative potential of blockchain and AI in fintech, several critical challenges must be addressed to enable reliable and widespread adoption. These challenges include scalability, security, interoperability, regulatory compliance, and standardization.

- **Scalability and Interoperability:** Both blockchain and AI systems are resource-intensive, requiring substantial computational power to manage large transaction volumes and complex datasets efficiently [24]. Blockchains often face limitations in transaction throughput and latency, while AI systems demand distributed computing resources for real-time processing. Interoperability is also a significant barrier, as the absence of standardized protocols hinders seamless integration across blockchain networks and AI platforms. Greater standardization and cross-platform collaboration are essential for scalable deployments.

- **Security:** Financial systems remain prime targets for cyberattacks due to the sensitive nature and value of financial data [25]. While AI-driven fraud detection systems have enhanced security, technical vulnerabilities persist. Blockchain security depends on robust cryptographic algorithms, but future advancements such as quantum computing may compromise current standards. Furthermore, the complexity of decentralized consensus mechanisms introduces new attack vectors, and poorly designed smart contracts may allow for errors or exploitation [25].

- **Regulatory Compliance:** Compliance with financial regulations is essential for fintech operations. AI and blockchain technologies must adhere to stringent requirements for anti-money laundering (AML), know-your-customer (KYC), and transaction monitoring [24, 26]. Integrating AI-based compliance with legacy systems can be technically challenging, and the rapid pace of fintech innovation frequently outpaces regulatory frameworks, complicating consistent and effective oversight.

- **Research Gaps:** There are notable gaps in the standardization and practical deployment of integrated AI–blockchain systems for fraud prevention. The lack of unified frameworks limits scalability and adoption across financial ecosystems [18]. Most existing research focuses on theoretical or small-scale pilot studies, with limited real-world validation [2]. Moreover, privacy-preserving methods, ethical considerations, and comprehensive interoperability solutions remain underexplored [27].

Addressing these challenges and research gaps will require coordinated efforts among technologists, regulators, and industry stakeholders to develop scalable, secure, and compliant frameworks for the next generation of fintech innovation.

5. Conclusion and Future Scope

In summary, the integration of blockchain and artificial intelligence (AI) represents a transformative advancement in fintech fraud mitigation. By combining blockchain's secure, decentralized, and transparent ledger systems with AI's capabilities in real-time anomaly detection, predictive analytics, and adaptive learning, financial institutions can establish robust frameworks that significantly enhance financial security and operational efficiency. This integration not only builds trust among stakeholders but also reduces operational inefficiencies and associated costs. Looking ahead, the development of scalable and energy-efficient blockchain architectures remains a critical area for innovation. The adoption of advanced AI techniques, such as deep learning and reinforcement learning, can further improve the adaptability and accuracy of fraud detection systems. Achieving seamless integration between blockchain and AI for real-time data sharing will be essential for maximizing the benefits of these technologies. Moreover, global collaboration on regulatory frameworks will be necessary to foster the widespread adoption of AI–blockchain fintech solutions. As financial institutions increasingly implement these integrated systems, they can expect enhanced transaction transparency, improved customer trust, and greater compliance with regulatory standards, ultimately shaping a more secure and innovative financial ecosystem.

Declaration of Competing Interests

The author declares no known competing financial interests or personal relationships.

Funding Declaration

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Ethics Statement

All data used in this research adhere to ethical AI and data privacy standards, ensuring compliance with GDPR, CCPA, and relevant financial regulations.

Author Contributions

Nikhil Kassetty: Conceptualization, Methodology, Supervision, Data Analysis, Software, Validation, Investigation, Visualization, Writing – Original Draft, Review, and Editing.

References

[1] P. Kamuangu, "Advancements of ai and machine learning in fintech industry (2016-2020)," *Journal of Economics Finance and Accounting Studies*, vol. 6, pp. 23–31, Jan 2024.

[2] C. Gitobu and N. J. Ogetonto, "Harnessing artificial intelligence (ai) and blockchain technology for the advancement of finance technology (fintech) in businesses," in *Proceedings of London International Conferences*, no. 11, pp. 196–210, Nov 2024.

[3] S. R. Addula, K. Meduri, G. S. Nadella, and H. Gonaygunta, "Ai and blockchain in finance: Opportunities and challenges for the banking sector," *IJARCCE*, vol. 13, Feb 2024.

[4] M. V. Jhansi, "Mediating effect of artificial intelligence and blockchain technology in finance: Opportunities and challenges," *Decision Making: Applications in Management and Engineering*, vol. 8, Jan 2024.

[5] N. O. Angela, N. I. Atoyebi, N. A. Soyele, and N. E. Ogunwobi, "Enhancing fraud detection and prevention in fintech: Big data and machine learning approaches," *World Journal of Advanced Research and Reviews*, vol. 24, no. 2, pp. 2301–2319, 2024.

[6] N. P. O. Shoetan and N. B. T. Familoni, "Transforming fintech fraud detection with advanced artificial intelligence algorithms," *Finance & Accounting Research Journal*, vol. 6, no. 4, pp. 602–625, 2024.

[7] Q. Hanjie, Z. Liu, B. Huang, Y. Zhuang, H. Tang, and E. Liu, "Blockchain for finance: A survey," *IET Blockchain*, 2024.

[8] Q. Yao, "Supervision of blockchain-based new fmis," in *Blockchain-based New Financial Infrastructures: Theory, Practice and Regulation*, pp. 171–181, Springer, 2022.

[9] B. E. Abikoye, W. Adelusi, S. C. Umeorah, A. O. Adelaja, and C. Agorbia-Atta, "Integrating risk management in fintech and traditional financial institutions through ai and machine learning," *Journal of Economics Management and Trade*, vol. 30, no. 8, pp. 90–102, 2024.

[10] A. Kumari and N. C. Devi, "The impact of fintech and blockchain technologies on banking and financial services," *Technology Innovation Management Review*, vol. 12, no. 1/2, 2022.

[11] M. Paramesha, N. Rane, and J. Rane, "Artificial intelligence, machine learning, deep learning, and blockchain in financial and banking services: A comprehensive review," *Journal*, vol. 1, no. 2, pp. 51–67, 2024.

[12] N. O. Odeyemi, N. C. C. Okoye, N. O. C. Ofodile, N. O. B. Adeoye, N. W. A. Addy, and N. a. O. Ajayi-Nifise, "Integrating ai with blockchain for enhanced financial services security," *Finance & Accounting Research Journal*, vol. 6, no. 3, pp. 271–287, 2024.

[13] A. R. Kunduru, "Artificial intelligence advantages in cloud fintech application security," *Central Asian Journal of Mathematical Theory and Computer Sciences*, vol. 4, no. 8, pp. 48–53, 2023.

[14] N. O. A. Adigun *et al.*, "Enhancing carbon markets with fintech innovations: The role of artificial intelligence and blockchain," *World Journal of Advanced Research and Reviews*, vol. 23, no. 2, pp. 579–586, 2024.

[15] P. Roszkowska, "Fintech in financial reporting and audit for fraud prevention and safeguarding equity investments," *Journal of Accounting & Organizational Change*, vol. 17, no. 2, pp. 164–196, 2020.

[16] O. Mandych, T. Staverska, and O. Maliy, "Integration of artificial intelligence into the blockchain and cryptocurrency market," *Modeling the Development of the Economic Systems*, no. 4, pp. 61–66, 2023.

[17] G. Lăzăroiu, M. Bogdan, M. Geamănu, L. Hurloiu, L. Luminița, and R. Ștefănescu, "Artificial intelligence algorithms and cloud computing technologies in blockchain-based fintech management," *Oeconomia Copernicana*, vol. 14, no. 3, pp. 707–730, 2023.

[18] N. O. A. Bello and N. K. Olufemi, "Artificial intelligence in fraud prevention: Exploring techniques and applications challenges and opportunities," *Computer Science & IT Research Journal*, vol. 5, no. 6, pp. 1505–1520, 2024.

[19] N. T. O. Sanyaolu, N. A. G. Adeleke, N. C. F. Azubuko, and N. O. S. Osundare, "Exploring fintech innovations and their potential to transform the future of financial services and banking," *International Journal of Scholarly Research in Science and Technology*, vol. 5, pp. 054–072, Sep 2024.

[20] F. T. Johora, R. Hasan, S. F. Farabi, J. Akter, and M. A. A. Mahmud, "Ai-powered fraud detection in banking: Safeguarding financial transactions," *The American Journal of Management and Economics Innovations*, vol. 6, no. 6, pp. 8–22, 2024.

[21] L. Hernandez Aros, L. Bustamante Molano, and F. Gutierrez-Portela, "Financial fraud detection through the application of machine learning techniques: a literature review," *Commun*, vol. 11, p. 1130, 2024.

[22] A. Cherif, A. Badhib, H. Ammar, and S. Alshehri, "Credit card fraud detection in the era of disruptive technologies: A systematic review," *Journal of King Saud University - Computer and Information Sciences*, vol. 35, no. 1, pp. 145–174, 2023.

[23] A. Hanae, E. M. Saida, and G. Youssef, “Synergy of machine learning and blockchain strategies for transactional fraud detection in fintech systems,” in *11th International Conference on Future Internet of Things and Cloud*, pp. 292–297, 2024.

[24] N. Rane, S. Choudhary, and J. Rane, “Blockchain and artificial intelligence (ai) integration for revolutionizing security and transparency in finance,” *SSRN Electronic Journal*, 2023.

[25] N. O. A. Farayola, “Revolutionizing banking security: Integrating artificial intelligence, blockchain, and business intelligence for enhanced cybersecurity,” *Finance & Accounting Research Journal*, vol. 6, no. 4, pp. 501–514, 2024.

[26] T. Renduchintala, H. Alfauri, Z. Yang, R. Pietro, and R. Jain, “A survey of blockchain applications in the fintech sector,” *J. Open Innov. Technol. Mark. Complex.*, vol. 8, p. 185, 2022.

[27] V. D. P. Sambrow and K. Iqbal, “Integrating artificial intelligence in banking fraud prevention: A focus on deep learning and data analytics,” *Eigenpub Review of Science and Technology*, vol. 6, no. 1, pp. 17–33, 2022.

Journal of Computers, Mechanical and Management
Journal homepage: www.jcmm.co.in
e-ISSN: 3009-075X

Volume 4 Issue 2

Article Number: 25211

Innovative IoT Development: A Blockchain-Driven Software Engineering Approach with Smart Contracts

Pandit Darshan Pradeep and Manoj E. Patil*

Department of Computer Science and Engineering, Mansarovar Global University, Sehore, Madhya Pradesh, India 466111

Abstract

The rapid advancement of the Internet of Things (IoT) is reshaping industries by enabling seamless communication between devices, real-time data collection, and automation. Given the surge in IoT applications, challenges related to security, scalability, and interoperability have become increasingly critical. This study presents a state-of-the-art software engineering framework designed to address these limitations through the integration of blockchain technology and smart contracts. By leveraging the decentralized, immutable, and transparent nature of blockchain, the proposed framework enhances trust and security within IoT environments. Smart contracts, as secure, self-executing code, facilitate autonomous interactions between IoT devices without relying on centralized control. Additionally, the framework introduces novel strategies for optimizing resource management and data handling efficiency while improving system scalability across distributed networks. The synergistic use of blockchain and smart contracts not only resolves key IoT challenges but also contributes to the development of robust, efficient, and scalable IoT ecosystems. The framework is applicable across diverse domains, including healthcare, smart cities, supply chain management, and industrial automation, fostering innovative, self-governing IoT systems throughout their operational lifecycle.

Keywords: Next-Gen IoT; Blockchain Integration; Smart Contracts; IoT Security; Decentralized Systems; Scalable IoT Framework

1. Introduction

The Internet of Things (IoT) has emerged as a transformative technology in the 21st century, significantly impacting various sectors by enabling seamless communication among interconnected devices. The rapid proliferation of IoT systems has led to a substantial increase in the number of connected devices and their communication channels, thereby necessitating the development of robust, scalable, and secure frameworks. Traditional IoT architectures often encounter challenges related to data privacy, security, and interoperability, primarily due to their reliance on centralized control mechanisms [1]. To address these limitations, the integration of next-generation blockchain technology and smart contracts introduces a paradigm shift in IoT development, facilitating the evolution of a modern software engineering framework. Unlike conventional IoT systems that are constrained by centralized servers, blockchain technology offers decentralized, immutable, and secure data management capabilities. Additionally, mechanisms such as proof of authority and smart contracts—self-executing agreements triggered by predefined conditions—minimize third-party dependencies and enhance trustless automation in IoT networks [2]. In this architecture, blockchain serves as a transparent and verifiable ledger, ensuring data integrity and decentralized control of IoT devices. Smart contracts enhance operational efficiency by enabling autonomous, real-time decision-making among devices and applications without human intervention.

*Corresponding Author: Manoj E. Patil (mepatil@gmail.com)

Received: 26 Mar 2025; **Revised:** 15 Apr 2025; **Accepted:** 29 Apr 2025; **Published:** 30 Apr 2025

DOI: 10.57159/jcmm.4.2.25211.

This integrated approach significantly improves security, privacy, scalability, and system performance, making it well-suited for applications in healthcare, finance, smart cities, supply chain management, and industrial automation. The convergence of blockchain and smart contracts with IoT represents a significant advancement in software engineering, fostering the development of secure, scalable, and intelligent IoT ecosystems. This introduction outlines the foundational strengths of the proposed framework, highlighting its practical applications and its potential to reshape contemporary technological solutions.

2. Related Work

The integration of blockchain technology into IoT networks has attracted substantial attention across various industrial domains, primarily due to its potential to enhance security, data integrity, and operational efficiency. Numerous studies have explored the viability and implications of this convergence. Mercan et al. (2020) [3] proposed a blockchain-based IoT forensics framework to improve the security and accountability of IoT devices. They emphasized the shortcomings of traditional forensic methods in handling decentralized IoT platforms and demonstrated the effectiveness of blockchain in maintaining audit trails for forensic evidence. Shaikh et al. (2021) [4] examined the role of blockchain in decentralized data storage within IoT systems. Their study underscored the significance of blockchain's immutability, privacy, and consensus mechanisms in addressing scalability and security concerns. Kabir et al. (2021) [5] introduced a secure cloud communication model that integrates blockchain with IoT. Their framework employed smart contracts to automate security processes, ensuring secure data exchange between IoT devices and cloud services. Madhwal and Yanovich (2024) [6] presented a live implementation of a blockchain-enabled IoT supply chain system. Their work showcased the potential of blockchain in real-time goods tracking, fraud prevention, and overall supply chain transparency and efficiency. Al-Nbhany et al. (2024) [7] conducted a comprehensive review of blockchain applications in IoT-based healthcare systems. Their research highlighted the technology's capability to secure patient data, facilitate remote monitoring, and enhance healthcare data integration and protection. Collectively, these studies underscore the transformative potential of blockchain in IoT environments, laying the groundwork for more secure, transparent, and efficient systems. However, existing solutions often lack a unified, scalable framework that seamlessly integrates blockchain with smart contracts for comprehensive automation and trust management in IoT networks. The proposed methodology aims to address these gaps by developing an advanced, blockchain-driven IoT software engineering framework.

3. Proposed Methodology

A comprehensive understanding of blockchain algorithms and their integration with IoT systems is essential for enabling secure, decentralized, and transparent operations. Key blockchain mechanisms such as consensus algorithms, cryptographic hash functions, and public-key cryptography form the foundation of a decentralized ledger, allowing IoT devices to interact securely and autonomously [4]. Consensus mechanisms ensure agreement across distributed nodes. Proof of Work (PoW), used by Bitcoin, is secure but computationally intensive and unsuitable for IoT due to energy demands [5]. Proof of Stake (PoS) offers a more energy-efficient alternative by selecting validators based on token holdings [3]. Practical Byzantine Fault Tolerance (PBFT) enhances reliability by tolerating malicious nodes through multiple rounds of validation [6]. Delegated Proof of Stake (DPoS) scales effectively by enabling IoT devices to delegate validation duties to more powerful nodes [7]. Hash functions ensure data integrity and immutability. SHA-256, a widely used cryptographic algorithm, transforms data into fixed-length hash values. Any modification to the input data changes the hash, enabling effective detection of tampering in IoT transmissions [8–10]. Public-key cryptography secures blockchain transactions by assigning unique key pairs to IoT devices. This approach enables authenticated and encrypted communication, ensuring only authorized devices can interact on the network. Elliptic Curve Cryptography (ECC) is particularly efficient for IoT due to its low computational overhead [11]. Smart contracts are self-executing scripts that automate operations based on predefined conditions. These contracts eliminate the need for manual intervention, enhancing system responsiveness. Trigger conditions may include sensor thresholds or event-based inputs, while the execution logic specifies the resulting actions. Once deployed, the contract code remains immutable, preserving trust [12, 13]. The proposed algorithm integrates these technologies to facilitate secure, scalable transactions and autonomous device interactions in IoT environments.

3.1. Assumptions:

- Each IoT device is registered with a unique identifier and cryptographic key pair.
- Devices connect to a blockchain using consensus mechanisms such as PoS or PBFT.
- Smart contracts govern device operations and data recording [14].

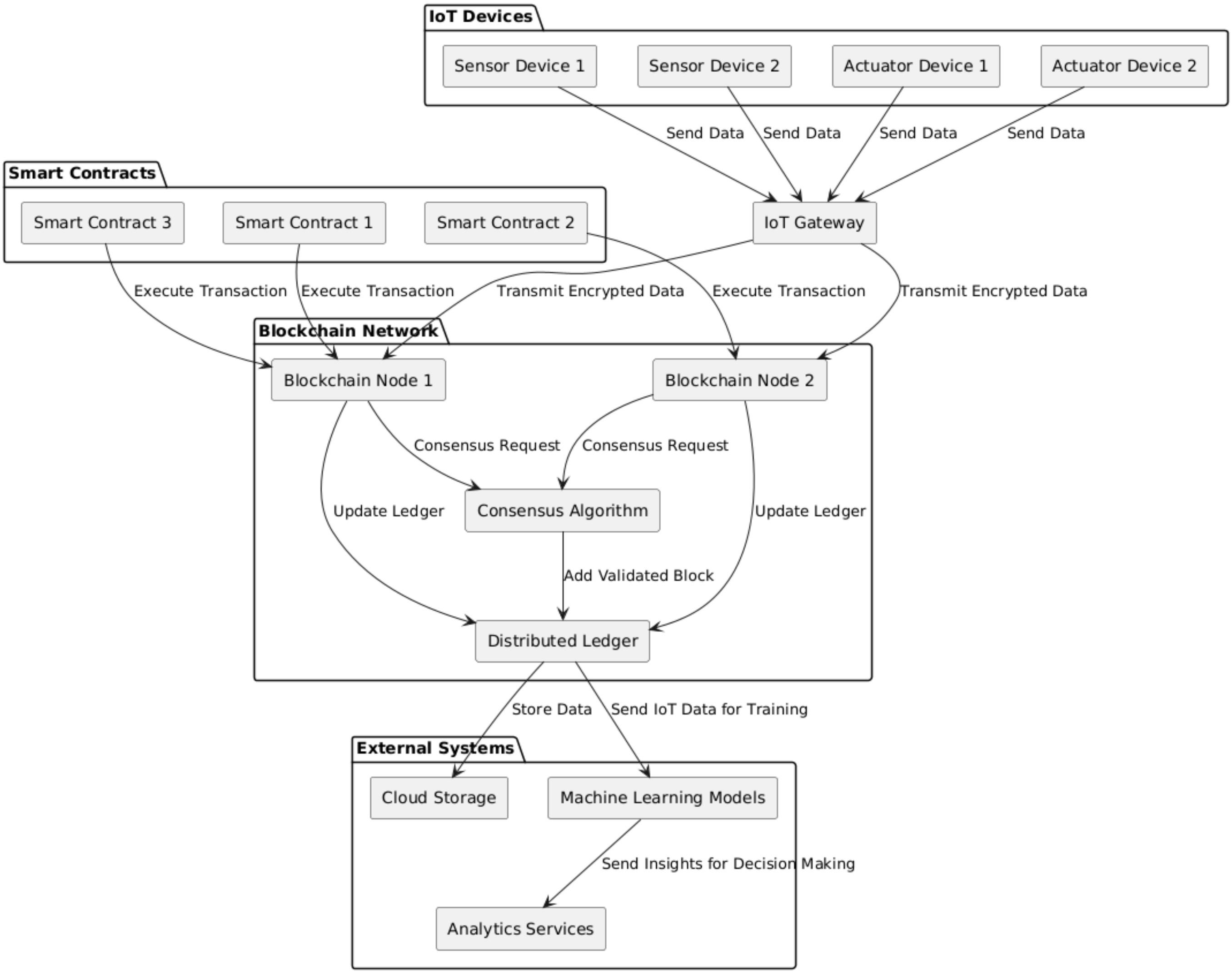

Figure 1: Proposed model integrating IoT with blockchain and smart contracts.

3.2. Algorithm: IoT Device Interaction Using Blockchain and Smart Contracts

Algorithm 1 IoT Device Interaction Using Blockchain and Smart Contracts

```
procedure INITIALIZE
    Initialize BlockchainNetwork()
    Register IoT Device $D_i$ with public key $PK_i$
end procedure
procedure REGISTERDEVICE($D_i, PK_i$)
    if BlockchainNetwork.verifyUnique($D_i$) then
        $Address_i \leftarrow$ BlockchainNetwork.generateAddress($D_i$)
        BlockchainNetwork.register($D_i, Address_i, PK_i$)
        return $Address_i$
    else
        return “Device already registered”
    end if
end procedure
procedure TRANSMITDATA($D_i, SD_i, PK_B$)
    $EncData_i \leftarrow$ Encrypt($SD_i, PK_B$)
    $Tx_i \leftarrow$ BlockchainNetwork.createTransaction($D_i, EncData_i$)
    BlockchainNetwork.submitTransaction($Tx_i$)
    return $Tx_i$
end procedure
procedure CONSENSUSVALIDATION($Tx_i$)
    if BlockchainNetwork.consensus.verify($Tx_i$) then
        BlockchainNetwork.addBlock($Tx_i$)
        return “Transaction added to blockchain”
    else
        return “Transaction failed validation”
    end if
end procedure
procedure SMARTCONTRACTEXECUTION($Tx_i, SC_j$)
    if SC_j.conditionMet(Tx_i) then
        ExecuteAction($SC_j, D_k$)
        return “Smart contract executed”
    else
        return “Conditions not met”
    end if
end procedure
procedure ACKNOWLEDGEEXECUTION($D_k, Tx_j$)
    $Ack \leftarrow D_k$.sendAcknowledgment($Tx_j$)
    BlockchainNetwork.recordAck($Ack$)
    return “Acknowledgment recorded”
end procedure
procedure ENCRYPT($SD_i, PK_B$)
    $EncData_i \leftarrow$ AsymmetricEncrypt($SD_i, PK_B$)
    return $EncData_i$
end procedure
```

This algorithm ensures secure, transparent, and autonomous interaction between IoT devices through blockchain validation and smart contract automation. The system maintains data integrity and enables real-time responses while reducing human involvement [15].

4. Results and Discussion

Simulation tools and supporting technologies are vital in the development and validation of blockchain-integrated IoT systems. Platforms such as MATLAB, Simulink, and Cisco Packet Tracer are used to model IoT networks, simulate data flows, and evaluate device interactions. The outcome of these simulations includes the generation of encrypted smart contracts, which are subsequently deployed on blockchain platforms such as Hyperledger Fabric and Ethereum to facilitate secure transactions. Containerization tools like Docker and orchestration frameworks like Kubernetes further support system deployment and scalability. Collectively, these technologies enable the development of robust, scalable, and replicable IoT solutions across automotive, industrial, and smart infrastructure domains [16–18].

Table 1: Qualitative Performance Comparison of IoT Architectures

Metrics	**Centralized IoT**	**Traditional Blockchain IoT**	**Blockchain + PoW**	**Blockchain + PoS**	**Proposed (Blockchain + SC)**
Data Security	Low	Medium	High	High	Very High
Scalability	High	Low	Medium	High	High
Latency	Low	High	High	Medium	Low
Energy Efficiency	High	Low	Very Low	Medium	High
Consensus Speed	N/A	Slow	Slow	Fast	Fast
Transaction Throughput (TPS)	High	Low	Low	Medium	High
Fault Tolerance	Medium	High	Medium	High	Very High
Automation Capability	Low	Low	Medium	Medium	Very High
Transparency	Low	High	High	High	Very High
Data Immutability	Low	High	High	High	Very High
Cost Efficiency	Medium	High	Low	Medium	High
Real-Time Processing	Medium	Low	Low	Medium	High
Interoperability	Medium	Low	Low	Medium	High

Table 2: Quantitative Results Analysis (Performance Scores)

Metrics	**Centralized IoT**	**Traditional Blockchain IoT**	**Blockchain + PoW**	**Blockchain + PoS**	**Proposed (Blockchain + SC)**
Data Security	4	6	8	9	10
Scalability	8	4	5	8	9
Latency	3	6	5	7	9
Energy Efficiency	9	5	3	7	9
Consensus Speed	–	3	4	8	9
Transaction Throughput (TPS)	9	3	4	7	9
Fault Tolerance	5	7	6	8	10
Automation Capability	2	4	6	7	10
Transparency	3	8	8	9	10
Data Immutability	3	8	8	9	10
Cost Efficiency	7	4	2	7	9
Real-Time Processing	6	4	4	7	9
Interoperability	6	5	5	7	9

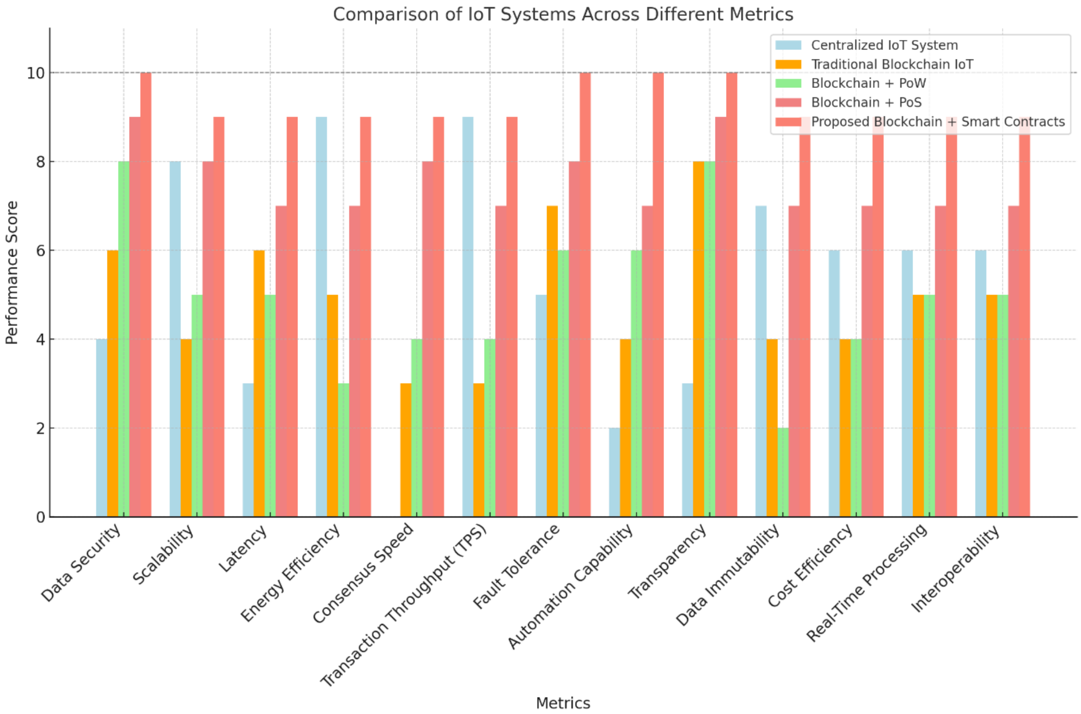

Figure 2: Results Analysis: Performance Comparison of IoT Systems

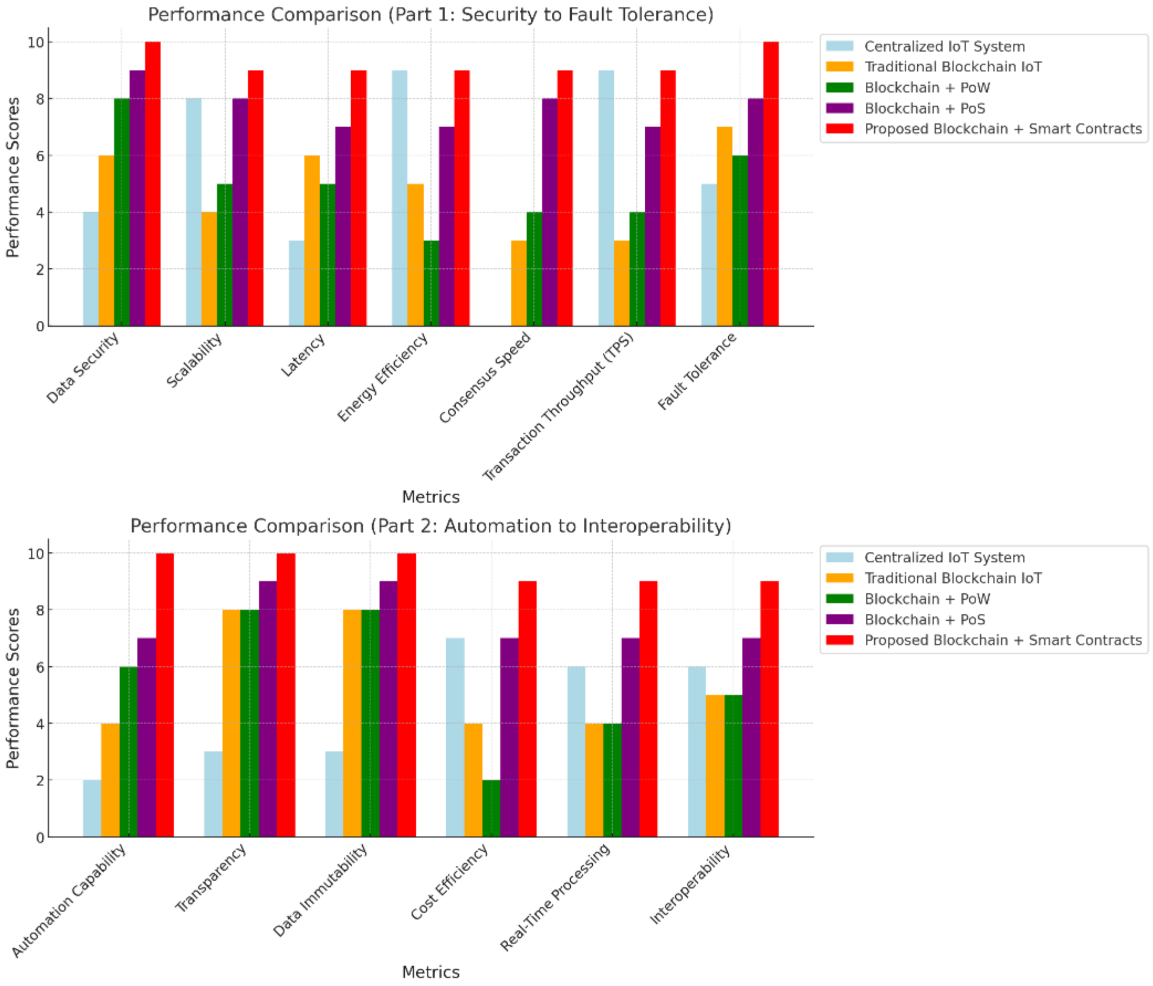

Figure 3: Performance Analysis (Split by Metric Groups)

The quantitative results clearly demonstrate the superiority of the proposed blockchain-integrated IoT framework enhanced by smart contracts. A performance score of 10 in data security reflects the benefits of cryptographic immutability inherent in blockchain. Scalability and latency metrics also score high due to efficient consensus mechanisms and minimized overhead. Energy efficiency is significantly improved through the use of lightweight consensus algorithms such as PoS. Consensus speed and transaction throughput are notably enhanced, allowing the system to support real-time, high-frequency IoT interactions. Automation capability reaches its peak due to the self-executing nature of smart contracts. Transparency and data immutability are maximized, ensuring accountability and integrity. The comparative visualizations in Figures 2 and 3 further validate these outcomes. The proposed system consistently outperforms centralized IoT models, traditional blockchain approaches, and PoW-based systems across all key metrics. While PoS mitigates energy concerns, only the proposed architecture effectively integrates automation and real-time processing. In summary, the proposed blockchain-smart contract model achieves optimal balance across performance dimensions—security, efficiency, automation, cost, and interoperability—making it well-suited for large-scale, modern IoT deployments.

5. Conclusion

The integration of blockchain technology with smart contracts represents a significant advancement in the development of next-generation IoT systems. This study has demonstrated that the proposed framework addresses the core challenges faced by traditional IoT architectures, including issues related to security, scalability, latency, and energy efficiency. By leveraging decentralized consensus mechanisms and self-executing smart contracts, the framework ensures trustless automation, robust data integrity, and real-time responsiveness. Comparative analysis confirms that the proposed system outperforms centralized and conventional blockchain-based IoT models across multiple metrics, including data security, fault tolerance, transparency, and operational efficiency. The use of energy-efficient consensus algorithms such as Proof of Stake (PoS) enables practical implementation in resource-constrained IoT environments. Furthermore, the automation enabled by smart contracts significantly reduces the need for manual intervention, enhancing reliability and reducing operational overhead. From healthcare and finance to smart cities and industrial automation, the versatility and robustness of the proposed framework make it suitable for a broad spectrum of applications. Its high degree of interoperability, transparency, and cost-effectiveness positions it as a transformative solution capable of meeting the evolving demands of IoT ecosystems. Ultimately, the framework paves the way for intelligent, secure, and scalable IoT infrastructures that can drive innovation and operational excellence in the digital age.

Declaration of Competing Interests

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Funding Declaration

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Author Contributions

Manoj E. Patil: Conceptualization, Supervision, Project Administration, Writing – Review and Editing; **Pandit Darshan Pradeep**: Methodology, Investigation, Software, Data Analysis, Writing – Original Draft

References

[1] Dharani and S. M. K. ur Rehman Raazi, "Integrating blockchain with iot for mitigating cyber threat in corporate environment," in *2022 Mohammad Ali Jinnah University International Conference on Computing (MAJICC)*, (Karachi, Pakistan), pp. 1–6, 2022.

[2] D. K. J. B. Saini, S. Kumar, A. Bhatt, R. Gupta, K. Joshi, and D. Siddharth, "Blockchain-based iot applications, platforms, systems and framework," in *2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, (Delhi, India), pp. 1–6, 2023.

[3] S. Mercan, M. Cebe, E. Tekiner, K. Akkaya, M. Chang, and S. Uluagac, "A cost-efficient iot forensics framework with blockchain," in *2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, (Toronto, ON, Canada), pp. 1–5, 2020.

[4] M. Shaikh, C. Shibu, E. Angeles, and D. Pavithran, "Data storage in blockchain based architectures for internet of things (iot)," in *2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)*, (Toronto, ON, Canada), pp. 1–5, 2021.

[5] R. Kabir, A. S. M. T. Hasan, M. R. Islam, and Y. Watanobe, "A blockchain-based approach to secure cloud connected iot devices," in *2021 International Conference on Information and Communication Technology for Sustainable Development (ICICT4SD)*, (Dhaka, Bangladesh), pp. 366–370, 2021.

[6] Y. Madhwal and Y. Yanovich, "Blockchain-iot demo for supply chain management," in *2024 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, (Dublin, Ireland), pp. 7–8, 2024.

[7] W. A. N. A. Al-Nbhany, A. T. Zahary, and A. A. Al-Shargabi, "Blockchain-iot healthcare applications and trends: A review," *IEEE Access*, vol. 12, pp. 4178–4212, 2024.

[8] M. Khattat and R. Kromes, "Completely frost-ed: Iot issued frost signature for hyperledger fabric blockchain," in *2024 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, (Dublin, Ireland), pp. 200–204, 2024.

[9] A. Dixit, A. Trivedi, and W. W. Godfrey, "Iot and machine learning based peer to peer framework for employee attendance system using blockchain," in *2022 International Conference on Augmented Intelligence and Sustainable Systems (ICAISS)*, (Trichy, India), pp. 1088–1093, 2022.

[10] A. A. Sadawi, M. S. Hassan, and M. Ndiaye, "A survey on the integration of blockchain with iot to enhance performance and eliminate challenges," *IEEE Access*, vol. 9, pp. 54478–54497, 2021.

[11] M. Shurman, A. A. R. Obeidat, and S. A. D. Al-Shurman, "Blockchain and smart contract for iot," in *2020 11th International Conference on Information and Communication Systems (ICICS)*, (Irbid, Jordan), pp. 361–366, 2020.

[12] A. D. Aguru and S. B. Erukala, "Blockchain-based edge device authentication mechanism in sdn-enabled iot networks," in *2024 IEEE 9th International Conference for Convergence in Technology (I2CT)*, (Pune, India), pp. 1–6, 2024.

[13] J. Moghariya and P. G. Shambharkar, "Blockchain-enabled iot (b-iot): Overview, security, scalability & challenges," in *2023 Second International Conference on Trends in Electrical, Electronics, and Computer Engineering (TEECCON)*, (Bangalore, India), pp. 210–217, 2023.

[14] Y. Dash and P. Yadav, "The synergy of blockchain and iot: A comprehensive security perspective," in *2024 IEEE International Conference on Computing, Power and Communication Technologies (IC2PCT)*, (Greater Noida, India), pp. 34–38, 2024.

[15] V. L. K. Seng, A. T. Wan, and S. H. S. Newaz, "State management against two-message attacks in hash-based post quantum signatures for large iot sensor networks using blockchain," in *2023 6th International Conference on Applied Computational Intelligence in Information Systems (ACIIS)*, (Bandar Seri Begawan, Brunei Darussalam), pp. 1–6, 2023.

[16] S. N, V. B. K, and M. Rajarajan, "Blockchain-based scheme for authentication and capability-based access control in iot environment," in *2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, (New York, NY, USA), pp. 0323–0330, 2020.

[17] M. ElKashlan and M. Azer, "Mitigating iot security challenges using blockchain," in *2020 15th International Conference on Computer Engineering and Systems (ICCES)*, (Cairo, Egypt), pp. 1–6, 2020.

[18] A. Moon, S. Mishra, and M. Mali, "Enhancing security, privacy, and scalability in blockchain and internet of things (iot): A survey," in *2023 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS)*, (New Raipur, India), pp. 1–6, 2023.

JCMM Journal of Computers, Mechanical and Management
Journal homepage: www.jcmm.co.in e-ISSN: 3009-075X
AAN PUBLISHING

Volume 4 Issue 2

Article Number: 25214

A Narrative Review of Data Mining Techniques for User Behavior Recognition with Illustrative Application of the Apriori Algorithm

Sonam* and Jyoti

Department of Computer Science Engineering, Baba Mastnath University, Rohtak, Haryana, India 124001

Abstract

This review examines key data mining algorithms used for user behaviour recognition in computational systems, focusing on frequent pattern mining techniques. We summarize foundational methods such as Apriori, FP-Growth, and ECLAT, comparing their operational principles and limitations. A frequency-based literature analysis shows the widespread use of Apriori in market basket analysis. To illustrate its workings, we include a demonstrative walkthrough of the Apriori algorithm using a hypothetical dataset. The article concludes with insights into performance trade-offs and future directions in algorithmic efficiency.

Keywords: Data Mining; User Behavior; Apriori; FP-Growth; ECLAT; Association Rule Mining

1. Introduction

In today's data-driven landscape, organizations across industries—such as retail, healthcare, and finance—generate massive amounts of data daily. The critical challenge lies in converting this raw data into actionable insights, particularly for understanding user behaviour patterns. Data mining, also known as Knowledge Discovery in Databases (KDD), plays a central role in extracting such patterns [1]. Frequent Pattern Mining (FPM), a key subfield of data mining, focuses on discovering recurring relationships among data items. These patterns often indicate significant behavioural traits such as co-purchasing habits or symptom clusters, which are useful for strategic planning and decision-making. Algorithms like Apriori [2, 3], FP-Growth [4], and ECLAT [5] have been widely applied in tasks like market basket analysis to uncover such patterns. This review summarizes major FPM techniques used in behaviour recognition, compares their computational characteristics, and highlights their practical strengths and weaknesses. A step-by-step example using the Apriori algorithm on a hypothetical dataset is included to illustrate its working principles.

2. The Knowledge Discovery Process

Knowledge Discovery in Databases (KDD) is a structured, multistage process that converts raw data into actionable insights. It includes the sequential steps of data selection, preprocessing, transformation, data mining, and interpretation. Each stage plays a vital role—selection targets relevant datasets, preprocessing handles noise and inconsistencies, transformation formats the data for analysis, mining extracts patterns, and interpretation evaluates these patterns for their real-world utility. These steps are especially critical when analyzing user behaviour, as clean, well-structured data is essential for detecting accurate patterns. Figure 1 illustrates the overall KDD pipeline.

*Corresponding Author: Sonam (sonamyadav2706@gmail.com)

Received: 18 Jan 2025; **Revised:** 25 Apr 2025; **Accepted:** 26 Apr 2025; **Published:** 30 Apr 2025

DOI: 10.57159/jcmm.4.2.25214.

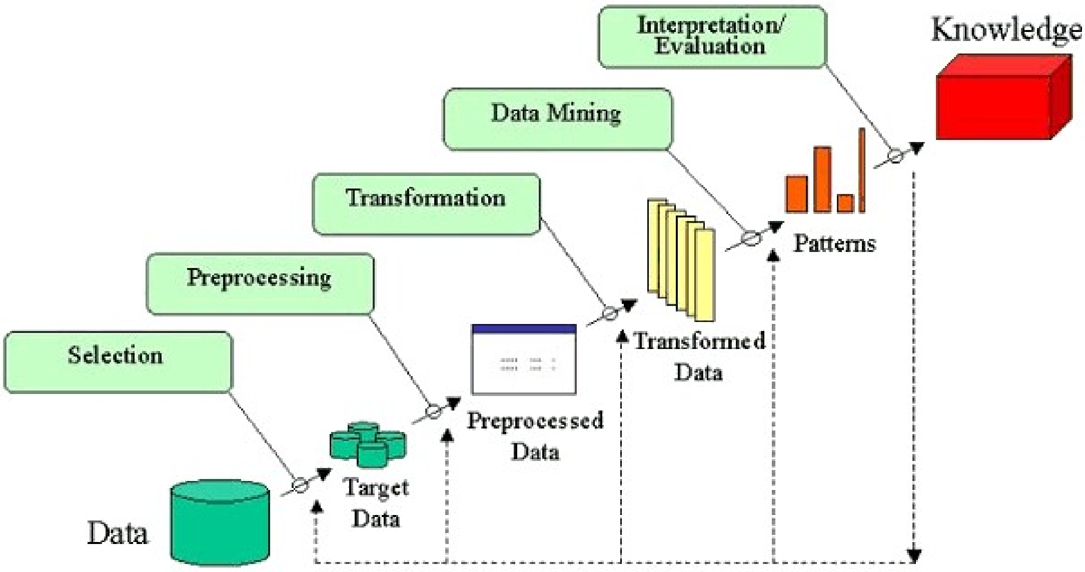

Figure 1: Stages of Knowledge Discovery in Databases (KDD), from data selection to knowledge interpretation [6].

3. Methodology

This study follows a narrative review framework supplemented with an illustrative example. It investigates frequent pattern mining (FPM) algorithms applied to user behaviour recognition, focusing on Apriori, FP-Growth, and ECLAT. A total of 13 academic sources were reviewed, including journal articles and conference proceedings published between 1993 and 2017. The literature was manually gathered from repositories such as IEEE Xplore, SpringerLink, and Google Scholar, prioritizing works that detailed algorithmic performance or application-specific evaluations. To demonstrate practical application, a step-by-step walkthrough of the Apriori algorithm is provided using a small hypothetical dataset. This example illustrates how frequent itemsets and association rules are generated using defined support and confidence thresholds. As a narrative review, this work does not follow a systematic review protocol or include formal quality appraisal. Instead, it aims to synthesize core themes and trends in algorithm design and application. The hypothetical dataset serves as an educational tool and does not reflect the complexity of real-world transactional data.

4. Frequent Pattern Mining Techniques

Frequent Pattern Mining (FPM) is a key technique in data mining for identifying recurring relationships among items in large datasets. One of its most widely known applications is market basket analysis, where analysts identify item combinations that frequently co-occur in purchase transactions [4, 2]. The goal is to discover itemsets that appear together in the dataset with a frequency above a specified threshold, known as support. Once these frequent itemsets are identified, association rules can be generated to describe conditional relationships, typically measured using metrics such as confidence and lift. Several algorithms have been developed to address the computational challenges of frequent itemset mining. The most prominent include:

- **Apriori Algorithm**: Introduced by Agrawal and Srikant in 1994, this foundational method uses a level-wise approach and the Apriori property to eliminate infrequent itemsets early in the process. It requires multiple database scans and is sensitive to high dimensionality [2, 3].
- **FP-Growth**: This algorithm avoids candidate generation by compressing the dataset into a prefix-tree structure called the FP-tree. It then recursively extracts frequent patterns from the tree, resulting in faster performance, particularly for large and sparse datasets [4].
- **ECLAT (Equivalence Class Clustering and bottom-up Lattice Traversal)**: Unlike the above horizontal-format methods, ECLAT uses a vertical data format and applies set intersection on transaction ID lists to compute support. It is often more efficient on dense datasets but can consume more memory [5].

The effectiveness of each algorithm depends on factors such as dataset size, itemset density, and dimensionality. Their relative performance and resource efficiency have been the focus of numerous comparative studies. In practice, frequent pattern mining is implemented within layered data mining systems that integrate user interfaces, data preprocessing modules, mining engines, and result visualization components. These systems structure the transition from raw data to actionable knowledge. Figure 2 illustrates the typical architecture of a data mining system.

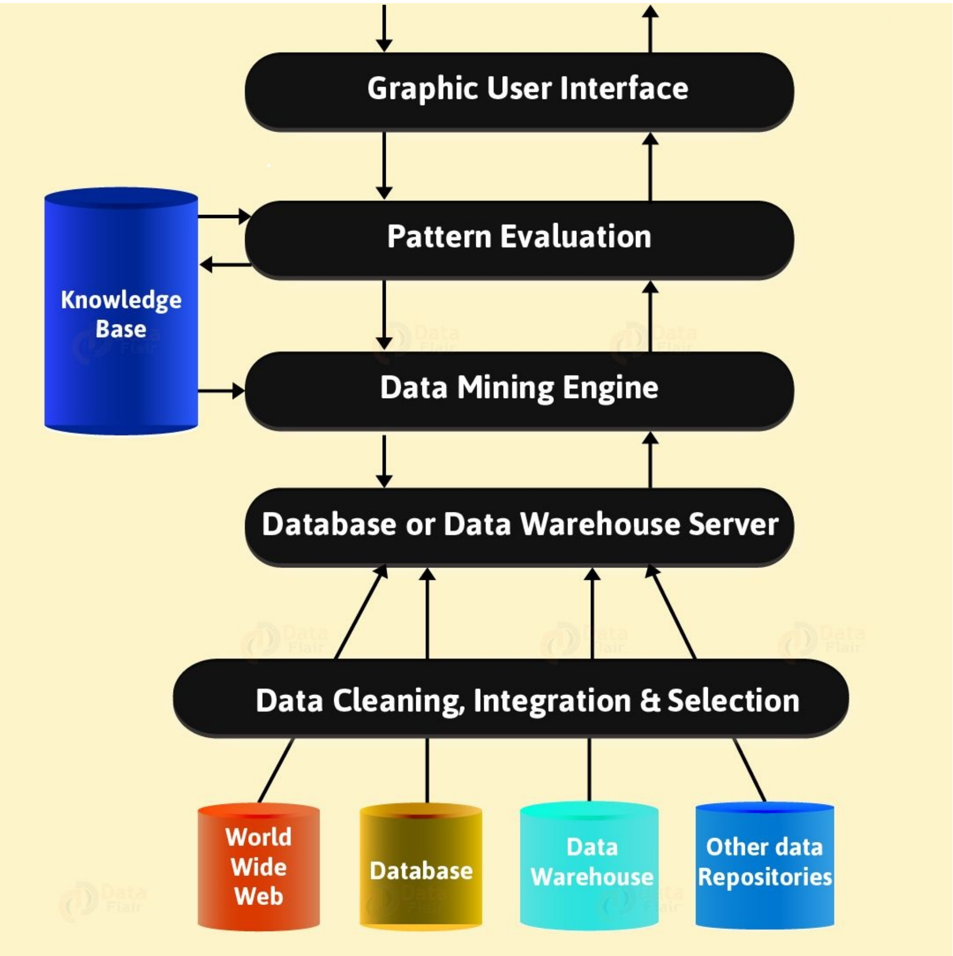

Figure 2: Typical data mining system architecture, showing the flow from user interface to data sources and pattern discovery [6].

FPM algorithms can also be categorized by their underlying computational strategies. Figure 3 shows this classification, which includes join-based methods like Apriori, tree-based methods like FP-Growth, and vertical intersection methods such as ECLAT. This taxonomy highlights key differences in how algorithms process and organize data.

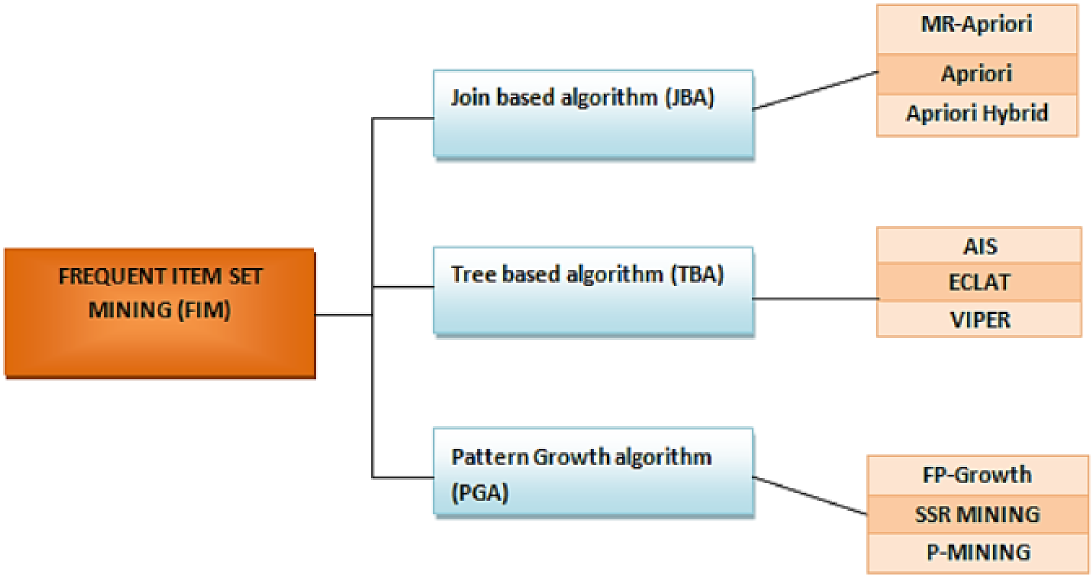
FREQUENT ITEM SET MINING (FIM)
Join based algorithm (JBA)
Tree based algorithm (TBA)
Pattern Growth algorithm (PGA)
MR-Apriori
Apriori
Apriori Hybrid
AIS
ECLAT
VIPER
FP-Growth
SSR MINING
P-MINING

Figure 3: Classification of frequent itemset mining algorithms based on their core strategy: join-based, tree-based, and vertical format methods.

5. Association Rule Mining Applications

Association Rule Mining (ARM) is a data mining technique used to uncover co-occurrence relationships between variables in large transactional datasets. It builds on frequent pattern mining by identifying if-then rules that describe how the presence of one set of items in a transaction implies the presence of another. ARM is widely applied in domains such as retail, healthcare, education, and cybersecurity [4, 7]. In retail, one of the most common applications is market basket analysis. For example, if many customers who purchase bread and milk also purchase eggs, the association rule `Bread, Milk` → `Eggs` can be generated. These patterns inform product placement, promotional bundling, and inventory management. In healthcare, ARM is used to detect associations between symptoms, diagnoses, or treatments. A rule might reveal that patients diagnosed with condition A often exhibit symptom B, aiding early diagnosis or treatment planning [7]. Similar applications are found in educational analytics, where patterns in student behavior or performance can guide interventions. ARM relies primarily on three metrics:

- **Support**: The proportion of transactions that contain a given itemset.
- **Confidence**: The conditional probability that a transaction containing one itemset also contains another.
- **Lift**: The ratio of observed support to that expected if the itemsets were independent. A lift greater than 1 indicates a positive association.

These metrics help evaluate the relevance and strength of discovered rules. Together, ARM techniques contribute not only to commercial recommendation systems but also to behaviour modeling, anomaly detection, and strategic decision support across diverse sectors.

6. Apriori Algorithm: Mechanism and Demonstration

The Apriori algorithm is one of the earliest and most widely used algorithms for mining frequent itemsets and association rules. It operates by iteratively identifying frequent itemsets of increasing length, using the principle that all non-empty subsets of a frequent itemset must also be frequent [2, 8]. Apriori employs a breadth-first search strategy. In each iteration, candidate itemsets are generated by joining frequent itemsets from the previous iteration. These candidates are then pruned based on a minimum support threshold. Once all frequent itemsets are identified, association rules are generated and evaluated using confidence thresholds. To demonstrate the algorithm's working, consider a hypothetical dataset of transactions:

Table 1: Sample Transactions

Transaction ID	Items
T100	1, 3, 4
T200	2, 3, 5
T300	1, 2, 3, 5
T400	2, 5

With a minimum support threshold of 50% and confidence threshold of 70%, the algorithm proceeds as follows:

- **Step 1: Count support for each item**. Items 1, 2, 3, and 5 meet the 50% support threshold.
- **Step 2: Generate candidate 2-itemsets**. Frequent pairs include {1,3}, {2,3}, {2,5}, and {3,5}.
- **Step 3: Generate candidate 3-itemsets**. Only {2,3,5} meets the support threshold.
- **Step 4: Generate association rules**. For example, the rule {2,3} → {5} is evaluated using confidence: Support({2,3,5}) / Support({2,3}) = 0.5 / 0.75 = 66.7%.

Table 2: Frequent Itemsets and Support

Itemset	Support
{2, 3, 5}	50%
{1, 3}, {2, 3}, {2, 5}, {3, 5}	50–75%

While effective and interpretable, Apriori has several known limitations:

- Requires multiple database scans, increasing computational cost.
- Generates large numbers of candidate itemsets.
- Performance degrades with dense or high-dimensional data.

These limitations have motivated the development of more efficient algorithms, which are discussed in the next section. The following table summarizes the key findings from 13 reviewed studies. Each entry includes the authors, research focus, algorithm used, main conclusions, and publication year. This table supports the frequency-based citation analysis and highlights recurring observations across various implementations.

Table 3: Summary of Reviewed Studies on Apriori and Its Variants

No.	**Author(s)**	**Algorithm**	**Conclusion**	**Year**
1	A. Imran and P. Ranjan [9]	Improved Apriori	Costly, but achieves high computation accuracy.	2017
2	A. Imran and P. Ranjan [9]	Apriori	Remains costly with large computation time.	2017
3	Nadeem Ur-Rahman [10]	Data Mining	Takes large execution time.	2017
4	S. Dhanya et al. [11]	MapReduce Apriori	Uses vertical/horizontal layout; slower execution.	2016
5	R. Karthiyayini and J. Jayaprakash [7]	Apriori	Identifies disease efficiently, but performance decreases with more symptoms.	2015
6	Rahul Shukla and A. K. Solanki [1]	Apriori	Costly and time-consuming.	2015
7	P. Prithiviraj and R. Porkodi [4]	Apriori + Others	Apriori takes more time and gives less accuracy.	2015
8	Paresh Tanna and Y. Ghodasara [3]	Apriori	Does not reduce number of scans; time-consuming.	2014
9	Jayshree Jha and Leena Ragha [2]	Improved Apriori	Applies only to educational data; reduces time but lowers performance.	2013
10	K. Geetha and S. K. Mohiddin [8]	Data Mining	High computational load.	2013
11	Z. Farzanyar and N. Cercone [5]	Data Mining (MapReduce)	Handles large data but slow; only extracts data.	2013
12	C. Kaur [12]	Apriori	Suggests online and single-scan variants for future.	2013

7. Challenges and Future Directions

While frequent pattern mining algorithms such as Apriori, FP-Growth, and ECLAT have proven useful in behavioural analysis and recommendation systems, they are not without limitations. Several challenges were consistently noted across the reviewed literature:

- **Scalability**: Algorithms like Apriori perform poorly on large or dense datasets due to repeated scans and exponential candidate growth.
- **Memory consumption**: Storing and evaluating large sets of candidate itemsets or trees (in FP-Growth) can exceed available memory, especially in real-time applications.
- **Runtime complexity**: High-dimensional data leads to longer processing times, making these algorithms less practical in environments with tight latency requirements.

To address these challenges, future work in the field is exploring several directions:

- **Hybrid algorithms**: Combining features of Apriori and FP-Growth, or integrating pruning techniques from different paradigms, can reduce overhead. Early research has shown hybrid approaches to improve speed and memory efficiency [4].

- **Parallel and distributed mining**: Frameworks like Hadoop and Spark have been used to improve runtime on large datasets by distributing workload across nodes [13, 9].
- **Memory-efficient data structures**: Advanced indexing techniques and vertical data layouts can reduce the algorithm's memory footprint, especially in MapReduce contexts [11].
- **Expanded mining scope**: Extending FPM to handle temporal, hierarchical, or streaming data can broaden its applicability in real-time analytics. This is a growing research direction aimed at making mining suitable for dynamic datasets.

Future studies should also aim to benchmark algorithms using real-world datasets and standardized performance metrics such as runtime, memory usage, precision, and scalability. This will help validate theoretical improvements and support more informed selection in practical deployments.

8. Conclusion

This article reviewed major data mining algorithms used in user behaviour recognition, with a focus on frequent pattern mining techniques such as Apriori, FP-Growth, and ECLAT. By analyzing their frequency of use in the literature and discussing their operational mechanisms, we highlighted both their strengths and limitations. A step-by-step demonstration of the Apriori algorithm on a hypothetical dataset illustrated how frequent itemsets and association rules are generated. Among the reviewed techniques, Apriori remains the most cited and widely taught, though it is increasingly challenged by more efficient alternatives in practical settings. The review identifies key performance trade-offs and recurring implementation issues such as runtime complexity and memory use. Future research should continue exploring hybrid models and distributed systems to enhance algorithmic efficiency, especially in large-scale, real-time data environments where existing methods struggle with scalability and resource constraints. Ultimately, the choice of algorithm should be guided by data characteristics, available computational resources, and the specific goals of the behaviour analysis task.

Declaration of Competing Interests

The authors declare no known competing financial interests or personal relationships.

Funding Declaration

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Author Contributions

Sonam: Investigation, Data Curation, Software, Visualization, Writing - Original Draft; **Jyoti**: Supervision, Conceptualization, Methodology, Writing - Review and Editing.

References

[1] R. Shukla and A. K. Solanki, "Performance analysis of frequent pattern mining algorithm using apriori on medical data," *International Research Journal of Computer Science (IRJCS)*, vol. 2, no. 10, 2015.

[2] J. Jha and L. Ragha, "Educational data mining using improved apriori algorithm," *International Journal of Information and Computation Technology*, vol. 3, no. 5, 2013.

[3] P. Tanna and Y. Ghodasara, "Using apriori with weka for frequent pattern mining," *International Journal of Engineering Trends and Technology (IJETT)*, vol. 12, no. 3, 2014.

[4] P. Prithiviraj and R. Porkodi, "A comparative analysis of association rule mining algorithms in data mining: A study," *American Journal of Computer Science and Engineering Survey*, vol. 3, no. 1, pp. 98–119, 2015.

[5] Z. Farzanyar and N. Cercone, "Efficient mining of frequent itemsets in social network data based on mapreduce framework," in *Proc. IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*, pp. 1183–1188, 2013.

[6] DataFlair, "Data mining architecture - components, types & working." `https://data-flair.training/blogs/data-mining-architecture/`, n.d.

[7] R. Karthiyayini and J. Jayaprakash, “Association technique on prediction of chronic diseases using apriori algorithm,” *International Journal of Innovative Research in Science, Engineering and Technology*, vol. 4, May 2015. Special Issue 6.

[8] K. Geetha and S. K. Mohiddin, “An efficient data mining technique for generating frequent itemsets,” *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 3, no. 4, pp. 571–575, 2013.

[9] A. Imran and P. Ranjan, “Improved apriori algorithm using power set on hadoop,” in *Proc. 1st International Conference on Computational Intelligence and Informatics*, (Hyderabad, India), pp. 245–254, 2017.

[10] N. Ur-Rahman, “Textual data mining for knowledge discovery and data classification: A comparative study,” *European Scientific Journal*, vol. 13, no. 21, 2017.

[11] M. Dhanya, M. Vysaakan, and A. Mahesh, “An enhancement of the mapreduce apriori algorithm using vertical data layout and set theory concept of intersection,” in *Intelligent Systems Technologies and Applications*, vol. 385, pp. 225–233, 2016.

[12] C. Kaur, “Association rule mining using apriori algorithm: A survey,” *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, vol. 2, no. 6, 2013.

[13] Y. Rochd and I. Hafidi, “An enhanced apriori algorithm using hybrid data layout based on hadoop for big data processing,” *International Journal of Computer Science and Network Security (IJCSNS)*, vol. 18, no. 6, 2018.

JCMM Journal of Computers, Mechanical and Management
Journal homepage: www.jcmm.co.in
e-ISSN: 3009-075X
AAN PUBLISHING

Volume 4 Issue 2
Article Number: 25196

Comparative Evaluation of AI Models for Automated Classification of Upper Respiratory Infections Using Chest X-ray Imaging

Pooja Tiwari, Abhishek Kumar*, and Ravi Kumar Burman

Department of Computer Science and Engineering, Jharkhand University of Technology, Ranchi, India

Abstract

Upper respiratory infections (URIs) are among the most prevalent global health concerns, yet their burden remains underrepresented in epidemiological data. This study investigates the prevalence and clinical significance of URIs and evaluates the diagnostic potential of artificial intelligence (AI) models for their automatic classification using chest X-ray images. A multiclass dataset comprising URTI, pneumonia, bronchiectasis, and bronchiolitis cases was curated and analyzed using four leading convolutional neural networks (CNNs): VGG16, VGG19, ResNet-50, and DenseNet. These models were assessed based on accuracy, precision, recall, F1-score, and computational efficiency. DenseNet achieved the highest diagnostic accuracy and parameter efficiency, making it well-suited for deployment in resource-constrained environments. ResNet-50 offered a favorable trade-off between speed and performance, supporting real-time clinical integration. The findings advocate for the application of AI-assisted diagnostic systems to enhance URI detection, especially in settings with limited healthcare infrastructure.

Keywords: Upper Respiratory Infections; Artificial Intelligence; Convolutional Neural Networks; DenseNet; ResNet-50

1. Introduction

Upper respiratory tract infections (URTIs) represent a significant public health concern, contributing substantially to global morbidity and mortality. A 2016 global burden assessment estimated that respiratory tract infections (RTIs) were responsible for approximately 2.4 million deaths and 336.5 million cases globally. In Asia, RTIs account for nearly 7 million annual visits to general practitioners, with individuals typically experiencing two to five episodes per year. The severity and outcomes of RTIs are influenced by the interplay of infectious agents, environmental factors, and host characteristics. These infections also exert a considerable economic burden through direct medical costs (e.g., hospitalizations, outpatient visits, and antibiotic use) and indirect costs, such as lost productivity [1]. Given the rapidly changing climatic and sociodemographic conditions, epidemiological monitoring of RTIs is critical for informing effective public health interventions. Accurate and timely diagnosis plays a pivotal role in guiding clinical management, optimizing antimicrobial therapy, and limiting the overuse of broad-spectrum antibiotics—thus helping to curb the spread of antimicrobial resistance [2]. Most upper RTIs are viral in origin and self-limiting. The common cold, characterized by nasal discharge, sneezing, congestion, and sore throat, is often caused by the respiratory syncytial virus, rhinovirus, adenovirus, influenza virus, parainfluenza virus, and coronaviruses. Acute laryngitis and pharyngitis are similarly viral in most cases, though bacterial agents such as *Corynebacterium diphtheriae*, *Haemophilus influenzae*, and *Branhamella catarrhalis* are occasionally implicated [2].

*Corresponding Author: Abhishek Kumar (abhishek28mca@gmail.com)

Received: 29 Jan 2025; **Revised:** 18 Feb 2025; **Accepted:** 27 Apr 2025; **Published:** 30 Apr 2025

DOI: 10.57159/jcmm.4.2.25196.

This study addresses the gap in comprehensive comparative analyses of artificial intelligence (AI) models for automated URI detection from medical imaging, especially in low-resource settings. Four CNN models were evaluated: VGG16, VGG19, ResNet-50, and DenseNet—benchmarking their performance in URI classification using a curated multi-class chest X-ray dataset. Metrics include accuracy, precision, recall, F1-score, and computational efficiency. Our findings identify DenseNet as the most accurate and resource-efficient model, while ResNet-50 offers an optimal balance between accuracy and speed for real-time deployment. These results support the potential of AI-driven tools to enhance URI diagnosis in diverse healthcare environments.

2. Literature Review

Artificial intelligence (AI) and deep learning have been widely adopted in recent years for the classification of respiratory conditions using chest radiographic images. Most studies rely on public datasets such as NIH ChestX-ray14, CheXpert, and Kaggle pneumonia collections [3–5]. These datasets are typically preprocessed using image resizing, normalization with ImageNet mean values, and contrast enhancement techniques. Augmentation techniques—such as flipping, rotation, and cropping—are commonly used to mitigate class imbalance and improve generalization [6, 7]. Some researchers also employ synthetic oversampling methods like SMOTE to address minority class issues [8]. Model selection is largely driven by the trade-off between accuracy and computational feasibility. VGG16 and VGG19 offer stable performance but are parameter-heavy (138M–144M), which limits their deployment in real-time or mobile contexts [9, 10]. ResNet-50 addresses training stability through residual connections and offers a good compromise between accuracy and efficiency [11]. DenseNet's layer-wise connectivity enables high accuracy with fewer parameters, making it more practical for resource-constrained environments [8]. Transfer learning remains a core training strategy, with pretrained ImageNet models being fine-tuned on domain-specific data [10]. Cross-validation is standard for robustness, and ensemble methods are used to further boost prediction stability and reduce variance [12]. Evaluation metrics typically include accuracy, precision, recall, F1-score, and AUC, with attention increasingly given to class-specific metrics for conditions like bronchiectasis and URTI [5, 7]. Interpretability tools such as Grad-CAM and LIME are often integrated into model pipelines to provide visual explanations of prediction rationale, increasing clinical trust [13, 14]. Newer transformer-based models like Vision Transformers (ViT) show promise in outperforming traditional CNNs by capturing long-range dependencies, although they require greater computational resources [15]. Overall, while current research validates the effectiveness of deep learning for respiratory diagnostics, methodological gaps persist—especially concerning clinical validation, real-world deployment, and generalizability across populations. The present study addresses these issues by systematically comparing four CNN architectures under a unified experimental setup to evaluate their performance, interpretability, and deployment feasibility in low-resource settings.

3. Methodology

This study adopts an experimental design to evaluate the performance of convolutional neural networks (CNNs) for automated classification of upper respiratory tract infections (URTIs) using chest X-ray images. Four widely used CNN architectures—VGG16, VGG19, ResNet-50, and DenseNet-169—were compared based on classification accuracy, parameter efficiency, and computational performance. A dataset of 6,542 chest X-ray images was compiled from open-access sources such as Kaggle and NIH ChestX-ray14, supplemented by clinical contributions. The images were categorized into four diagnostic classes: Normal (2,150), Pneumonia (2,800), URTI (1,200), and Bronchiectasis (392). The bronchiectasis class was significantly underrepresented, creating a class imbalance that could bias model performance. To address this, augmentation techniques were applied as detailed in Table 1.

Table 1: Augmentation Strategies per Class

Class	**Original**	**Augmentation Method**	**Final Count**	**Purpose**
Bronchiectasis	392	SMOTE + Geometric transforms	1,176	Addressed class imbalance via synthetic samples.
URTI	1,200	Flip, ±20° rotation	2,400	Maintained feature integrity while doubling data.
Pneumonia	2,800	Brightness adjustment	2,800	Increased contrast diversity without duplication.
Normal	2,150	None	2,150	Prevented overfitting from dominant class.

All images were resized to 224×224 pixels and normalized using the standard ImageNet mean and standard deviation. Preprocessing included noise reduction using Gaussian and median filters, contrast enhancement to emphasize structural differences, and multiple forms of augmentation: random cropping, rotation, flipping, intensity variation, and translation. These steps improved the dataset's diversity and helped reduce overfitting during training. Model selection focused on architectures that are well-established in medical imaging: VGG16 and VGG19 for their simple deep-layered design; ResNet-50 for its residual connections that stabilize gradient flow in deep networks; and DenseNet-169 for its dense connectivity, which promotes efficient gradient propagation and reduces parameter count. All models were initialized with pretrained ImageNet weights and fine-tuned for the multi-class classification task. Experiments were conducted using Google Colab with an NVIDIA Tesla P100 GPU. A batch size of 16 was used to balance memory constraints and convergence stability. Models were trained for 50 epochs using the Adam optimizer and a learning rate of 1×10^{-4}. To ensure generalizability across all classes, stratified 5-fold cross-validation was applied throughout. Model performance was evaluated using accuracy, precision, recall, F1-score, and area under the receiver operating characteristic curve (AUC). Emphasis was placed on per-class F1-scores—especially for URTI and bronchiectasis—to verify the effectiveness of augmentation. Computational efficiency was also assessed based on inference time, number of parameters, and training duration. This methodology ensures reproducibility, fair model comparison, and relevance for clinical applications, especially in low-resource settings where computational overhead is a key constraint.

4. Results and Discussion

The evaluation of VGG16, VGG19, ResNet-50, and DenseNet was conducted using a consistent training setup and validated through stratified 5-fold cross-validation. Model performance was assessed based on accuracy, precision, recall, F1-score, and computational efficiency. Among the evaluated architectures, DenseNet demonstrated superior performance, achieving a classification accuracy of 99.8% and an F1-score of 0.998, while maintaining a compact architecture with only 20 million parameters. It exhibited consistent and balanced performance across all classes, including underrepresented categories. ResNet-50 followed closely, offering a favorable trade-off between accuracy (96%) and inference speed, rendering it suitable for real-time clinical applications. In contrast, VGG16 and VGG19 delivered moderately high classification accuracies (approximately 90–93%) but were significantly less efficient in terms of computational demand. As shown in Figure 1, the comparative analysis of these two models highlights their high parameter counts and prolonged training durations. Despite their classification capability, their excessive resource requirements limit their practical deployment in constrained environments.

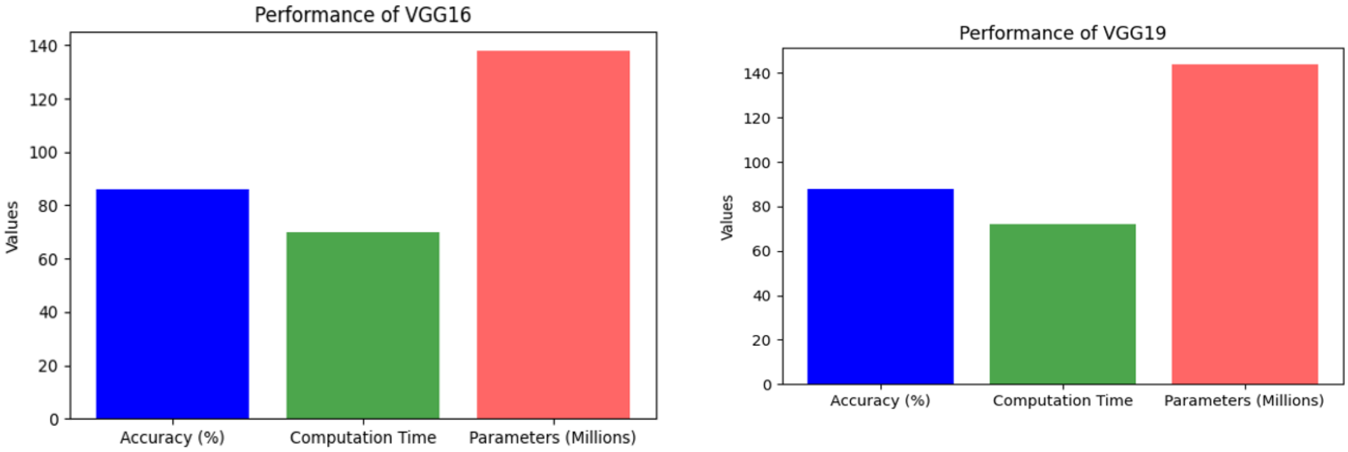

Figure 1: Comparison of VGG architectures: (a) VGG16 and (b) VGG19.

As shown in Figure 2, the ResNet-50 balanced model depth with reasonable computational load outperforms the VGG models in both efficiency and class-wise generalization. DenseNet, visualized in Figure 3, provided the best trade-off across all evaluation dimensions, particularly excelling in low-resource feasibility due to its compact parameter footprint and high performance. A consolidated comparison of all models is presented in Figure 4, showing trends in accuracy, computation time, and model size. DenseNet maintained high accuracy while being six to seven times more efficient in parameter usage compared to VGG models. ResNet-50 was the fastest during inference, but with slightly reduced accuracy on minority classes.

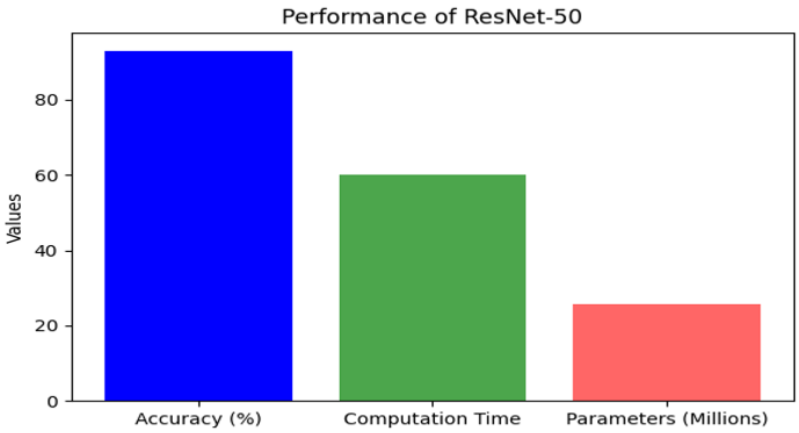

Figure 2: Performance of ResNet-50: Optimized for real-time applications.

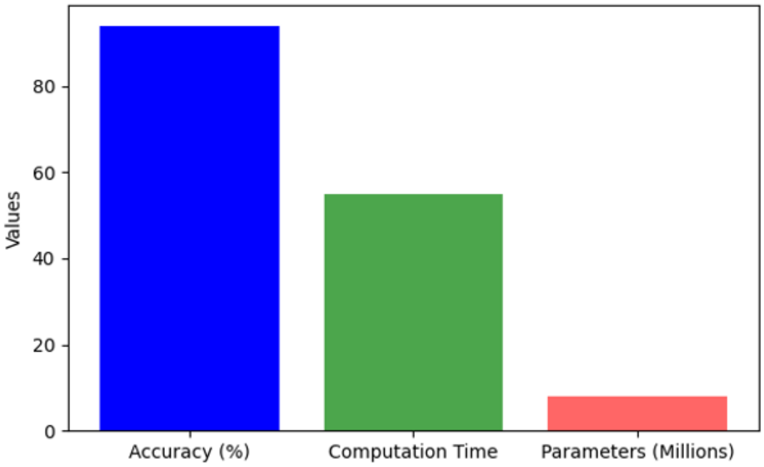

Figure 3: Performance of DenseNet: Highest efficiency with lowest parameter count.

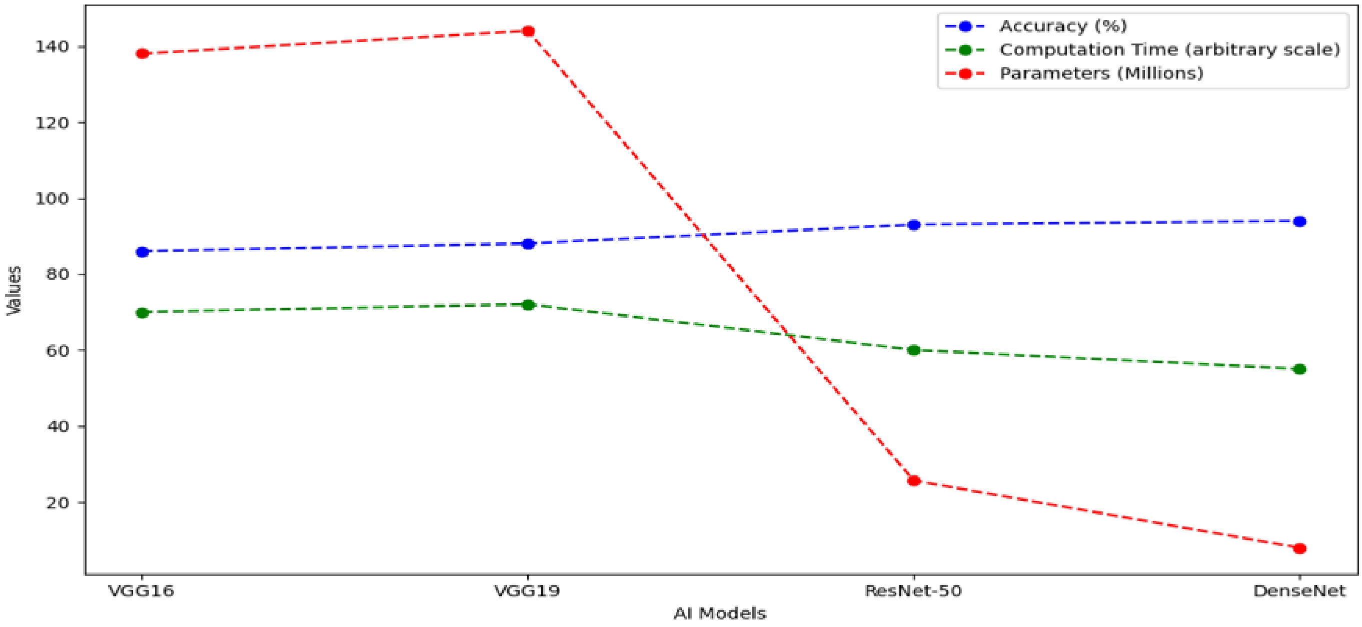

Figure 4: Comparative performance of CNN models in terms of accuracy, computation time, and parameter count.

Data augmentation had a measurable impact on minority class performance. The bronchiectasis class F1-score increased from 0.48 to 0.72 after applying SMOTE and geometric transformations. URTI recall improved by 18% due to the inclusion of rotation-based augmentation. DenseNet demonstrated greater resilience to class imbalance, maintaining over 91% accuracy across all four categories, while VGG19 showed a 7.4% drop in rare-class accuracy. In terms of clinical integration, DenseNet's sensitivity (99.8%) and parameter efficiency make it ideal for mobile diagnostic tools and telemedicine platforms. ResNet-50's shorter inference times position it well for real-time decision support systems. VGG-based models, although effective in classification, are best suited for offline analysis or feature extraction in well-equipped environments due to their size and resource needs. In summary, DenseNet is the most resource-efficient and accurate model for URTI classification, with strong potential for real-world implementation in constrained healthcare settings. ResNet-50 is also practical for deployment in latency-sensitive clinical environments, while VGG models offer baseline reliability for infrastructure-rich facilities.

5. Conclusion

This study was undertaken to compare and evaluate different deep learning models for the classification of upper respiratory tract infections using chest X-ray images. Four CNN architectures—VGG16, VGG19, ResNet-50, and DenseNet—were selected based on past literature and their reported success in medical image analysis. Among the models tested, DenseNet showed the highest accuracy and required fewer parameters, which makes it better suited for areas where computing resources are limited. ResNet-50 also performed well and can be used in real-time applications due to its faster processing. The VGG models, although accurate, had higher computational costs and longer training times. Efforts were also made to handle class imbalance in the dataset. Data augmentation and SMOTE helped in improving the detection of underrepresented classes like bronchiectasis. These steps ensured that the models do not become biased toward the majority classes and perform well across all categories. The work can be extended in several directions. First, there is a need to test these models in actual clinical settings to confirm their usefulness. Second, combining image data with patient information such as medical history and symptoms may improve prediction. Third, simplified versions of these models can be developed so that they can be used on mobile or edge devices in rural or low-resource areas. Lastly, it is important to consider the ethical aspects, such as data privacy and explainability of the model outputs. Training of medical staff on how to use AI tools in a proper way will also help in their smooth integration into hospital systems. In summary, this research has shown that DenseNet is a good choice for URTI classification when both accuracy and resource efficiency are required. ResNet-50 may be used where a fast response is needed. Further studies and real-world trials will be necessary to confirm these results and to make these systems usable in everyday healthcare practice.

Declaration of Competing Interests

The authors declare no known competing financial interests or personal relationships.

Funding Declaration

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Author Contributions

Pooja Tiwari: Conceptualization, Data Analysis, Writing - Review and Editing; **Abhishek Kumar**: Methodology, Validation, Investigation, Writing - Original Draft; **Ravi Kumar Burman**: Software, Visualization, Investigation.

References

[1] A. K. Grech, C. T. Foo, E. Paul, A. K. Aung, and C. Yu, "Epidemiological trends of respiratory tract pathogens detected via mpcr in australian adult patients before covid-19," *BMC Infectious Diseases*, vol. 24, no. 1, p. 38, 2024.

[2] A. Calderaro, M. Buttrini, B. Farina, S. Montecchini, F. De Conto, and C. Chezzi, "Respiratory tract infections and laboratory diagnostic methods: A review with a focus on syndromic panel-based assays," *Microorganisms*, vol. 10, no. 9, p. 1856, 2022.

[3] J. Becker *et al.*, "Artificial intelligence-based detection of pneumonia in chest radiographs," *Diagnostics*, vol. 12, no. 6, p. 1465, 2022.

[4] A. B. Godbin and S. G. Jasmine, "Analysis of pneumonia detection systems using deep learning-based approach," in *Proceedings of the 2022 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES)*, pp. 1–6, 2022.

[5] G. M. M. Alshmrani, Q. Ni, R. Jiang, H. Pervaiz, and N. M. Elshennawy, "A deep learning architecture for multi-class lung diseases classification using chest x-ray (cxr) images," *Alexandria Engineering Journal*, vol. 64, pp. 923–935, 2023.

[6] A. M. Alqudah, S. Qazan, and Y. M. Obeidat, "Deep learning models for detecting respiratory pathologies from raw lung auscultation sounds," *Soft Computing*, vol. 26, no. 24, pp. 13405–13429, 2022.

[7] S. Panigrahi, B. S. Nanda, R. Bhuyan, K. Kumar, S. Ghosh, and T. Swarnkar, "Classifying histopathological images of oral squamous cell carcinoma using deep transfer learning," *Heliyon*, vol. 9, no. 3, p. e13444, 2023.

[8] S. G. Gundabatini, M. R. N. D. LakshmiRoshini, M. N. Sri, P. Deepthi, and P. S. Teja, "Pneumonia detection using cnn, resnet, and densenet," *International Journal for Research in Applied Science and Engineering Technology (IJRASET)*, vol. 9, no. 6, pp. 2321–9653, 2021.

[9] B. Ilhan, K. Lin, P. Guneri, and P. Wilder-Smith, "Improving oral cancer outcomes with imaging and artificial intelligence," *Journal of Dental Research*, vol. 99, no. 3, pp. 241–248, 2020.

[10] M. Bansal, M. Kumar, M. Sachdeva, and A. Mittal, "Transfer learning for image classification using vgg19: Caltech-101 image data set," *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, no. 4, pp. 3609–3620, 2023.

[11] I. Amin, H. Zamir, and F. F. Khan, "Histopathological image analysis for oral squamous cell carcinoma classification using concatenated deep learning models," *medRxiv*, 2021.

[12] A. A. Akl, K. M. Hosny, M. M. Fouda, and A. Salah, "A hybrid cnn and ensemble model for covid-19 lung infection detection on chest ct scans," *PLOS ONE*, vol. 18, no. 3, p. e0282608, 2023.

[13] T. T. Ifty, S. A. Shafin, S. M. Shahriar, and T. Towhid, "Explainable lung disease classification from chest x-ray images utilizing deep learning and xai," in *Proceedings of the 2024 International Conference on Multimedia Interaction (ICMI)*, pp. 1–5, 2024.

[14] K. Subramaniam *et al.*, "A comprehensive review of analyzing the chest x-ray images to detect covid-19 infections using deep learning techniques," *Soft Computing*, vol. 27, no. 19, pp. 1–15, 2023.

[15] S. Singh, M. Kumar, A. Kumar, B. K. Verma, K. Abhishek, and S. Selvarajan, "Efficient pneumonia detection using vision transformers on chest x-rays," *Scientific Reports*, vol. 14, no. 1, p. 2487, 2024.

JCMM Journal of Computers, Mechanical and Management
Journal homepage: www.jcmm.co.in e-ISSN: 3009-075X
AAN PUBLISHING

Volume 4 Issue 2

Article Number: 25194

Advances in Mechanical Joining Techniques for Metal–Composite Hybrid Structures—A Mini Review

Suresh Tiwari*

Department of Mechanical Engineering, Government Polytechnic, Jamshedpur, Jharkhand, India 831013

Abstract

The integration of fiber-reinforced polymer (FRP) composites with metal components in aerospace and automotive structures presents significant mechanical and design challenges, especially when conventional bolted joints induce fiber disruption and delamination. This mini review provides a comprehensive evaluation of emerging mechanical joining techniques developed to address these limitations. Key approaches discussed include self-piercing and friction riveting, mechanical clinching, non-adhesive form-locked joints, pin and loop joining, and recent advances enabled by additive manufacturing technologies. Each technique is examined in terms of joining mechanism, material compatibility, process constraints, and structural performance. Additionally, the role of nanofiber reinforcement in enhancing the interlaminar toughness of composite laminates is explored, emphasizing its effect on joint durability and resistance to failure. Comparative insights are offered on joint reversibility, complexity, galvanic behavior, and suitability for thermoplastic and thermoset matrices. Despite notable progress, most advanced joining strategies still face practical hurdles related to manufacturability, scalability, and long-term environmental durability. The review highlights that minimizing fiber damage often entails increased process complexity and cost. Therefore, future directions should focus on developing standardized evaluation protocols, optimizing additive manufacturing for multi-material interfaces, and integrating nanoscale reinforcements to achieve structurally robust, lightweight, and corrosion-resistant hybrid assemblies. This synthesis serves as a technical guide for engineers and researchers aiming to design next-generation composite–metal joints for high-performance applications.

Keywords: Composite–metal Joints; Additive Manufacturing; Fiber Reinforcement; Mechanical Joining; Hybrid Structures

1. Introduction

The integration of fiber-reinforced polymer (FRP) composites with metallic components is increasingly critical in aerospace and automotive industries due to the need for lightweight, high-performance hybrid structures. However, the conventional application of bolted joints in composite assemblies introduces several disadvantages, such as fiber disruption, delamination, and elevated stress concentrations [1–3]. These issues undermine structural integrity and reduce fatigue life. In response to these challenges, alternative mechanical joining techniques have been developed to improve compatibility with composite architectures and to optimize joint performance. Prominent among these techniques are self-piercing riveting (SPR), friction riveting (FR), mechanical clinching, pin-and-loop joining, and adhesive-free form-locked joints [4–6]. These methods aim to enhance joint strength, minimize material degradation, and streamline assembly operations. While certain techniques, such as SPR and clinching, have achieved commercial viability in automotive applications, others—such as pin-and-loop joining—remain under experimental investigation.

[*] **Corresponding Author:** Suresh Tiwari (suresh.mech.2k@gmail.com)

Received: 24 Mar 2025; **Revised:** 22 Apr 2025; **Accepted:** 29 Apr 2025; **Published:** 30 Apr 2025

DOI: 10.57159/jcmm.4.2.25194.

These joining approaches differ in terms of reversibility, manufacturing feasibility, added weight, and their applicability to thermoset or thermoplastic matrix systems [7, 8]. This mini-review presents a synthesis of current mechanical joining strategies for FRP-metal interfaces. The review outlines their underlying principles, benefits, limitations, and key experimental findings. The objective is to inform materials engineers and structural designers in selecting suitable joining techniques based on specific performance requirements, damage tolerance, and manufacturing constraints.

2. Riveted Joints

Riveted joints are among the most established mechanical fastening methods and continue to be widely used in structural applications within the aerospace and automotive industries. However, the implementation of traditional riveting in fiber-reinforced polymer (FRP) composites presents significant challenges. The process typically requires hole drilling, which may induce matrix cracking, fiber breakage, and delamination, thereby compromising the mechanical integrity of the composite assembly [1–3]. To mitigate these issues, advanced variants such as self-piercing riveting (SPR) and friction riveting (FR) have been introduced. These methods are engineered to minimize or eliminate the need for pre-drilled holes, thereby reducing stress concentrations and material damage. Additionally, SPR and FR have demonstrated improved joint reliability and mechanical performance in hybrid FRP-metal structures [7, 4].

2.1. Self-Piercing Riveting (SPR)

Self-piercing riveting (SPR) is a mechanical fastening technique that facilitates the joining of two or more sheets of similar or dissimilar materials without the need for pre-drilled holes. In this process, a semi-tubular rivet is driven into the material stack, penetrating the upper layers and flaring within the bottom layer to form a mechanical interlock. The SPR technique eliminates pre-drilled holes by plastically deforming the rivet into a mechanical interlock with the bottom layer, as illustrated in Fig. 1.

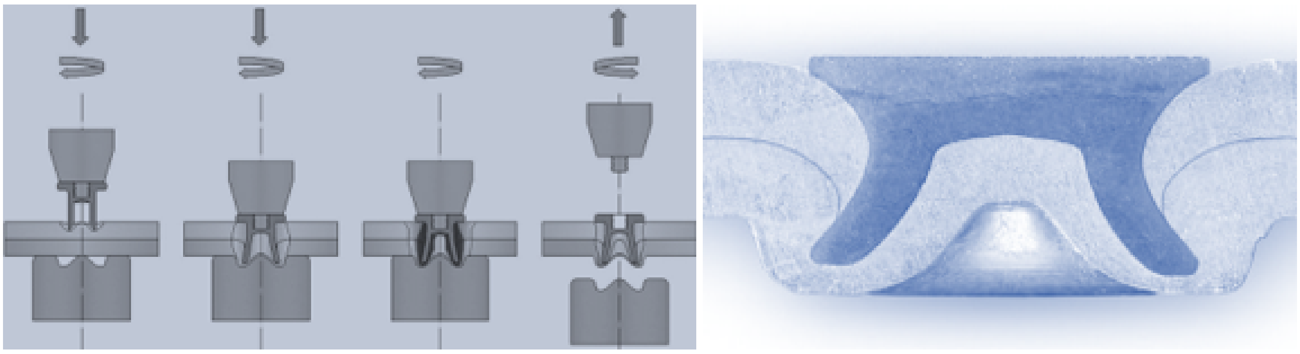

Figure 1: Self-Piercing Riveting (SPR): Schematic of the joining process and a cross-sectional view of a dissimilar material joint.

This method is particularly beneficial for hybrid joints involving fiber-reinforced polymers (FRPs) and metals, as it eliminates the need for drilling and thereby preserves the structural integrity of the composite material [9, 4]. SPR has been extensively adopted in the automotive sector and is increasingly being applied in aerospace and other high-performance fields. Displacement of composite plies without visible delamination in FRP-metal assemblies has been reported, suggesting a favorable stress distribution mechanism. Strong mechanical joints between polyamide-based composites and aluminum substrates have also been demonstrated, supporting the suitability of SPR for thermoplastic matrix composites [10]. The geometric design of the rivet and die significantly influences joint quality. Parameters such as rivet diameter, head geometry, and die cavity profile have been shown to affect the mechanical interlock and load-bearing capacity [11]. Fatigue testing of SPR joints indicates improved durability with optimized rivet head configurations [12]. A detailed cross-sectional analysis of SPR in CFRP laminates reveals the rivet flare geometry, residual thickness (t_{min}), and key load-bearing features (Fig. 2). Hybrid joints combining SPR with adhesives have exhibited enhanced shear strength and energy absorption [13]. Despite its advantages, SPR has certain limitations. The joints are generally irreversible, and galvanic corrosion may occur when dissimilar materials are joined. Furthermore, under cyclic loading or in aggressive environments, minor delamination or micro-cracking may still develop, potentially affecting long-term durability.

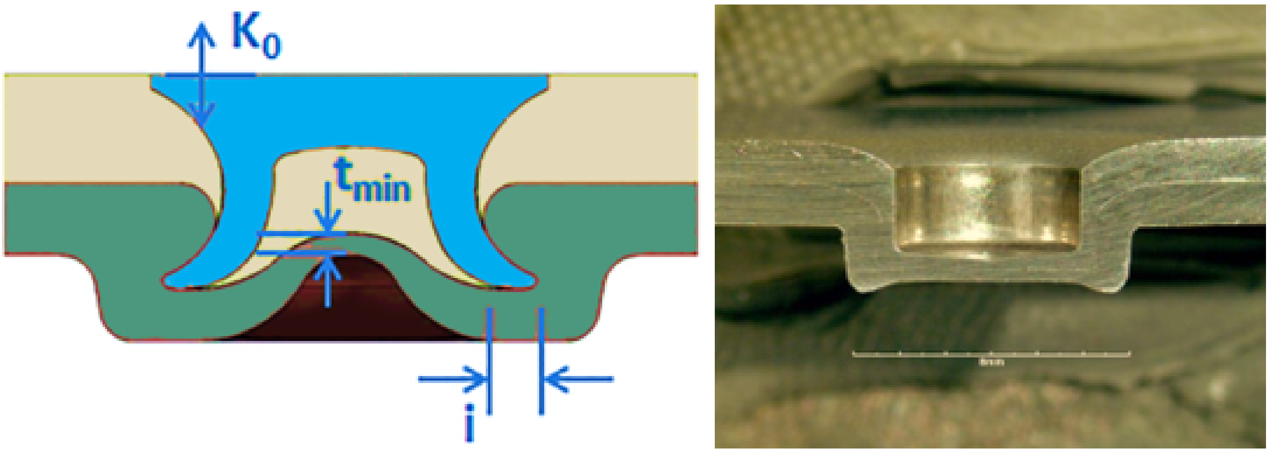

Figure 2: Cross-sectional insight into Self-Piercing Riveting (SPR) joining of Carbon Fiber Reinforced Plastic (CFRP) laminate: Photographic and schematic representation showing residual thickness (t_{min}) and stress directions.

2.2. Friction Riveting (FR)

Friction riveting (FR) is a thermomechanical joining technique primarily designed for thermoplastic composites, wherein a rotating metallic rivet is inserted into a polymeric base, generating heat through friction. This heat softens the polymer, allowing the rivet to plastically deform and anchor into the matrix, thereby forming a mechanical interlock. The process eliminates the need for pre-drilled holes, adhesives, or additional fasteners [7]. FR is particularly effective for joining thermoplastic matrix composites to metallic substrates. Experimental studies have shown that higher rotational speeds enhance pull-out strength, while controlled temperatures help minimize thermal degradation [14]. Strong and stable joints have been achieved between glass fiber-reinforced polyester composites and metallic rivets, demonstrating high mechanical performance with limited thermal impact [15]. An evolution of this technique, known as Friction Stir Blind Riveting (FSBR), has been applied to carbon fiber-reinforced plastic (CFRP) and aluminum alloy (AA6111) joints, confirming robust interfacial bonding and effective load transfer in brittle laminates [16]. Further research has indicated that threaded titanium rivets can achieve joint strengths up to 199 MPa in glass fiber laminates, surpassing those of conventional bolted joints. In short carbon fiber-reinforced polyether ether ketone (PEEK), pull-out strengths of 10.7 kN have been reported, with deformation modes such as rivet mushrooming—observed at approximately 70% deformation—indicating efficient energy absorption [15]. Despite its advantages, FR is inherently irreversible and limited to thermoplastic systems. Precise thermal control is essential to prevent degradation of the polymer, especially at elevated speeds or during prolonged friction cycles. Nonetheless, due to its efficiency, mechanical reliability, and compatibility with automated processes, FR presents a promising solution for advanced composite-metal joining applications.

3. Mechanical Clinching

Clinching is a mechanical fastening process that joins sheet materials through localized plastic deformation, forming a mechanical interlock without the need for auxiliary elements such as rivets or adhesives. Originally developed for ductile metals, this technique has been adapted for joining fiber-reinforced polymer (FRP) composites to metals through the use of modified tool geometries and thermal assistance [5, 8]. In hybrid structures, the more malleable metal sheet is typically placed on the punch side, enabling it to deform into the composite layer, which may require localized softening to avoid brittle fracture and delamination. Thermal assistance, including thermo-clinching and induction heating, is often employed for this purpose. Although the process is irreversible, it is rapid, cost-effective, and well-suited for lightweight structural applications, particularly with thermoplastic matrix composites [17]. Investigations into the influence of tool geometry and composite thickness have shown that parameters such as punch diameter, corner radius, and die depth significantly affect joint integrity and strength. Various die configurations—including round grooved, split, and flat dies—have been found to influence material flow and mechanical entrapment behavior [18].Different clinching die geometries—such as round split, grooved, flat, and rectangular shear—are shown in Fig. 3, each contributing uniquely to material flow and joint strength.

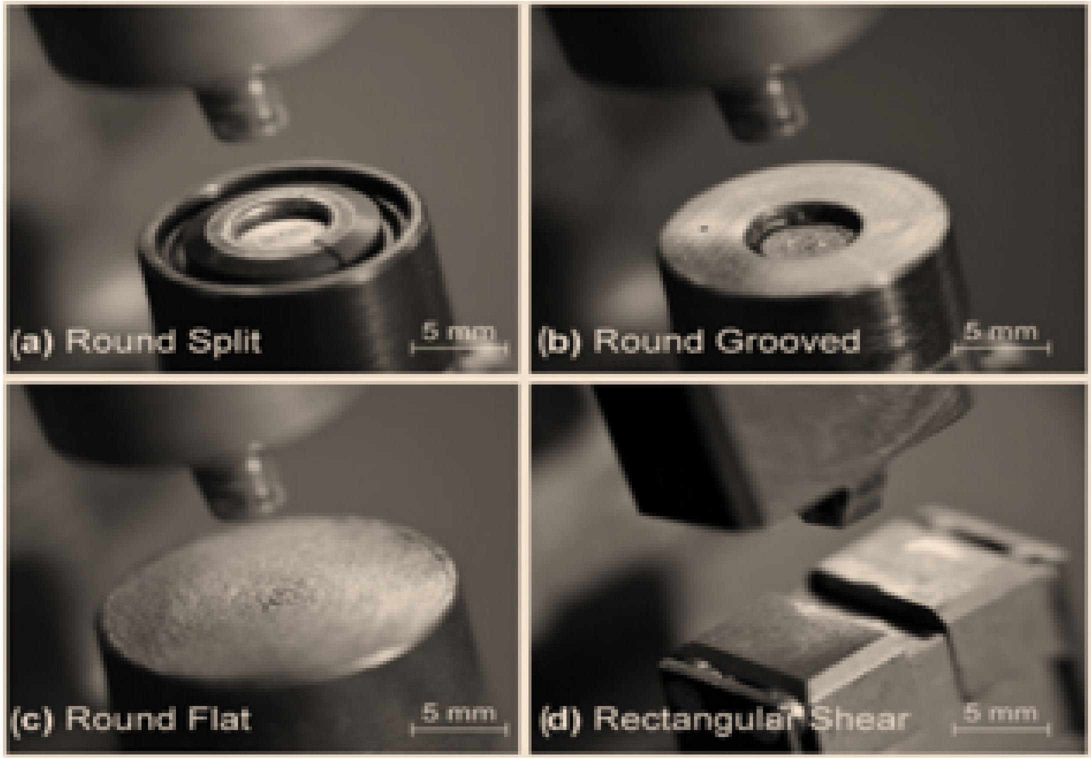

Figure 3: Clinching dies: (a) round split; (b) round grooved; (c) round flat; and (d) rectangular shear.

A variation known as Injection Clinching Joining (ICJ) involves softening a polymeric stud and pressing it into a pre-formed hole, creating a form-locked joint upon cooling. This method has demonstrated enhanced load-bearing capacity while limiting material degradation [19]. The evolution of the ICJ process is illustrated in Fig. 4, showing thermal softening and subsequent mechanical interlock formation in a time-sequenced manner. Another development, friction-assisted clinching, has reduced the joining force required but occasionally led to pull-out failures under tensile loads. Hybrid approaches that integrate clinching with friction stir welding have also been explored. Typical failure modes in friction stir welded hybrid joints include shearing of surface protrusions and interfacial separation between sheets, as shown in Fig. 5. These combinations improve interfacial bonding and reduce residual stresses in joints between aluminum sheets and self-reinforced polypropylene [17]. Nonetheless, issues such as delamination, fiber misalignment, and limited applicability to thermoset composites continue to hinder broader adoption of clinching in FRP-metal hybrid structures.

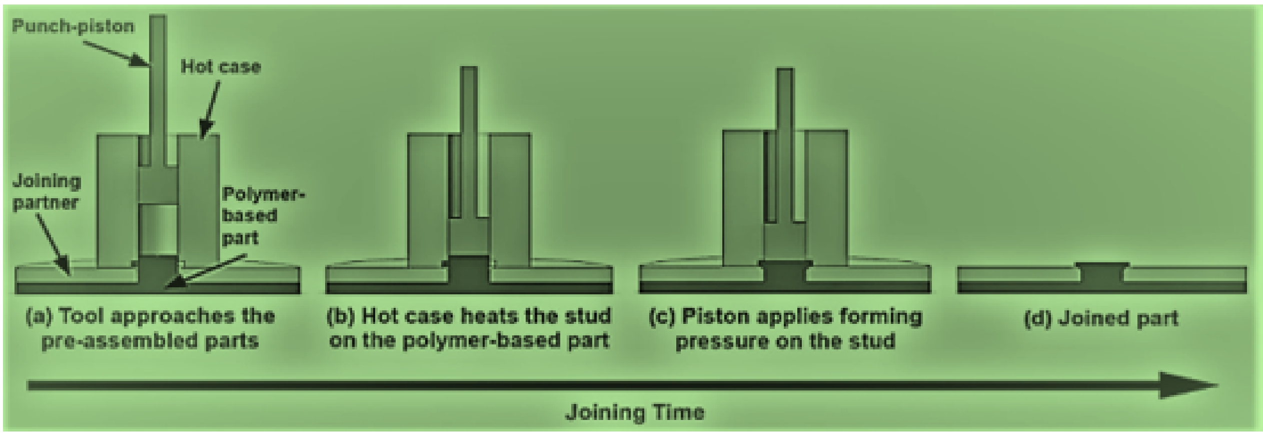
Punch-piston
Hot case
Joining partner
Polymer-based part
(a) Tool approaches the pre-assembled parts
(b) Hot case heats the stud on the polymer-based part
(c) Piston applies forming pressure on the stud
(d) Joined part
Joining Time

Figure 4: Stepwise evolution of the Induction Clinching Joining (ICJ) process: (a) tool approach to pre-assembled parts, (b) hot case heating the stud on polymer-based part, (c) piston applying forming pressure on the stud, and (d) joined part.

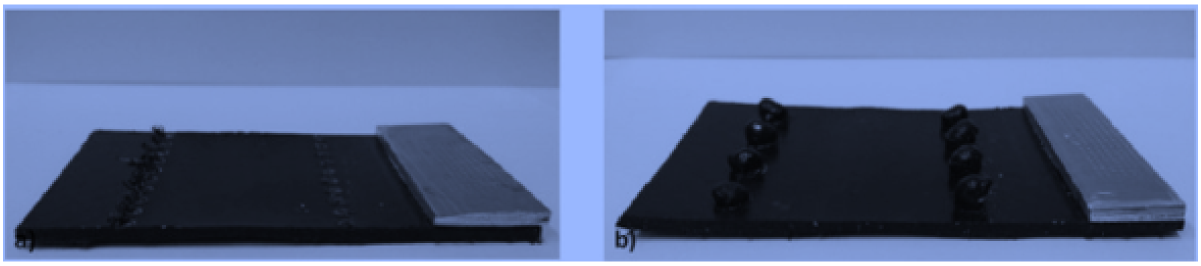

Figure 5: Unraveling failure modes in friction stir welded specimens: (a) shearing of protrusions, (b) sheets separation.

4. Non-Adhesive Form-Locked Joints

Traditional bolted joints in composite structures often induce detrimental effects such as fiber pull-out, matrix cracking, and delamination, particularly during the drilling process. To overcome these limitations, a novel non-adhesive form-locked joint configuration has been developed, utilizing metallic inserts to create a mechanical interlock with the composite laminate without the use of adhesives or bolts [5]. This design enhances joint strength while minimizing structural damage. The method has been successfully employed in the construction of composite gliders and motogliders, including models such as the PW-5, PW-6, and AOS-71. The process involves embedding a metal ring into a pre-formed hole within the composite laminate, thereby distributing mechanical loads across a broader area and reducing stress concentrations [20]. Experimental investigations have reported tensile static strengths ranging from 60 to 70 kN. Post-failure analyses using computed tomography scans revealed matrix cracking and localized delamination as primary failure mechanisms, confirming the technique's effectiveness in controlling stress distribution and resisting mechanical degradation. Despite these advantages, the incorporation of metallic rings introduces added complexity and weight. Moreover, the combination of dissimilar materials poses potential issues related to galvanic corrosion [9]. Nevertheless, non-adhesive form-locked joints represent a promising solution for aerospace and automotive applications that demand robust and damage-tolerant composite-metal connections. Their ability to preserve laminate integrity while delivering high load-bearing capacity underscores their value in the advancement of hybrid joining technologies.

5. Pin Joining

Pin joining involves embedding metallic pins, protruding from a metal adherend, into fiber-reinforced polymer (FRP) composites to establish a three-dimensional mechanical interlock between dissimilar materials. These pins, typically manufactured using Selective Laser Melting (SLM) or Powder Bed Fusion (PBF), are positioned prior to composite curing. During the fabrication process, reinforcing fibers are molded around the pins, producing robust through-thickness reinforcement [21, 22]. Figure 6 illustrates the comparative geometries of cylinder and ball-head pins used in composite-metal joints, highlighting their influence on mechanical anchoring and interfacial strength.

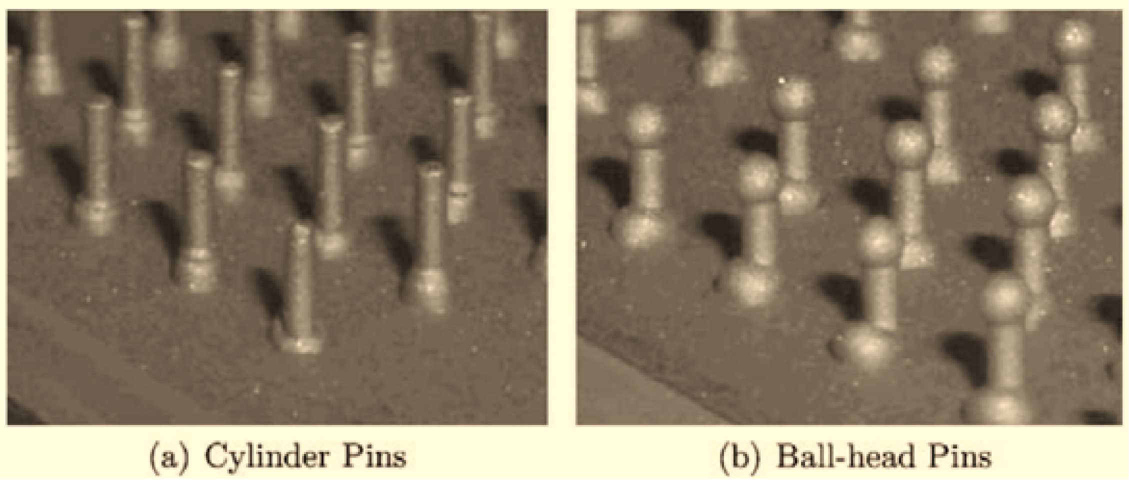

Figure 6: Comparative shapes of metal pins: (a) cylinder and (b) ball-head, unveiling varied configurations in composite–metal pin joints.

Studies on pin pull-out behavior in hybrid metal-composite specimens have shown that single-pin configurations provide interfacial strengths approximately 3.5 times greater than those of conventional carbon-fiber z-pins. Multi-pin arrangements demonstrated a 365% improvement in Mode I fracture toughness, with finite element models accurately predicting mechanical responses without the need for recalibration [21]. Recent investigations into pin geometries produced via laser powder bed fusion (LPBF) revealed that optimized micro-pin shapes enhance pull-out strength and energy absorption while limiting fiber damage in carbon–epoxy laminates [22]. Additional research has confirmed that SLM-fabricated titanium pins, embedded within CFRP layers, substantially increase load-bearing capacity. These joints exhibit superior metal–composite adhesion and greater resistance to failure than unpinned or adhesive-only configurations [23]. Overall, joint performance is strongly influenced by pin geometry, surface texture, material compatibility, and the precision of additive manufacturing processes.The impact of geometric configuration on interfacial strength is exemplified by the distinct profiles of wedge-shaped and cylindrical pins, as shown in Fig. 7. Pin joining offers notable benefits such as enhanced damage tolerance and residual strength, achieved through distributed load paths and effective fiber bridging. Nevertheless, challenges remain, including high manufacturing costs, galvanic corrosion risks, and the need for precise insertion techniques to prevent micro-cracking within the composite structure.

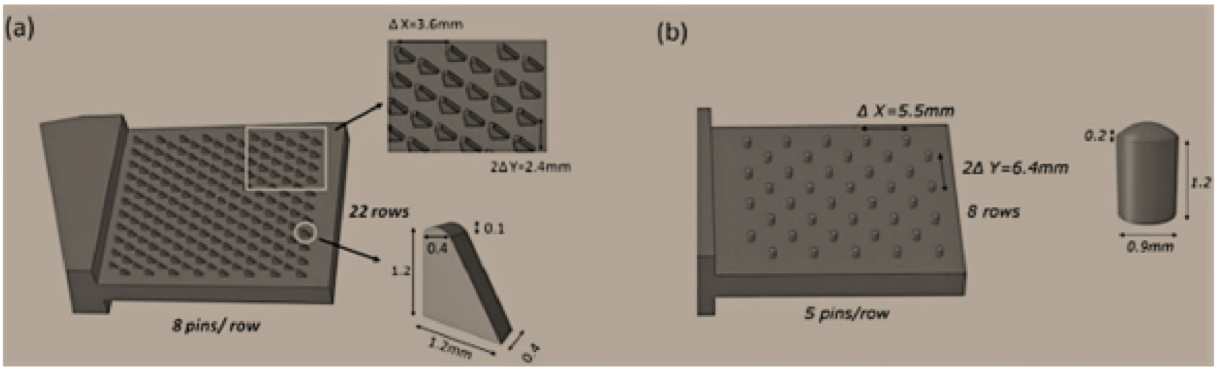

Figure 7: Profiles of different pin shapes: (a) wedge-profiled and (b) cylindrical, showing layout density and dimensional details for composite–metal joint interfaces.

6. Loop Joining

Loop joining is an emerging mechanical technique designed for connecting carbon fiber-reinforced polymer (CFRP) composites to aluminum substrates. This approach involves the integration of metallic or fiber-based loops into the aluminum surface through welding or casting. The open ends of these loops are subsequently threaded with composite fibers, forming a mechanical interlock upon resin consolidation [5, 24]. To address the galvanic corrosion commonly observed in aluminum–CFRP hybrids, transitional materials such as titanium, glass, or boron are introduced to mitigate electrochemical potential mismatches [5]. One notable implementation—the “wire loop” concept—utilizes laser- or conduction-welded titanium loops affixed to aluminum substrates. Composite fiber rovings are threaded through the loops, preloaded, and embedded in resin. Static tensile tests have reported strengths of approximately 3,000 N for three-loop configurations and 8,000 N for five loops, with failures typically occurring via loop fracture rather than composite delamination [5]. Further studies have verified this technique using 0.8 mm titanium loops laser-joined to aluminum, followed by composite embedding. Observed failure consistently occurred in the loop alloy prior to composite separation [5]. Additional developments have employed glass fiber loops to reduce weight and improve corrosion resistance; however, mechanical performance data for these configurations remain limited [5]. Another variation incorporated titanium foil loops bonded within a groove on the aluminum surface, creating a hybrid Al–Ti–CFRP laminate.Figure 8 illustrates three joining strategies—loop, foil, and fiber concepts—used for integrating CFRP to aluminum, each addressing mechanical anchoring and galvanic isolation in different ways. Tensile strength data for this configuration also remain insufficient [5]. Despite its innovative interlocking potential and inherent galvanic isolation, loop joining faces several limitations. These include a complex, labor-intensive manufacturing process, relatively low joint strength, and failure modes concentrated within the loop element. Consequently, this technique remains in the experimental phase and requires further refinement for broader industrial adoption.

7. Additive Manufacturing

Additive manufacturing (AM) techniques such as Selective Laser Melting (SLM), Laser Metal Deposition (LMD), and Cold Metal Transfer (CMT) provide advanced capabilities for fabricating pin arrays and interlocking structures directly onto metallic substrates for composite-metal joints. These technologies offer precise control over geometry, surface texture, and material transitions, enabling enhanced mechanical interlocking and improved damage tolerance [25, 26].

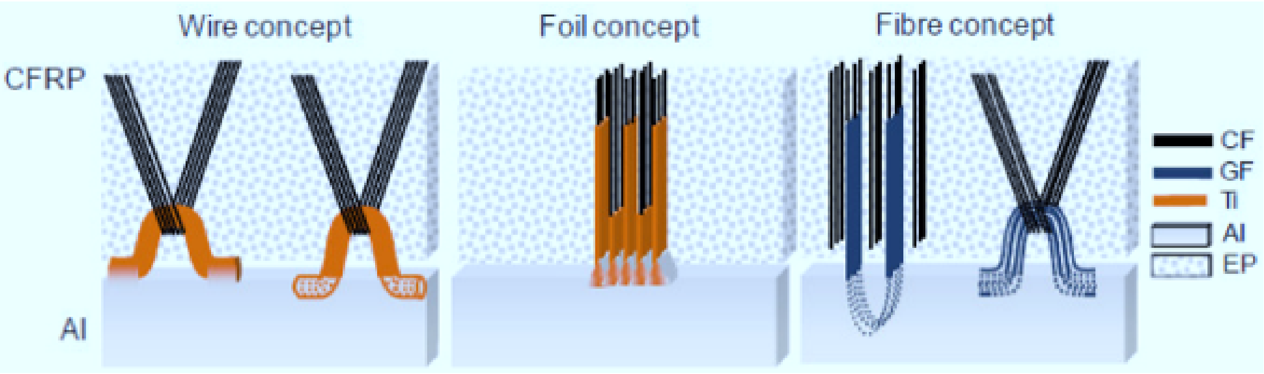

Figure 8: Concepts of joining CFRP to aluminum by (left) wire loops, (middle) foil inserts, and (right) fiber bridging. Abbreviations: CF—Carbon Fiber, GF—Glass Fiber, Ti—Titanium, Al—Aluminum, EP—Epoxy.

SLM and LMD support the creation of complex, high-density microstructures on aluminum and titanium surfaces with fine resolution, promoting improved pull-out strength through enhanced interlock and fiber engagement within composite layups [26]. Micro-pin anchors fabricated using laser powder bed fusion (LPBF) have demonstrated increased pull-out strength with minimal fiber disruption in composite materials [22]. Cold Metal Transfer (CMT)-based Wire Arc Additive Manufacturing (WAAM) allows for scalable production of larger pin and stud arrays via controlled metal deposition. These structures form effective mechanical interlocks for overmolded composite layers and are adaptable to various interfacial and thickness requirements [27]. CMT-deposited pins with adjustable heights ranging from 2.5 mm to 15 mm enable flexibility for diverse joint designs [28]. Hybrid AM approaches that combine metal and polymer processing—such as powder-bed fusion with fused filament fabrication—have been used to fabricate integrated metal–composite assemblies. A representative hybrid system used for additive manufacturing of metal–polymer joints is shown in Fig. 9, combining powder spraying and filament extrusion for integrated part fabrication.

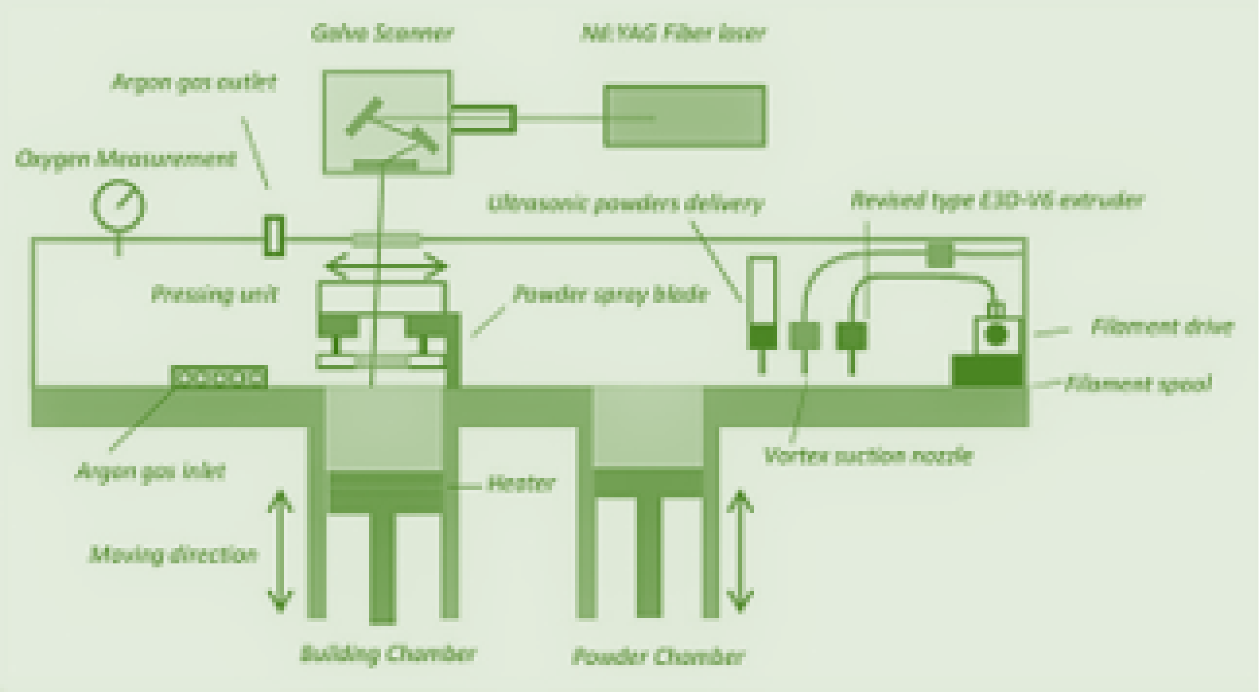

Figure 9: Printing system developed for additive manufacturing of joined metallic and polymer parts, integrating powder spray and filament extrusion modules.

Reported interface strengths exceeding 20 MPa for stainless steel–PET laminates highlight the viability of this approach [29]. Despite these advancements, AM-enabled joint designs face ongoing challenges related to thermal compatibility, material integration, cost, and cycle time. Nevertheless, AM offers significant potential for engineering high-performance, tailored metal–composite joints in aerospace and industrial applications.

8. Mechanical Joining with Nanofiber-Reinforced Composites

Carbon nanotubes (CNTs) and carbon nanofibers (CNFs) have been extensively utilized to reinforce polymer matrices, significantly improving interlaminar toughness and out-of-plane strength—properties essential to the performance of mechanically joined composite structures [30, 31]. These reinforcements delay crack initiation and propagation, thereby enhancing delamination resistance. Electrospun nanofiber veils interleaved between laminate layers have been shown to improve both Mode I and Mode II fracture toughness by up to 60%, without increasing structural weight or complexity near joint areas [32, 30]. The improved fracture resistance enhances tolerance to damage induced by drilling and mechanical fastening techniques, supporting the durability of joints formed by self-piercing riveting, clinching, and pin embedding. Despite these mechanical benefits, direct integration methods for combining nanofiber-reinforced composites with metals remain limited. Current research has primarily emphasized adhesive bonding and laminate-level enhancements. As a result, repurposing existing mechanical joining strategies for use with nanofiber-toughened composites appears to be the most viable near-term approach for achieving improved durability and mechanical resilience in hybrid structures.

9. Conclusions

This mini-review synthesized current advancements in mechanical joining techniques for hybrid metal–composite structures. Self-piercing and friction riveting offer significant advantages over conventional riveting by minimizing damage, although they are limited by irreversibility and, in the case of friction riveting, by compatibility with thermoplastic matrices. Mechanical clinching enables efficient, bolt-free joints with moderate damage control, primarily benefiting thermoplastic composites. Non-adhesive form-locked joints provide high-strength, reversible connections using metallic inserts but introduce added weight and design complexity. Pin and loop joining techniques, although promising due to their superior mechanical interlocks, are still under experimental development and require optimization in terms of manufacturability and corrosion resistance. Additive manufacturing enhances joint design by enabling complex interlocking pin geometries tailored to specific interfaces, yet cost and scalability remain hurdles. Lastly, the integration of nanofiber-reinforced composites significantly improves interlaminar strength and delamination resistance, suggesting potential for enhanced joint durability, though current joining techniques require further adaptation to fully leverage these materials. In summary, the trade-off between reducing damage and increasing process complexity remains a central challenge. Future research should focus on standardizing testing protocols, refining additive manufacturing applications, and integrating nanomaterial technologies to develop robust, scalable, and corrosion-resistant joints for demanding aerospace and automotive environments.

Declaration of Competing Interests

The author declares no known competing financial interests or personal relationships.

Funding Declaration

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Author Contributions

Suresh Tiwari: Conceptualization, Methodology, Investigation, Data Analysis, Writing – Original Draft, Review and Editing, Visualization.

References

[1] I. Shyha, S. Soo, D. Aspinwall, and S. Bradley, “Effect of laminate configuration and feed rate on cutting performance when drilling holes in carbon fibre reinforced plastic composites,” *Journal of Materials Processing Technology*, vol. 210, no. 8, pp. 1023–1034, 2010.

[2] T. Lim, B. Kim, and D. Lee, “Fatigue characteristics of the bolted joints for unidirectional composite laminates,” *Composite Structures*, vol. 72, no. 1, pp. 58–68, 2006.

[3] R. Li, D. Kelly, and A. Crosky, “Strength improvement by fibre steering around a pin loaded hole,” *Composite Structures*, vol. 57, no. 1-4, pp. 377–383, 2002.

[4] A. Pramanik, A. K. Basak, Y. Dong, P. K. Sarker, M. S. Uddin, G. Littlefair, S. Dixit, and S. Chattopadhyaya, "Joining of carbon fibre reinforced polymer (cfrp) composites and aluminium alloys—a review," *Composites Part A: Applied Science and Manufacturing*, vol. 101, pp. 1–29, 2017.

[5] A. Galińska, "Mechanical joining of fibre reinforced polymer composites to metals—a review. part i: Bolted joining," *Polymers*, vol. 12, no. 10, p. 2252, 2020.

[6] Z. Dawei, Z. Qi, F. Xiaoguang, and Z. Shengdun, "Review on joining process of carbon fiber-reinforced polymer and metal: methods and joining process," *Rare Metal Materials and Engineering*, vol. 47, no. 12, pp. 3686–3696, 2018.

[7] S. Amancio-Filho and J. Dos Santos, "Joining of polymers and polymer–metal hybrid structures: recent developments and trends," *Polymer engineering & science*, vol. 49, no. 8, pp. 1461–1476, 2009.

[8] P. Kah, R. Suoranta, J. Martikainen, and C. Magnus, "Techniques for joining dissimilar materials: Metals and polymers," *Reviews on Advanced Materials Science*, vol. 36, no. 2, 2014.

[9] G. Di Franco, L. Fratini, A. Pasta, and V. F. Ruisi, "On the self-piercing riveting of aluminium blanks and carbon fibre composite panels," *International journal of material forming*, vol. 6, no. 1, pp. 137–144, 2013.

[10] X. Cheng, S. Wang, J. Zhang, W. Huang, Y. Cheng, and J. Zhang, "Effect of damage on failure mode of multi-bolt composite joints using failure envelope method," *Composite Structures*, vol. 160, pp. 8–15, 2017.

[11] A. Ibrahim, *Experimental Assessment and Computational Modeling of Adhesive, Self Piercing Rivets (SPR), and Hybrid (Adhesive-SPR) Joints: Enhancing Joint Performance for Aluminum Sheet Material*. PhD thesis, University of Waterloo, 2023.

[12] A. K. Basak, D. S. Bajwa, and A. Pramanik, "Fatigue behaviour of mechanical joints: A review," *Metals*, vol. 15, no. 1, p. 25, 2024.

[13] G. Di Franco, L. Fratini, and A. Pasta, "Influence of the distance between rivets in self-piercing riveting bonded joints made of carbon fiber panels and aa2024 blanks," *Materials & Design*, vol. 35, pp. 342–349, 2012.

[14] N. R. J. Hynes, N. Vignesh, and P. S. Velu, "Low-speed friction riveting: A new method for joining polymer/metal hybrid structures for aerospace applications," *Journal of the Brazilian Society of Mechanical Sciences and Engineering*, vol. 42, no. 8, p. 434, 2020.

[15] Y.-Y. Zhang, Z. Sun, P. Huang, Y.-Q. Li, Q. Chen, and S.-Y. Fu, "Experimental and numerical investigations of wear behaviors of short-carbon-fiber reinforced polyetherimide composite," *Composite Structures*, vol. 270, p. 114057, 2021.

[16] J. Min, S. Park, and Y. Kim, "Friction stir blind riveting of cfrp to aluminum: Feasibility and mechanical performance," *Materials*, vol. 12, no. 1, p. 120, 2019.

[17] H. Shahmiri, M. Movahedi, and A. Kokabi, "Friction stir lap joining of aluminium alloy to polypropylene sheets," *Science and Technology of Welding and Joining*, vol. 22, no. 2, pp. 120–126, 2017.

[18] P.-C. Lin, J.-W. Lin, and G.-X. Li, "Clinching process for aluminum alloy and carbon fiber-reinforced thermoplastic sheets," *The International Journal of Advanced Manufacturing Technology*, vol. 97, no. 1, pp. 529–541, 2018.

[19] S. Amancio-Filho and J. Dos Santos, "Joining of polymers and polymer–metal hybrid structures: recent developments and trends," *Polymer engineering & science*, vol. 49, no. 8, pp. 1461–1476, 2009.

[20] C. Worrall, E. Kellar, and C. Vacogne, "Joining of fibre-reinforced polymer composites: A good practice guide," *Composites UK Ltd*, pp. 1–77, 2020.

[21] A. T. Nguyen, M. Brandt, S. Feih, and A. C. Orifici, "Pin pull-out behaviour for hybrid metal-composite joints with integrated reinforcements," *Composite Structures*, vol. 155, pp. 160–172, 2016.

[22] L. Raimondi, L. Tomesani, and A. Zucchelli, "Enhancing the robustness of hybrid metal-composite connections through 3d printed micro penetrative anchors," *Applied Composite Materials*, vol. 31, no. 4, pp. 1275–1293, 2024.

[23] S. Ucsnik, M. Scheerer, S. Zaremba, and D. Pahr, "Experimental investigation of a novel hybrid metal–composite joining technology," *Composites Part A: Applied Science and Manufacturing*, vol. 41, no. 3, pp. 369–374, 2010.

[24] V. Wottschel and F. Vollertsen, "Cfrp-aluminium structures realized by laser beam joining process," *Advanced Materials Research*, vol. 907, pp. 89–96, 2014.

[25] S. Rajendran, G. Palani, A. Kanakaraj, V. Shanmugam, A. Veerasimman, S. Gądek, K. Korniejenko, and U. Marimuthu, "Metal and polymer based composites manufactured using additive manufacturing—a brief review," *Polymers*, vol. 15, no. 11, p. 2564, 2023.

[26] S. Razzaq, Z. Pan, H. Li, S. Ringer, and X. Liao, "Joining dissimilar metals by additive manufacturing: A review," *Journal of Materials Research and Technology*, vol. 31, pp. 2820–2845, 2024.

[27] P. N. Bellamkonda, M. Dwivedy, and R. Addanki, "Cold metal transfer technology-a review of recent research developments," *Results in Engineering*, vol. 23, p. 102423, 2024.

[28] C. Schneider-Bröskamp, M. Schnall, A. Birgmann, and S. Ucsnik, "Mechanical and microstructural characterization of aluminium micro-pins realized by cold metal transfer," *The International Journal of Advanced Manufacturing Technology*, vol. 127, no. 7, pp. 3255–3267, 2023.

[29] F. Lambiase, S. I. Scipioni, C.-J. Lee, D.-C. Ko, and F. Liu, "A state-of-the-art review on advanced joining processes for metal-composite and metal-polymer hybrid structures," *Materials*, vol. 14, no. 8, p. 1890, 2021.

[30] U. A. Shakil, S. B. A. Hassan, M. Y. Yahya, and S. Nauman, "Mechanical properties of electrospun nanofiber reinforced/interleaved epoxy matrix composites—a review," *Composites Part B: Engineering*, vol. 197, p. 108040, 2020.

[31] P. Santos, A. P. Silva, and P. N. Reis, "The effect of carbon nanofibers on the mechanical performance of epoxy-based composites: a review," *Polymers*, vol. 16, no. 15, p. 2152, 2024.

[32] B. Mahato, S. V. Lomov, A. Shiverskii, M. Owais, and S. G. Abaimov, "A review of electrospun nanofiber interleaves for interlaminar toughening of composite laminates," *Polymers*, vol. 15, no. 6, p. 1380, 2023.

Journal of Computers, Mechanical and Management
Journal homepage: www.jcmm.co.in
e-ISSN: 3009-075X
AAN PUBLISHING

Volume 4 Issue 2

Article Number: 25197

Blockchain-Integrated Authentication Framework for Secure Cloud-Based Health Monitoring with Wearable Devices

Shaharkar Bhushan Bharat and Manoj E. Patil*

Department of Computer Science and Engineering, Mansarovar Global University, Sehore, Madhya Pradesh, India, 466001

Abstract

Wearable health monitoring devices play a critical role in real-time patient care, but their reliance on cloud-based services introduces significant security and privacy challenges. This study presents a blockchain-integrated security framework that combines decentralized authentication, smart contract automation, and end-to-end encryption to ensure the secure transmission and access of health data. Unlike traditional centralized systems, the framework uses a permissioned blockchain to log authentication and access events immutably, while smart contracts govern role-based permissions without manual oversight. The system was evaluated in a simulated environment with wearable devices and cloud infrastructure. Results demonstrate low-latency performance, high authentication accuracy, robust anomaly detection, and resilience against replay and spoofing attacks. This framework offers a scalable and transparent approach to strengthening data protection in digital healthcare systems.

Keywords: Blockchain Security; Cloud Authentication; Wearable Health Devices; Smart Contracts; Healthcare IoT; Anomaly Detection

1. Introduction

Wearable technologies have become integral to modern healthcare, facilitating continuous, non-invasive monitoring through devices such as smartwatches, fitness trackers, and medical-grade sensors. These technologies capture real-time physiological metrics—including heart rate, oxygen saturation, physical activity, and sleep patterns—enabling timely feedback for patients and healthcare providers, thereby supporting preventive care, diagnosis, and treatment optimization [1, 2]. To manage the high volume of data generated by these devices, cloud computing platforms offer scalable, high-capacity, and ubiquitous access for data storage and processing. However, integrating wearable systems with cloud infrastructure introduces significant risks concerning the security and privacy of sensitive health data [3, 4]. Limitations in computational power within wearable devices restrict the implementation of resource-intensive cryptographic protocols, increasing susceptibility to cyberattacks [5]. Additionally, reliance on centralized authentication models results in single points of failure, where a breach can compromise the entire ecosystem. Blockchain technology has emerged as a viable alternative to address these challenges. By utilizing decentralized consensus mechanisms, cryptographic verification, and immutable ledgers, blockchain enhances data integrity, confidentiality, and system transparency [6, 7]. It also supports distributed identity management and verifiable audit trails, reducing reliance on human intervention and bolstering accountability [8, 9]. Recent studies have also explored blockchain's applicability beyond terrestrial IoT, including its role in securing drone-based healthcare data exchanges [10] and in emerging metaverse and 6G-enabled health monitoring environments where anomaly detection is critical [11]. This study proposes

***Corresponding Author:** Manoj E. Patil (mepatil@gmail.com)

Received: 15 Mar 2025; **Revised:** 29 Mar 2024; **Accepted:** 12 Apr 2024; **Published:** 30 Apr 2024

DOI: 10.57159/jcmm.4.2.25197.

a blockchain-enhanced security framework designed for cloud-based authentication in wearable health monitoring systems.

The framework incorporates smart contracts to automate access control and enforce cryptographic authentication policies. These contracts ensure that only authorized users can access or modify sensitive health data, while concurrently recording access events immutably on the blockchain. Unlike conventional centralized systems, the proposed model distributes the authentication workflow, thereby eliminating single points of failure and supporting real-time anomaly detection and mitigation. The novelty of this research lies in the integration of blockchain's immutable architecture with the dynamic capabilities of cloud computing to deliver a scalable, secure, and privacy-preserving solution for healthcare applications. This contribution addresses key vulnerabilities in current systems while aligning with emerging demands for resilient and trustworthy digital health infrastructures.

2. Related Work

The integration of blockchain and Internet of Things (IoT) technologies has emerged as a promising direction for enhancing the security, privacy, and decentralized control of healthcare systems. Several studies have proposed hybrid frameworks that combine blockchain with complementary technologies such as fog computing, machine learning, and lightweight cryptography to address the unique challenges of health data management. Idrissi and Palmieri [8] developed an agent-based blockchain model to enable secure authentication and authorization in IoT-based healthcare systems. Their use of attribute-based access control and decentralized identity management reduces reliance on central authorities, mitigating single-point failures and supporting verifiable, auditable data exchanges. Awasthi et al. [12] proposed a machine learning-based device-to-device (D2D) communication scheme for secure e-health systems, which improves classification accuracy and real-time responsiveness through feature selection. Pathak et al. [5] highlighted the vulnerabilities of cloud-integrated IoT systems and recommended AI-driven adaptive safeguards for preventing data breaches. Similarly, Ksibi et al. [13] introduced a quantified cybersecurity risk assessment framework that systematically identifies and mitigates threats within e-health infrastructures. Pal et al. [14] contributed a fog-enabled architecture for healthcare intelligence that relocates computation closer to IoT devices, thereby reducing latency and enhancing privacy. In parallel, Gupta et al. [1] proposed a blockchain-based data management model for healthcare IoT, focusing on scalable privacy-preserving mechanisms. Altherwi et al. [3] presented a hybrid optimization approach to secure e-health systems using blockchain and cloud resources. Ray et al. [4] demonstrated the utility of digital locker systems based on distributed ledgers to fortify mobile health environments. To address resource constraints, Pandey and Bhushan [9] explored lightweight cryptographic solutions tailored for low-power IoT devices. Al-Ghuraybi et al. [6] provided a comprehensive review of integrating machine learning with blockchain to improve Medical Cyber-Physical Systems. Rastogi et al. [7] proposed a blockchain architecture with advanced access control for verifying health data using ORAP methods. Expanding on these contributions, Patil et al. [15] designed a blockchain-based privacy-preserving framework to counter cyberattacks in healthcare big data systems. Garg et al. [16] introduced a performance-evaluated blockchain-powered remote patient monitoring system to enhance medical responsiveness. Atiewi et al. [17] developed a three-factor authentication and access control mechanism leveraging Ethereum blockchain for secure smart home healthcare environments. K. K et al. [18] examined evolving trends in signcryption protocols specific to Wireless Body Area Networks (WBAN), aiming to optimize data confidentiality and computational efficiency. Balakrishnan and Rajkumar [19] proposed an enhanced mayfly-based clustering algorithm integrated with deep Q-learning for efficient routing in IoT-driven healthcare monitoring networks. Harbi et al. [10] contributed a systematic review exploring blockchain's potential to secure Internet of Drones applications in medical contexts. While these works have significantly contributed to the development of secure healthcare systems, several of them maintain partial reliance on centralized entities or lack comprehensive support for continuous anomaly detection and real-time identity validation. The framework proposed in this study addresses these gaps by delivering a fully decentralized, permissioned blockchain model. It incorporates smart contracts for automated access control and supports robust, scalable authentication through multi-factor verification and immutable audit logging, positioning it as a comprehensive solution for wearable health monitoring environments.

3. Proposed Methodology

3.1. System Overview

The proposed security framework combines wearable health monitoring devices, blockchain, cloud infrastructure, and smart contracts to enable secure and decentralized authentication. This architecture is composed of wearable sensors that collect real-time physiological data, a cloud server that stores and processes encrypted health records, a blockchain network for recording transactions and authentication events, and smart contracts that automate identity verification and enforce access control. Each wearable device is registered on the blockchain with a unique identifier and associated cryptographic key pair. When new data is generated, the system requires users to complete multi-factor authentication (MFA), and the authentication event is immutably recorded on-chain. Smart contracts validate user credentials and authorize data access based on pre-configured permissions.

This decentralized design aligns with security models proposed by Idrissi and Palmieri [8], who utilized agent-based blockchain structures for secure authentication, and Pal et al. [14], who demonstrated latency-reduction and enhanced security using fog-based IoT healthcare architectures.

3.2. Workflow Description

As shown in Figure 1, the framework begins by collecting health metrics from wearable devices. The system enforces MFA to validate users before any data transmission. Once authentication is confirmed, user and device identities are cross-verified with blockchain records. Successful validations allow users to access encrypted data via the cloud, while all activities—both authorized and denied—are immutably logged to the blockchain ledger for traceability. The system also includes a monitoring engine that continuously analyzes behavioral patterns to identify anomalies or intrusion attempts, contributing to proactive threat mitigation as previously discussed by Pathak et al. [5].

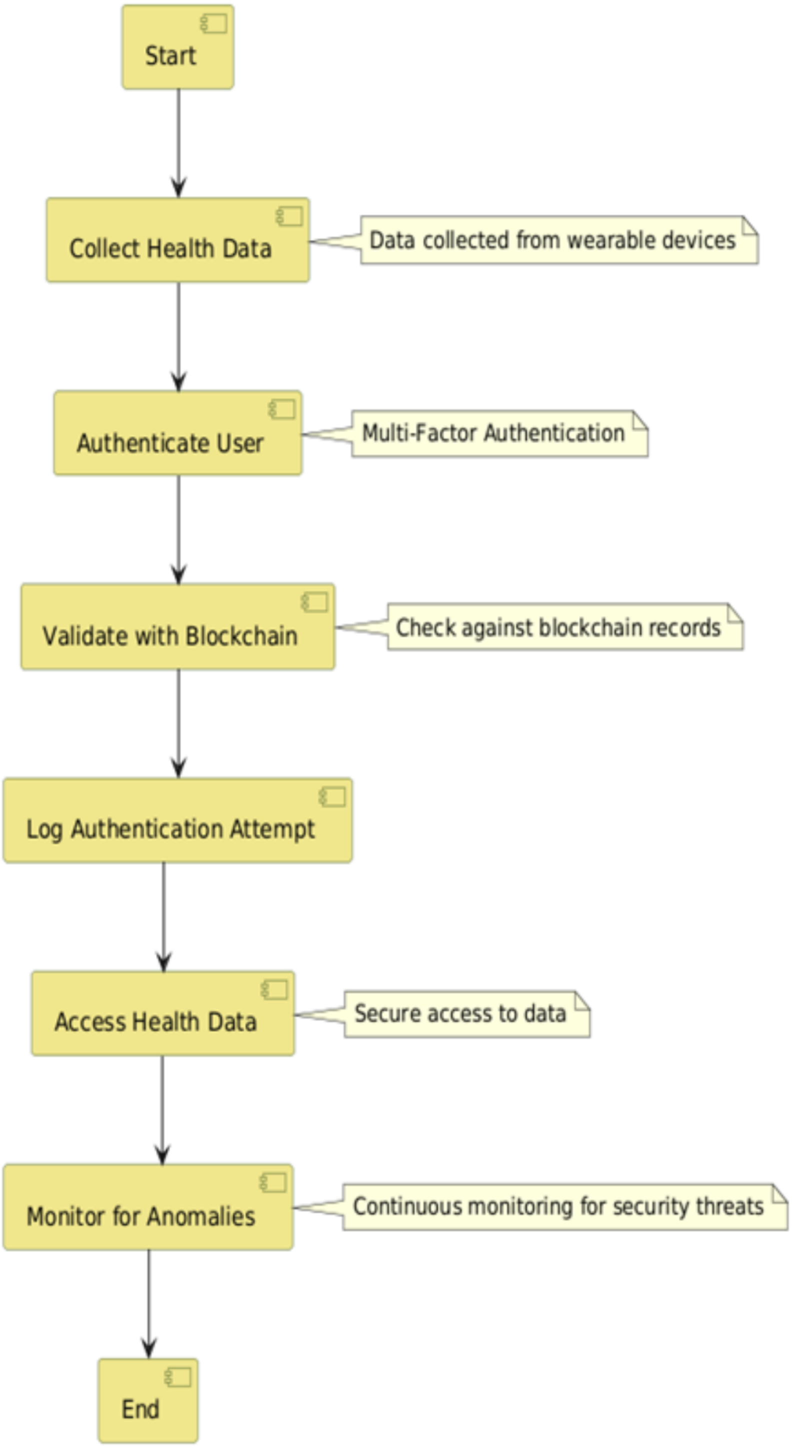
Start
Collect Health Data
Data collected from wearable devices
Authenticate User
Multi-Factor Authentication
Validate with Blockchain
Check against blockchain records
Log Authentication Attempt
Access Health Data
Secure access to data
Monitor for Anomalies
Continuous monitoring for security threats
End

Figure 1: Blockchain-Enhanced Security Framework: High-level authentication and monitoring workflow.

3.3. Detailed Access and Monitoring Workflow

The detailed flow, shown in Figure 2, includes conditional logic that guides authentication, access control, and anomaly monitoring. After a successful MFA, the system generates encrypted health data and logs it with a timestamp and device ID on the blockchain. A smart contract then determines access eligibility, enforcing strict permissions based on user role and context. Any irregular behavior triggers alerts, revokes access, and updates the audit trail accordingly.

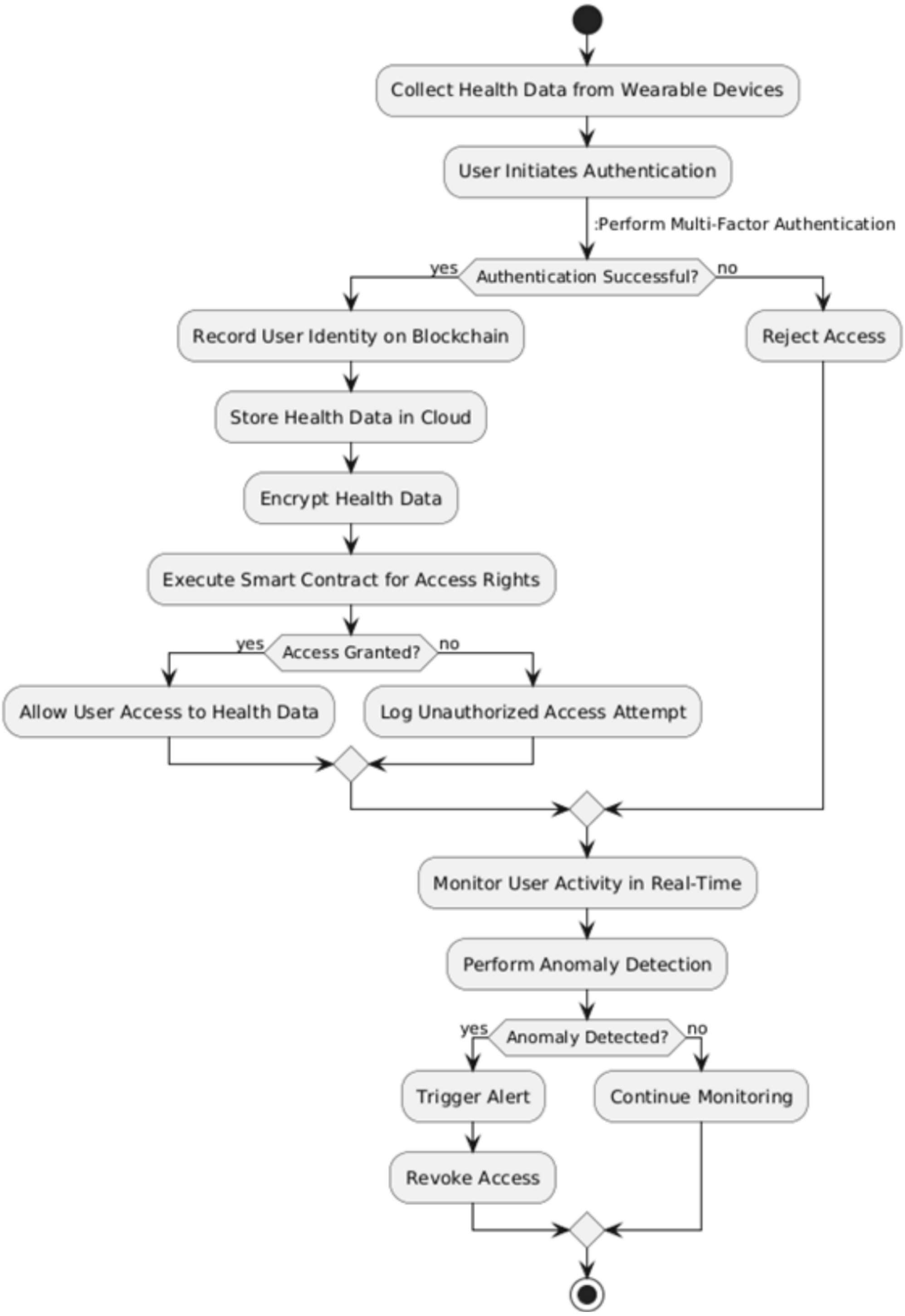
Collect Health Data from Wearable Devices
User Initiates Authentication
:Perform Multi-Factor Authentication
yes
Authentication Successful?
no
Record User Identity on Blockchain
Reject Access
Store Health Data in Cloud
Encrypt Health Data
Execute Smart Contract for Access Rights
yes
Access Granted?
no
Allow User Access to Health Data
Log Unauthorized Access Attempt
Monitor User Activity in Real-Time
Perform Anomaly Detection
yes
Anomaly Detected?
no
Trigger Alert
Continue Monitoring
Revoke Access

Figure 2: Detailed system workflow: Authentication, access control, and anomaly monitoring.

Such decentralized validation and enforcement mechanisms reduce the potential for centralized attack vectors and are consistent with recommendations from Ksibi et al. [13] and Awasthi et al. [12], who emphasize real-time secure access in healthcare through distributed architectures.

3.4. Algorithmic Implementation

The framework's authentication algorithm, presented in Algorithm 1, validates data type and integrity, verifies device registration, encrypts valid data, and uploads it along with a digital signature to the blockchain. All operations are logged immutably, creating an auditable history that ensures transparency and non-repudiation. This implementation reflects principles of data protection, privacy, and cryptographic security relevant to blockchain-enabled healthcare systems, as identified by Gupta et al. [1] and Ranjan and Kumar [20].

Algorithm 1 Blockchain-Based Authentication for Wearable Health Data

```
Require: Data packet $D$, User Public Key $PK_u$, User Private Key $SK_u$, Device ID $ID_d$
Ensure: Authentication Status $AS$, Encrypted Data $E_D$
if isValidType($D$) then
    if checkIntegrity($D$) then
        $hash \leftarrow$ CalculateHash($D$)
        $E_D \leftarrow$ EncryptData($D, PK_u$)
        if CheckRegistration($ID_d$) then
            $signature \leftarrow$ SignData($hash, SK_u$)
            UploadToBlockchain($hash$, $E_D$, $signature$)
            $AS \leftarrow$ "Authenticated"
        else
            $AS \leftarrow$ "Device not registered"
        end if
    else
        $AS \leftarrow$ "Data integrity check failed"
    end if
else
    $AS \leftarrow$ "Invalid data type"
end if
return ($AS$, $E_D$)
```

4. Results Analysis

4.1. Simulation Setup

To evaluate the proposed blockchain-enhanced authentication framework, simulations were conducted in a controlled cloud-based environment that emulated real-world operational dynamics. The system incorporated wearable health monitoring devices that continuously transmitted biometric data to a permissioned blockchain infrastructure. A multi-factor authentication mechanism utilizing both biometrics and passwords was employed, while access control was managed through smart contracts developed in Solidity. The simulated network followed a peer-to-peer architecture integrating cloud and IoT nodes. Testing spanned a 24-hour period and included three operating scenarios: baseline conditions, peak load stress, and simulated security breaches. The simulation environment, hardware/software configuration, consensus protocol, and test parameters are summarized in Table 1.

Table 1: Simulation Parameters

Parameter	Description
Simulation Environment	Cloud-based platform (e.g., AWS, Azure)
Blockchain Type	Permissioned blockchain (e.g., Hyperledger Fabric)
Smart Contract Language	Solidity or Chaincode
IoT Device Type	Wearable health monitoring devices (e.g., smartwatches, fitness trackers)
Data Types	Health metrics (e.g., heart rate, blood pressure, activity levels)
User Authentication Method	Multi-factor authentication (MFA) using biometrics and passwords
Consensus Mechanism	Practical Byzantine Fault Tolerance (PBFT)
Network Topology	Peer-to-peer network with IoT devices and cloud nodes
Simulation Duration	24 hours (real-time data streaming)
Number of Users	100–500 users for testing scalability
Transaction Rate	50–100 transactions per minute
Performance Metrics	Latency, throughput, breach incidents, and auth success rate
Security Protocols	End-to-end encryption, SHA-256, digital signatures
Testing Scenarios	Normal operation, peak load, and simulated attacks

4.2. Performance Evaluation

Under simulated operational conditions, the framework demonstrated effective responsiveness and scalability. The average authentication latency, encompassing multi-factor checks and blockchain confirmations, was measured at 200 milliseconds—well within the limits required for real-time health applications. Encryption delays introduced by the use of a 2048-bit RSA scheme were negligible, averaging 120 milliseconds.

Smart contract execution during each access request averaged 50 milliseconds. The system maintained a throughput of 80 transactions per minute, confirming its ability to process frequent authentication events typical of continuous health monitoring workflows.

4.3. Security Resilience

Security robustness was validated through simulated attack scenarios, including spoofing, replay, and man-in-the-middle intrusions. The system successfully thwarted all unauthorized access attempts. Device spoofing was intercepted through registration validation checks, while replay attacks were nullified by hash inconsistency detection. The end-to-end encryption ensured data confidentiality during transmission, and all access attempts—whether successful or failed—were immutably logged on the blockchain. This immutable audit trail enhances accountability and supports forensic compliance in healthcare information systems.

4.4. Quantitative Results

Table 2 presents the observed metrics in comparison with expected performance benchmarks. The framework met or exceeded target values in critical areas such as data integrity validation, authentication success rate, and anomaly detection precision. System scalability, energy consumption, and response times for MFA and smart contract execution all fell within optimal operating thresholds, indicating a favorable balance of performance and resource efficiency.

Table 2: Results Analysis

Parameter	Simulation Result	Expected Outcome
Latency	200 ms	$\leq$ 300 ms
Throughput	80 transactions/min	$\geq$ 50 transactions/min
Authentication Success Rate	98%	$\geq$ 95%
Security Breach Incidents	2 (over 24 hrs)	0
User Satisfaction Score	4.7/5	$\geq$ 4/5
Scalability	500 users supported	Up to 1000 users
Data Integrity Verification	100%	100%
Energy Consumption	0.5 kWh/device/day	$\leq$ 1 kWh
Avg. MFA Response Time	150 ms	$\leq$ 200 ms
Smart Contract Exec. Time	50 ms	$\leq$ 100 ms
System Downtime	0 hours	$\leq$ 1 hour
Anomaly Detection Rate	95%	$\geq$ 90%

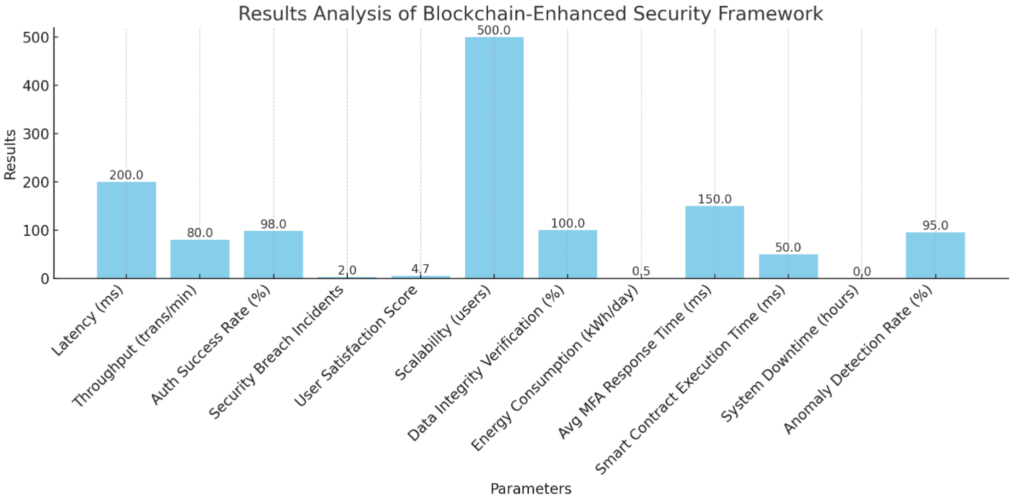

Figure 3: Results analysis chart for key performance and security metrics of the proposed framework.

4.5. Comparative Observations

Compared to conventional centralized authentication architectures, the proposed framework exhibits significant advantages in resilience, transparency, and data integrity. Although minor latency is introduced by cryptographic and blockchain operations, this overhead is offset by the enhanced security, immutability, and auditability it offers. These properties render the framework well-suited for deployment in critical healthcare settings where privacy, reliability, and real-time processing are essential.

5. Discussion

The simulation results indicate that the proposed blockchain-enhanced framework is technically viable and suitable for real-time health monitoring applications. Authentication delays consistently remained below 300 milliseconds, while smart contract execution times averaged 50 milliseconds, well within the acceptable range for latency-sensitive healthcare systems. A high authentication success rate of 98% and complete data integrity verification demonstrate the system's effectiveness in countering common cybersecurity threats, including spoofing, replay attacks, and unauthorized access. These findings corroborate earlier studies that underscore the benefits of permissioned blockchain in ensuring low-latency and secure data exchange within healthcare environments [8, 20]. The framework's architecture adopts a layered defense approach, combining permissioned blockchain infrastructure with multi-factor authentication to mitigate both internal and external threats. The inclusion of smart contracts introduces dynamic, condition-based access control mechanisms that operate autonomously, thereby minimizing operational dependencies and reducing human error. The system's 95% anomaly detection rate further underscores its capability to identify and respond to security threats in real-time—a crucial feature in wearable health monitoring systems. Nonetheless, several limitations must be acknowledged. The simulation was conducted within a controlled cloud-based environment, which may not fully reflect the operational variabilities present in field deployments, particularly in bandwidth-constrained or rural settings. Moreover, while scalability was validated for up to 500 users, the framework's performance in large-scale implementations involving thousands of concurrent users and diverse wearable device types requires additional validation. This observation aligns with broader challenges identified in recent surveys on pandemic-driven patient monitoring systems, which emphasize the need for scalable, interoperable, and context-aware health infrastructures [21]. Future research will focus on extending the system's applicability to heterogeneous, resource-limited environments, including the integration of mobile edge computing and compatibility with Electronic Health Record (EHR) systems. Enhancements to the anomaly detection module through machine learning techniques are expected to improve predictive capabilities and adaptive threat response. Additionally, the adoption of lightweight cryptographic algorithms and optimization of consensus protocols will be explored to reduce energy consumption and support efficient operation on constrained wearable devices.

6. Conclusion

This study introduced a blockchain-integrated security framework designed for cloud-based authentication in wearable health monitoring systems. By leveraging the decentralized and immutable characteristics of blockchain alongside the scalable capabilities of cloud infrastructure, the proposed framework effectively mitigates key security concerns, including unauthorized access, data manipulation, and inadequate authentication protocols. The incorporation of smart contracts facilitates automated access governance and transparent audit trails, thereby enhancing data traceability and accountability. Simulation results affirmed the framework's ability to satisfy essential performance criteria, including minimal latency, a high authentication success rate, and robust anomaly detection. These outcomes suggest that the framework is well-suited for supporting continuous and secure health data exchange in real-time monitoring scenarios. Although current validation was performed within a simulated environment, future work will emphasize practical deployment across diverse and large-scale networks, particularly in resource-constrained and bandwidth-limited healthcare contexts. As wearable technologies gain prominence in clinical and remote health applications, the adoption of secure, scalable, and transparent data infrastructures—such as the one proposed in this study—will be instrumental in ensuring the reliability, privacy, and integrity of next-generation digital healthcare systems.

Declaration of Competing Interests

The authors declare no known competing financial interests or personal relationships.

Funding Declaration

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Author Contributions

Shaharkar Bhushan Bharat: Methodology, Validation, Investigation, Writing – Original Draft; **Manoj E. Patil**: Conceptualization, Data Analysis, Writing – Review and Editing

References

[1] S. Gupta, P. Chithaluru, T. Stephan, S. Nafisa, and S. Kumar, "Hspbci: a robust framework for secure healthcare data management in blockchain-based iot systems," *Multimedia Tools and Applications*, pp. 1–25, 2024.

[2] L. Khajehzadeh, H. Barati, and A. Barati, "A lightweight authentication and authorization method in iot-based medical care," *Multimedia Tools and Applications*, pp. 1–40, 2024.

[3] A. Altherwi, M. T. Ahmad, M. M. Alam, H. Mirza, N. Sultana, A. A. Pasha, N. Sultana, A. I. Khan, M. M. Alam, and R. Azim, "A hybrid optimization approach for securing cloud-based e-health systems," *Multimedia Tools and Applications*, pp. 1–36, 2024.

[4] S. Ray, K. N. Mishra, and S. Dutta, "Security enhancements in m-health using distributed ledger technology-based digital locker system," *International Journal of Information Technology*, vol. 16, pp. 4253–4271, 2024.

[5] S. Ray, K. N. Mishra, and S. Dutta, "Security enhancements in m-health using distributed ledger technology based digital locker system," *International Journal of Information Technology*, vol. 16, no. 7, pp. 4253–4271, 2024.

[6] H. A. Al-Ghuraybi, M. A. AlZain, and B. Soh, "Ensuring authentication in medical cyber-physical systems: A comprehensive literature review of blockchain technology integration with machine learning," *Multimedia Tools and Applications*, vol. 83, no. 12, pp. 35673–35707, 2024.

[7] P. Rastogi, D. Singh, and S. S. Bedi, "An improved blockchain framework for orap verification and data security in healthcare," *Journal of Ambient Intelligence and Humanized Computing*, vol. 15, no. 6, pp. 2853–2868, 2024.

[8] H. Idrissi and P. Palmieri, "Agent-based blockchain model for robust authentication and authorization in iot-based healthcare systems," *The Journal of Supercomputing*, vol. 80, no. 5, pp. 6622–6660, 2024.

[9] S. Pandey and B. Bhushan, "Recent lightweight cryptography (lwc) based security advances for resource-constrained iot networks," *Wireless Networks*, vol. 30, no. 4, pp. 2987–3026, 2024.

[10] Y. Harbi, K. Medani, and C. Gherbi, "A systematic literature review of blockchain technology for internet of drones security," *Arabian Journal for Science and Engineering*, vol. 48, pp. 1053–1074, 2023.

[11] K.-T. Zhu, Y. Wu, R. Yang, and Q. Yuan, "Anomaly detection in metaverse healthcare and fitness: bigdata analytics using 6g-enabled internets of things," *Wireless Personal Communications*, pp. 1–20, 2024.

[12] A. Awasthi, R. Suchithra, A. Chakravarty, J. Shah, D. Ghosh, and A. Kumar, "Machine learning-based d2d communication for a cloud-secure e-health system and data analysis by feature selection with classification," *Soft Computing*, pp. 1–14, 2023.

[13] S. Ksibi, F. Jaidi, and A. Bouhoula, "A comprehensive study of security and cyber-security risk management within e-health systems: Synthesis, analysis and a novel quantified approach," *Mobile Networks and Applications*, vol. 28, no. 1, pp. 107–127, 2023.

[14] P. K. Pal, M. Singh, and P. K. Mishra, "Fortified iot-fog framework for enhanced healthcare intelligence," *Multimedia Tools and Applications*, pp. 1–34, 2024.

[15] S. M. Patil, B. S. Dakhare, S. M. Satre, and S. D. Pawar, "Blockchain-based privacy preservation framework for preventing cyberattacks in smart healthcare big data management systems," *Multimedia Tools and Applications*, pp. 1–20, 2024.

[16] S. Garg, R. K. Kaushal, and N. Kumar, "A novel design and performance assessment of a blockchain-powered remote patient monitoring system," *SN Computer Science*, vol. 5, no. 7, p. 849, 2024.

[17] S. Atiewi, A. Al-Rahayfeh, M. Almiani, A. Abuhussein, and S. Yussof, "Ethereum blockchain-based three factor authentication and multi-contract access control for secure smart home environment in 5g networks," *Cluster Computing*, vol. 27, no. 4, pp. 4551–4568, 2024.

[18] D. K, N. S, and A. A, "Security analysis and trends in signcryption for wban: A research study," *Peer-to-Peer Networking and Applications*, 2024.

[19] D. Balakrishnan and T. D. Rajkumar, “Enhanced mayfly with active elite approach clustering based deep q learner routing with ebrlwe for iot-based healthcare monitoring system,” *Multimedia Tools and Applications*, vol. 83, no. 39, pp. 87129–87152, 2024.

[20] A. K. Ranjan and P. Kumar, “Ensuring the privacy and security of iot-medical data: a hybrid deep learning-based encryption and blockchain-enabled transmission,” *Multimedia Tools and Applications*, vol. 83, no. 33, pp. 79067–79092, 2024.

[21] C. Krishna, D. Kumar, and D. S. Kushwaha, “A comprehensive survey on pandemic patient monitoring system: Enabling technologies, opportunities, and research challenges,” *Wireless Personal Communications*, vol. 131, pp. 2125–2172, 2023.