A Systematic Review of Blockchain and Metaheuristic Algorithms for Secure and Scalable Healthcare Systems

Karam Hatem Alkhater[1,2,*], Mohana Shanmugam[3], Pritheega Magalingam[4]

[1]Department of Computer Engineering Techniques, College of Technical Engineering, University of Al Maarif, Al Anbar, 31001, Iraq

[2]Department of Information & Communication Technology, College of Graduate Studies, Universiti Tenaga Nasional, Selangor, Malaysia

[3]Department of Informatics, College of Computing and Informatics, Universiti Tenaga Nasional, Selangor, Malaysia

[4]Faculty of Artificial Intelligence, Universiti Teknologi Malaysia (UTM), Kuala Lumpur, Malaysia

Emails: KaramKhater.92@gmail.com; mohana@uniten.edu.my; mpritheega.kl@utm.my

Abstract

The integration of blockchain technology and metaheuristic optimization has transformed healthcare systems by improving security, scalability, and data interoperability. Blockchain ensures decentralization, immutability, and privacy, making it a viable solution for electronic medical records (EMRs) and secure healthcare data management. Meanwhile, metaheuristic algorithms optimize blockchain networks by enhancing transaction efficiency, consensus mechanisms, and real-time medical data processing. This paper systematically reviews recent advancements in blockchain and metaheuristics for healthcare applications. We discuss existing privacy-preserving models, AI-driven optimization techniques, and hybrid consensus mechanisms, addressing their strengths and limitations. Through a structured methodology, we analyze research trends, security challenges, and computational bottlenecks. This study encompassed 300 research articles from nine global databases. Then, inclusion and exclusion criteria were applied, leading to the exclusion of 144 studies and the retention of 156 studies. Subsequently, quality assessments were conducted, resulting in the final inclusion of only 8 studies for data extraction. A three-phase methodology was followed: planning, conducting, and reporting. The studies covered the period from January 2020 to January 2025, and 10 evaluation questions were used to assess the quality of the studies. Our findings reveal that while blockchain enhances data security and interoperability, metaheuristic-driven AI further optimizes system efficiency. However, challenges such as scalability constraints, energy consumption, regulatory compliance, and AI-based cyber threats remain significant. Future research should focus on developing lightweight blockchain architectures, quantum- resistant cryptographic models, and federated AI-enhanced security frameworks to address these issues. By leveraging advanced blockchain and AI-driven metaheuristics, healthcare systems can achieve greater resilience, efficiency, and adaptive security.

Keywords: Blockchain; Metaheuristics; Healthcare Security; Optimization; AI-driven Security; Electronic Medical Records (EMRs); Data Privacy; Consensus Mechanisms

1. Introduction

Advancements in informatics have significantly enhanced healthcare delivery, despite existing challenges [1]. Modern healthcare systems are increasingly shifting towards patient-centric applications [2]. Patients are no longer restricted to receiving medical care solely from specific hospitals. This is particularly crucial in emergencies or when a patient is unconscious, as the exchange of medical records plays a vital role in ensuring effective treatment [3]. Tracking a patient's medical history becomes essential for accurate diagnosis and treatment planning [4]. Therefore, the implementation of electronic medical records (EMRs) is necessary. However, patient medical records and histories are often inaccessible to medical professionals outside the institutions where these records were originally created [5]. Additional challenges

DOI: https://doi.org/10.54216/FPA.210105
Received: February 05, 2025 Revised: May 22, 2025 Accepted: July 01, 2025

include: (a) ineffective coordination of care, (b) lack of telemedicine support, despite the ability of patients to access and control their medical data [6, 7, 8], (c) risks of data tampering, theft, or mishandling [9], and (d) unauthorized exchange of medical records with healthcare providers, with or without patient consent [10, 11, 12]. The implementation of EMRs necessitates addressing critical issues such as data exchange interoperability, confidentiality, privacy, and security.

Traditional approaches to the collection, storage, and processing of electronic health records often rely on centralized systems, which pose significant risks, including data breaches and cyber- attacks that compromise data availability [13, 14, 15]. Blockchain technology is emerging as a solution to these issues due to its immutability, which prevents unauthorized data modification. Integrating blockchain in healthcare can enhance user trust and ensure secure dissemination of sensitive medical information [16, 17]. Blockchain technology offers several advantages, such as enhanced transparency, improved authentication, and consensus-based verification, which contribute to secure record-sharing mechanisms [18]. In addition to addressing key challenges in healthcare, blockchain presents opportunities for businesses to integrate it with other emerging technologies for improved efficiency [19, 20]. However, beyond interoperability, the absence of standardized frameworks for developing blockchain-based healthcare applications remains a critical concern that must be addressed to facilitate a structured approach for researchers and healthcare practitioners [21, 22, 23].

Blockchain technology functions as an incorruptible and distributed database, maintained and validated across a network of interconnected nodes worldwide [24, 25]. Unlike traditional databases, blockchain enhances security by timestamping data to prevent unauthorized modifications [26]. There are multiple types of blockchain, including private/permissioned, public/permissionless, consortium, and hybrid blockchains, each with its unique applications, benefits, and limitations [27]. In this study, we adopt a permissioned blockchain due to its enhanced security measures. The permissioned blockchain: (a) enables controlled access, ensuring that only authorized stakeholders can view patient medical records, (b) facilitates identity verification and customization, allowing access only to verified stakeholders instead of relying on peer approval, (c) operates with known participants, ensuring high fault tolerance and continuous system functionality, (d) achieves higher transaction throughput since participants are preselected, and (e) consumes less energy for mining and transaction processing [28]. Additionally, the permissioned blockchain model simplifies security protocols by restricting access to designated stakeholders, including patients, medical professionals, healthcare administrators, and medical institutions, ensuring secure exchange and management of medical records.

In addition, an important type of blockchain is the public blockchain that can be completely decentralized and availed by everyone. It uses consensus mechanisms such as proof-of-work and proof- of-stake to validate transactions. In addition, public blockchains are permissionless, which means any participant can access and validate data [29]. Whereas the consortium blockchain brings a closer environment, where different organizations should manage their networks effectively but can allow data transfers and mine as well. The hybrid blockchain is a type that combines both public and private blockchains and provides greater control without sacrificing decentralization. It offers better security than public blockchains but not better privacy from what private blockchains offer. The merit of hybrid blockchains is to provide greater integrity, transparency, and security while restricting access to sensitive data [29].

Metaheuristic algorithms have attracted attention in blockchain-based healthcare systems because of their optimization capability for securely and efficiently processing big medical data. Genetic algorithms, particle swarm optimization, and swarm intelligence, to name a few, optimize consensus mechanisms, improve fault tolerance, reduce transaction latency, and enhance blockchain networks. Metaheuristics in healthcare supports safe and effective patient data management in healthcare, allows rapid access, processing and credentials of health records with privacy. Combining metaheuristic optimization and blockchain can enhance healthcare interoperability, improve scalability, and offer greater resilience against single points of failure, leading to more robust and adaptive systems for managing patient data. The main contributions of this study are:

1. Inspired by the development in the field, this paper conducts a comprehensive survey of the recent research on the combination of blockchain and metaheuristic optimization in healthcare, from January 2020 to January 2025.
2. The paper assesses existing privacy-preserving schemes, AI-driven optimization approaches and hybrid consensus models to highlight strengths and weaknesses to serve as secure healthcare data management.
3. It describes the principles that drive decentralisation, immutability, privacy, and interoperability in EMRs and similar healthcare systems using blockchain.

2. Related Works

As seen in our methodology, only **8** articles were obtained after applying the defined filtering criteria. This section reviews existing research related to Blockchain, Metaheuristics, and E-Health, focusing on their contributions to security, optimization, and healthcare applications.

DOI: https://doi.org/10.54216/FPA.210105
Received: February 05, 2025 Revised: May 22, 2025 Accepted: July 01, 2025

Several studies have explored the role of Blockchain in securing the Internet of Medical Things (IoMT) and improving healthcare cybersecurity. These studies introduce hybrid metaheuristic models to dynamically optimize security mechanisms and enhance performance in real-time health- care monitoring.

The work done in [30] the authors proposed a hybrid metaheuristic model, which works to secure and improve the IoMT. With the incorporation of Blockchain technology, the model employs Elephant Herding Optimization (EHO) and Grey Wolf Optimization (GWO) to follow a programmed set of instructions in changing encryption and hashing standards in response to any recognized security threats. We evaluated the model under multiple attacks such as DDoS, man- in-the-middle, masquerading, and Sybil attacks. Specifically, the performance evaluation results indicate 8.7%, 6.4%, 8.2%, and 9.4% of enhancements in the network stability, network consistency, throughput, packet delivery ratio, as well as attack detection and mitigation rate through POC. We conclude that such a combination of metaheuristic optimization with the blockchain can provide suitable solutions for enhancing quality assurance and security on real-time health care monitoring systems.

A different research avenue explores trust management and cryptographic approaches in IoT safety. Due to resource limitations and the risk of routing attacks, ensuring secure data transmission in interconnected medical devices is still challenging.

In [31] A trust management model for IoT security is proposed in which the combinations of cryptographic algorithms and Meta heuristic-based key management. Propositions: The proposed approach combines RSA encryption with Self-Adaptive Tasmanian Devil Optimization (SA-TDO) for optimal key generation and Secure Hash Algorithm 3-512 (SHA3-512) to ensure security in IoT communication. Additionally, a Real-time Convolutional Spiking Neural Network (CSNN) based Intrusion Detection System (IDS) optimized using the Archimedes Optimization Algorithm (AOA) was developed. Simulation results showed that the presented method was both highly secure, achieving accuracy, precision, and false positive at 98.94%, 98.88%, and 3.43% respectively, and capable of extremely low computational overhead.

Data integrity and privacy protection has been a critical concern as electronic health record (EHR) adoption rises. To mitigate these issues, researchers have investigated blockchain-enabled EHR systems utilizing AI-inspired authentication and encryption methods.

The authors of [32] proposed a privacy preserving EHR system based on blockchain, and AI based authentication techniques. The novel architectures of Merkle Tree structures allow for their authenticated glow to be verified with ease, ensuring the veracity of the latter's authentication as they are generated using the Iteration-Based Firefly Reptile Search Algorithm (IFRSA), the latter ensuring the minimal computational expense in cryptographic key generation and authentication. Additionally, the model improves privacy protection by implementing a multi-objective optimization method incorporating the Euclidean distance, hiding ratio, and data preservation ratio of both encrypted and original medical records. By doing so, it is able to provide secure data sanitization and restoration while making EHR systems privacy aware, resilient and reliable.

Despite the traditional security measures, other researchers used Blockchain and Deep Learning models as security solutions in IoT and healthcare.

In [33] the authors developed an Enhanced Metaheuristic with Deep Learning Model for Blockchain-Assisted Cybersecurity Solutions (EMDLM-BCCS) in IoT environments. The model utilizes Extreme Learning Machines (ELM) and the Elite-Oppositional Grasshopper Optimization Algorithm (EGOA) to optimize the detection of DDoS attacks in IoT networks. Performance evaluation using the BoTIoT dataset showed superior attack mitigation, demonstrating higher accuracy in detecting malicious traffic while reducing false alarms. The findings suggest that combining Deep Learning and Metaheuristics in blockchain-based cybersecurity frameworks can significantly enhance IoT security.

Supply chain management in healthcare, particularly blood supply chains, has also benefited from blockchain integration. Recent studies emphasize using simulation-optimization frameworks to enhance transparency and resource allocation in healthcare logistics.

In [34] the study introduced a Blockchain-based Blood Supply Chain model utilizing a bi- objective optimization framework. The proposed system integrates Data Envelopment Analysis (DEA) with a simulation-optimization approach to improve the efficiency of blood distribution among hospitals. By analyzing factors such as service quality, hospital efficiency, and donor behavior, the study demonstrated that blockchain technology enhances traceability and donor participation, increasing donation rates by 6%, 3%, and 12% under various conditions.

The security of electronic health records (EHRs) remains a major challenge, especially with increasing cyber threats targeting patient data privacy. Researchers also have proposed certain privacy enhancing through Blockchain based access control mechanisms.

DOI: https://doi.org/10.54216/FPA.210105
Received: February 05, 2025 Revised: May 22, 2025 Accepted: July 01, 2025

In [35] the authors synthesized blockchain in safeguarding the healthcare data and that it is potential in alleviating the cyber security risks in EHR systems. It proposed privacy-aware smart contracts and authentication methods based on zero-knowledge proofs to improve patient data protection. Overall, the results indicate that a blockchain-based mechanism provides a robust solution for secure transfer of medical data across multiple domains, while maintaining compliance with the regulatory considerations and minimizing risk of unauthorized data access.

The emerging areas of energy-efficient blockchain storage and processing have been well studied in research, especially in WSNs for healthcare applications.

In [36] the work studied minimizing energy consumption in relation to the database in a WSN based on blockchain. The new system improves the storage efficiency of the blockchain while ensuring the safety of the data being transmitted by examining spatial–temporal correlation characteristics. These results suggest that network node distribution optimization may greatly decrease processing overhead and enhance the execution time, while making the blockchain storage less vulnerable and more energy efficient.

The introduction of Blockchain with Adaptive Deep Learning for secure IoT-based healthcare data storage is also a recent movement in the research field.

In [37] Proposed A Secure IoT-Based Health Care Data Storage System Using Blockchain and Deep Learning Models. The system combines an Adaptive Dilated Long Short-Term Memory with Attention Network (AD-LSTM-AN) for trust verification and a Hybrid Elliptical Curve Cryptography with Attribute Based Encryption (HECC- ABE) for data encryption. Apart from that, the Golden Eagle-Harris Hawks Optimization (AFP-GEHHO) approach was used for key management. The Experiments simulations were performed, which shows that the proposed model obtained the accuracy of 96%, which is significantly helpful in data security, and efficiency of retrieval process.

The studies reviewed illustrate important developments within the areas of Blockchain, Meta- heuristics and E-Health security and optimization. Blockchain has well-established properties in terms of data integrity, decentralization, and access control. Metaheuristics are essential in optimizing security models, minimizing computational overhead, and maximizing threat detection mechanisms. The integration of AI-driven optimization further strengthens real-time security, interoperability, and efficiency in blockchain-based healthcare applications.

These findings indicate that future research should focus on scalable and adaptive blockchain frameworks, integrating advanced metaheuristic techniques to enhance security, privacy, and overall system performance in healthcare environments.

Table 1: Summary of Related Work in Blockchain, Metaheuristics, and E- health

Ref	Focus Area	Proposed Method	Key Contributions
[30]	IoMT Security	Hybrid Blockchain with Elephant Herding Optimization (EHO) and Grey Wolf Optimization (GWO)	Improved network consistency (8.7%), throughput (6.4%), packet delivery (8.2%), and attack detection (9.4%). Enhanced adaptability against security threats.
[31]	IoT Security	Cryptographic-based Trust Management Model using RSA encryption, Self-Adaptive Tasmanian Devil Optimization (SA-TDO), and SHA3-512	Secure data exchange with 98.94% accuracy, reduced false positives (3.43%), and real-time threat detection using Deep Learning Intrusion Detection System (DNN-IDS).
[32]	Privacy-Preserving EHRs	Blockchain-based Electronic Health Records (EHR) model with Merkle Tree authentication and Firefly Reptile Search Algorithm (IFRSA) for key management	Secure EHR sharing and privacy preservation, using multi-objective optimization (Euclidean distance, hiding ratio, data preservation ratio).

DOI: https://doi.org/10.54216/FPA.210105
Received: February 05, 2025 Revised: May 22, 2025 Accepted: July 01, 2025

[33]	Blockchain-Assisted IoT Cybersecurity	Extreme Learning Machines (ELM) with Elite-Oppositional Grasshopper Optimization Algorithm (EGOA) for DDoS attack detection	Improved cybersecurity with high attack detection rates, reducing false alarms and improving network resilience. Tested on BoT-IoT dataset.
[34]	Blood Supply Chain Management	Blockchain-based Bi-Objective Optimization Model integrating Data Envelopment Analysis (DEA) for healthcare logistics	Optimized blood distribution and donor management; increased traceability and donor participation (6%, 3%, 12%).
[35]	EHR Security	Zero-Knowledge Proofs and Privacy-Preserving Smart Contracts for securing medical data	Enhanced privacy, interoperability, and compliance with regulatory standards, reducing unauthorized access risks.
[36]	Energy-Efficient Blockchain Storage	Blockchain with Spatial–Temporal Correlation Analysis for Wireless Sensor Networks (WSNs)	Improved energy efficiency in blockchain- based storage, reducing computational overhead and improving execution time.
[37]	IoT-Based Healthcare Security	Adaptive Deep Learning Model using AD-LSTM-AN and Hybrid Elliptic Curve Cryptography (HECC-ABE)	Achieved 96% accuracy in secure healthcare data storage, optimizing encryption keys with AFP-GEHHO algorithm.

2.1 Blockchain Applications in Electronic Health Records (EHRs)

Blockchain technology has gained widespread attention for its ability to improve the integrity, traceability, and security of Electronic Health Records (EHRs). In recent years, researchers have focused on leveraging blockchain to eliminate centralized data silos and enable secure record sharing across healthcare institutions. For instance, [32] proposed a privacy-preserving EHR system utilizing Merkle Tree structures for authentication and key management through the Iteration-Based Firefly Reptile Search Algorithm (IFRSA). This solution demonstrated effective data sanitization while preserving the integrity and confidentiality of medical records.

In another approach, [35] presented a blockchain framework incorporating smart contracts and zero-knowledge proofs to protect patient data from unauthorized access. These smart contracts autonomously enforce access rules, and zero-knowledge proofs verify identity without revealing private information. These studies collectively highlight the effectiveness of blockchain in safeguarding sensitive healthcare information while enhancing transparency and patient control over their data.

Despite these advancements, most solutions focus primarily on privacy and access control without addressing challenges related to large-scale EHR management, such as performance under high transaction loads or real-time responsiveness. Furthermore, current models do not offer sufficient optimization mechanisms to minimize the energy consumption and computational complexity associated with blockchain operations in healthcare. There is a need for more comprehensive architectures that combine blockchain with computational intelligence to meet both security and scalability requirements.

2.2 Metaheuristic Optimization in Healthcare Systems

Metaheuristic algorithms have been widely used in healthcare systems to optimize complex, multi- dimensional problems such as medical scheduling, resource allocation, and diagnostic processes. These algorithms, inspired by natural phenomena, offer flexible and adaptive solutions for dynamic environments. In [34], a bi-objective optimization model integrating Data Envelopment Analysis (DEA) with blockchain was proposed for efficient blood supply chain management. The model demonstrated enhanced traceability and donor participation through improved allocation strategies.

DOI: https://doi.org/10.54216/FPA.210105
Received: February 05, 2025 Revised: May 22, 2025 Accepted: July 01, 2025

Similarly, [31] introduced a trust management model for IoT healthcare using RSA encryption and the Self-Adaptive Tasmanian Devil Optimization (SA-TDO) for cryptographic key generation. The integration of metaheuristics ensured secure data communication while minimizing the overhead involved in encryption processes. These studies demonstrate the potential of metaheuristics in boosting operational efficiency, reducing computational time, and enabling secure and scalable healthcare applications.

Nevertheless, most existing works apply metaheuristics in isolated use cases without considering system-level integration with blockchain technology. Optimization methods are often limited to enhancing individual modules (e.g., key generation or scheduling), rather than addressing the holistic demands of blockchain-based healthcare systems. Moreover, the performance of these algorithms under adversarial conditions or real-time constraints remains underexplored, indicating a significant research opportunity in developing metaheuristic frameworks tailored for secure, distributed environments.

2.3 Hybrid Blockchain-Metaheuristic Models for Security Enhancement

Hybrid frameworks combining blockchain and metaheuristic algorithms have shown promise in addressing the limitations of conventional healthcare cybersecurity solutions. For instance, [30] introduced a model employing Elephant Herding Optimization (EHO) and Grey Wolf Optimization (GWO) to dynamically adjust encryption and hashing rules in response to emerging threats. The integration of metaheuristics enhanced adaptability, resulting in higher throughput, packet delivery ratio, and threat mitigation rates under simulated attack conditions.

Additionally, the work in [33] utilized the Elite-Oppositional Grasshopper Optimization Algorithm (EGOA) with Extreme Learning Machines (ELM) to develop a blockchain-assisted cybersecurity solution. This framework demonstrated superior DDoS detection capabilities in IoT environments, significantly reducing false alarms while maintaining high classification accuracy.

These findings suggest that combining metaheuristics with blockchain can enhance the responsiveness and resilience of healthcare systems against cybersecurity threats.

However, these hybrid models tend to be narrow in scope, often focusing on specific attack scenarios or localized security functions. Their scalability to large, heterogeneous healthcare infrastructures with varying compliance and interoperability requirements is rarely evaluated. Moreover, the integration of such models into real-time data environments remains a challenge, especially considering the processing latency introduced by complex optimization algorithms. This calls for the design of lightweight, adaptive hybrid architecture with generalizable security guarantees.

2.4 AI-Driven Security and Anomaly Detection in IoT Healthcare Net- works

AI-enhanced models have gained momentum in securing IoT-enabled healthcare systems, where massive amounts of heterogeneous sensor data must be processed and protected in real-time. The study in [37] introduced a model combining Adaptive Dilated LSTM with Attention Networks (AD- LSTM-AN) for trust verification, supported by a Hybrid Elliptical Curve Cryptography (HECC- ABE) encryption layer. The framework achieved 96% accuracy in healthcare data authentication and efficient encryption key management using Golden Eagle-Harris Hawks Optimization.

Further, [33] demonstrated that integrating Deep Learning with metaheuristics into a blockchain system for intrusion detection could significantly reduce false positives and improve threat classification. Their architecture, designed around Extreme Learning Machines (ELM), displays the benefit of AI in processing complex attack patterns while ensuring low-latency detection. These studies reveal that AI models can enhance system responsiveness and support intelligent threat management in smart healthcare networks.

Despite their potential, such AI-driven models often require substantial computational re- sources, limiting their deployment in constrained medical IoT environments. In addition, the integration between deep learning models and blockchain's immutable and distributed nature is not fully optimized, particularly when real-time anomaly detection and data encryption are jointly required. Future work should explore federated AI models and edge-level optimization techniques to reduce computational burdens while maintaining detection accuracy.

2.5 Privacy-Preserving Techniques and Cryptographic Advances

Protecting patient privacy remains a central theme in healthcare blockchain research. Several works have proposed advanced cryptographic mechanisms such as attribute-based encryption, zero-knowledge proofs, and secure hash functions to ensure data confidentiality. In particular, [35] introduced privacy-aware smart contracts and access controls using zero-knowledge proofs, which authenticate users without revealing sensitive identity information. This approach supports compliance with data protection regulations like GDPR and HIPAA.

DOI: https://doi.org/10.54216/FPA.210105
Received: February 05, 2025 Revised: May 22, 2025 Accepted: July 01, 2025

Another significant contribution is the work in [31], where Secure Hash Algorithm 3-512 (SHA3- 512) and RSA-based encryption were paired with Self-Adaptive metaheuristics for key management. This model ensured data confidentiality during IoT communication, while achieving strong accuracy and low false-positive rates in threat detection. Similarly, [32] employed a multi-objective optimization approach to preserve the hiding ratio and Euclidean distance between encrypted and original data in EHR systems.

While these methods are effective in theory, their deployment in practical systems raises concerns about scalability and computational efficiency. Many privacy-preserving algorithms involve high overhead due to encryption/decryption and verification stages, making them unsuitable for real-time applications. Furthermore, few studies explore post-quantum cryptographic models that are essential for long-term data security. More research is needed to design lightweight, scalable, and future-proof cryptographic techniques for healthcare blockchain systems.

2.6 Energy Efficiency and Scalability in Blockchain-Based Systems

Blockchain networks, particularly those using traditional consensus mechanisms like Proof-of-Work (PoW), are known for their high-energy consumption. This is especially problematic in healthcare systems where resources are limited, and latency must be minimized. In [36], a novel approach using spatial–temporal correlation analysis was proposed to reduce blockchain processing overhead in Wireless Sensor Networks (WSNs). The study demonstrated that optimizing node distribution could enhance energy efficiency and minimize execution time.

The need for sustainable blockchain implementations has also led to research on lightweight consensus protocols and energy-aware smart contracts. Although some proposals aim to replace PoW with Proof-of-Stake (PoS) or delegated mechanisms, many healthcare applications still lack consensus models optimized for real-time decision-making. Further exploration into energy-efficient architecture remains essential, particularly for IoT-connected medical devices and portable systems.

Existing solutions often lack support for heterogeneous devices and varying network conditions in healthcare settings. Moreover, while energy efficiency has been addressed in some studies, the trade-offs with scalability, fault tolerance, and data throughput are not well understood. Future research should focus on cross-layer optimization strategies that consider energy, latency, and throughput holistically to enable truly efficient and scalable blockchain-based healthcare infrastructures.

2.7 Limitations of Current Methods and Identified Research Gaps

Although many studies offer effective models for privacy, security, and optimization in healthcare, several critical gaps persist. First, the siloed approach to blockchain and metaheuristics has resulted in fragmented solutions that lack interoperability and unified frameworks. Hybrid systems integrating blockchain with optimization and AI models often suffer from complexity and poor scalability in real-world healthcare environments.

Second, many proposed solutions are evaluated using synthetic datasets or simulations without practical deployment or validation in clinical settings. This limits their generalizability and fails to capture the dynamic and compliance-driven nature of healthcare operations. Moreover, few studies explicitly consider regulatory standards or real-time requirements when designing blockchain-based architectures, creating a gap between theory and implementation.

Finally, emerging threats like adversarial AI attacks and quantum computing are not addressed in most current frameworks. Future studies should prioritize resilience by incorporating adaptive cryptographic techniques, federated learning, and post-quantum security standards. Addressing these limitations will enable the development of robust, secure, and intelligent blockchain-powered systems capable of transforming digital healthcare ecosystems.

3 Methodology

This segment outlines the methodology used in this research, addressing the major steps taken during the study. The methodology consists of three core phases: Planning, Conducting, and Reporting. These phases and their components are illustrated in Figure 1.

DOI: https://doi.org/10.54216/FPA.210105
Received: February 05, 2025 Revised: May 22, 2025 Accepted: July 01, 2025

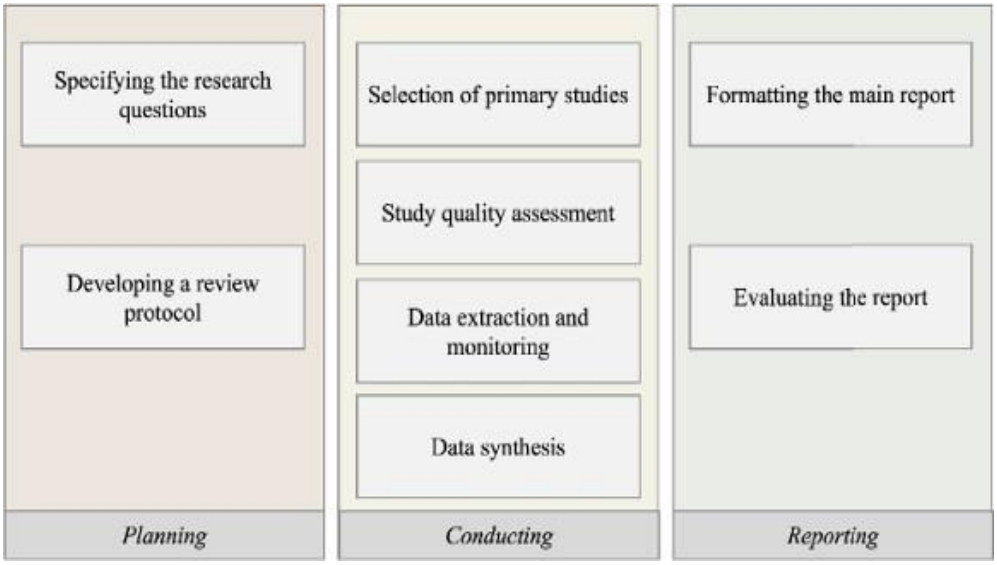

Figure 1. The systematic review process, structured into three phases: Planning, Conducting, and Reporting. The Planning phase involves defining research questions and developing a review protocol. The Conducting phase encompasses the selection of primary studies, study quality assessment, data extraction, and synthesis. The Reporting phase includes report formatting and evaluation.

Only metaheuristic algorithms have gained significant attention to dealing with such complex optimization problems in blockchain-based healthcare-based systems. In addition, these algorithms enhance efficiency, adaptability, and robustness of processing high-scale medical records securely. Data integrity, transparency, and privacy are assured by blockchain, making it essential for electronic medical record management in healthcare. This chapter discusses how metaheuristic techniques can be integrated with blockchain to optimize consensus mechanisms, improve transaction processing, and enhance fault tolerance in distributed healthcare networks.

This approach ensures secure and efficient patient data management through blockchain and metaheuristic optimization methods while ensuring privacy and interoperability among healthcare institutions. By utilizing the decentralized architecture of blockchain in conjunction with the adaptability and approach of metaheuristic methods, not only do healthcare systems benefit from an increase in security and a decrease in computational costs but also provide easier accessibility to medical information. Figure 2 illustrates the study selection process followed in this systematic review. The process begins with formulating the research questions, followed by defining the search strategy, which includes specifying search terms and identifying literature resources. The search process is conducted across multiple digital libraries, such as ACM Digital Library, IEEE Xplore, ScienceDirect, Springer, MDPI, Hindawi, Wiley, Emerald, and Taylor and Francis.

The search process initially retrieves **300** studies. These studies are then filtered based on inclusion and exclusion criteria, reducing the number to **156**. A further screening process involves scanning the full papers, narrowing down the selection to **40** studies. After applying quality assessment (QA) rules, only **8** studies meet the criteria for data extraction.

Following the selection process, data is extracted from these **8** studies. Figure 2 also includes a decision point labeled "Done Extraction?" to ensure completeness. If the extraction process is incomplete, further review is performed; otherwise, the data synthesis phase is initiated.

DOI: https://doi.org/10.54216/FPA.210105
Received: February 05, 2025 Revised: May 22, 2025 Accepted: July 01, 2025

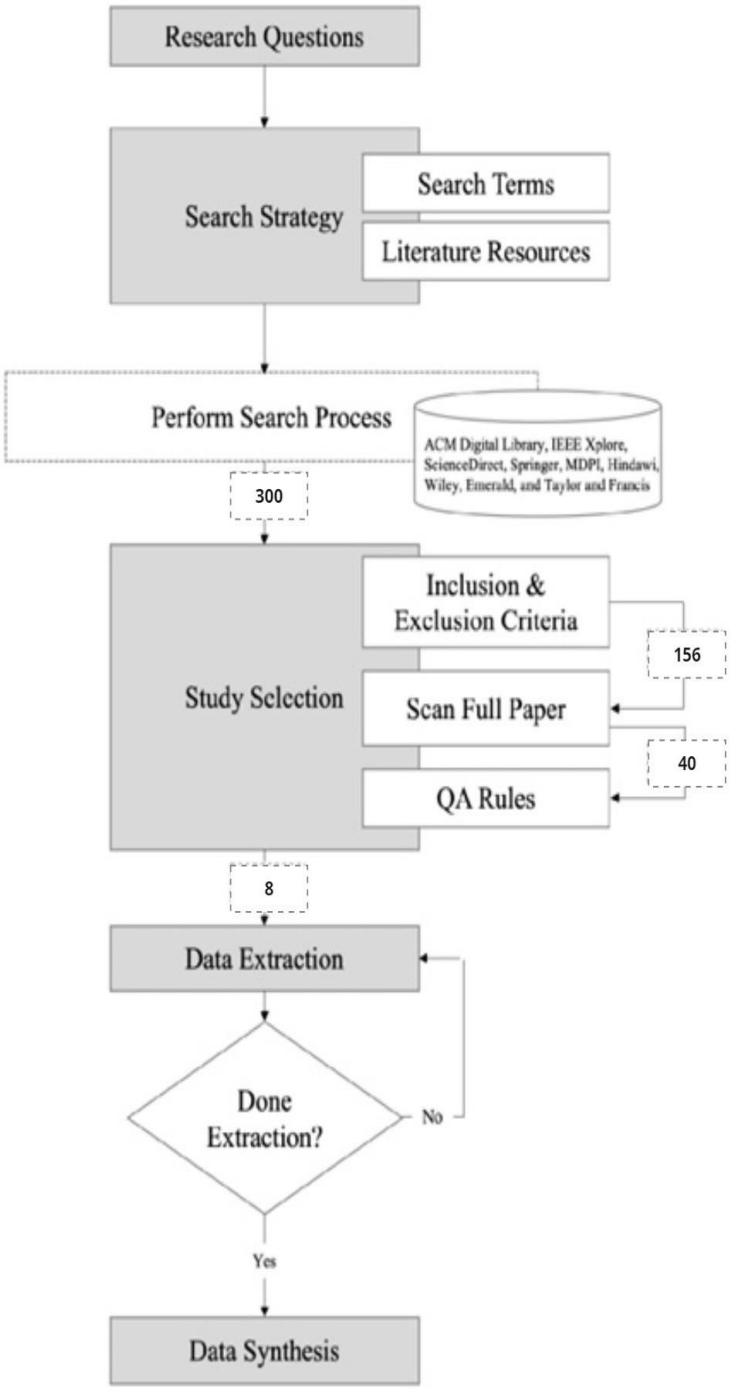

Figure 2. Study selection process in the systematic review. The process involves defining research questions, performing a search strategy, selecting studies based on inclusion and exclusion criteria, scanning full papers, applying quality assessment rules, extracting data, and proceeding to data synthesis. The numbers represent the count of studies at each filtering stage.

4 Research Questions

This study aims to address key research questions related to the integration of blockchain and metaheuristic optimization in healthcare. Table 1 presents the research questions (RQ) along with their descriptions.

DOI: https://doi.org/10.54216/FPA.210105
Received: February 05, 2025 Revised: May 22, 2025 Accepted: July 01, 2025

Table 1: Research Questions and Their Descriptions

RQ	Description
RQ1	How can blockchain technology improve the security and privacy of electronic medical records (EMRs) in healthcare systems?
RQ2	What are the advantages of integrating metaheuristic algorithms in optimizing blockchain performance for healthcare applications?
RQ3	How does the adoption of blockchain enhance interoperability and data ex- change among different healthcare institutions?
RQ4	What are the challenges and limitations associated with implementing blockchain and metaheuristics in healthcare environments?
RQ5	What are the potential improvements in healthcare data management when combining blockchain with AI-driven metaheuristic techniques?

The research questions outlined in Table 1 guide this study's investigation into blockchain-based healthcare solutions, focusing on security, optimization, interoperability, challenges, and potential improvements.

5 Search Strategy

The search strategy is designed to systematically identify relevant literature related to blockchain, metaheuristics, and healthcare. The methods involve formulating search terms, choosing suitable digital databases, inclusion and exclusion criteria for narrowing down the search results.

a. Search Terms

Multiple search terms were used in conjunction with logical operators AND and OR to narrow query results to facilitate a thorough review. Search queries comprised of the following were applied for multiple digital databases:

i. (**Blockchain** AND **Healthcare**) OR (**Blockchain** AND **Medical Records**)

ii. (**Metaheuristics** AND **Blockchain**) OR (**Optimization** AND **Blockchain**)

iii. (**Blockchain** AND **Security** AND **Healthcare**) OR (**Blockchain** AND **Privacy**)

iv. (**Metaheuristic Optimization** AND **Healthcare**) OR (**AI-based Metaheuristics** AND **Medical Data**)

v. (**Interoperability** AND **Blockchain** AND **Healthcare**) OR (**Secure Data Exchange** AND **Blockchain**)

The following search terms were used to cover digital libraries, including ACM Digital Library, IEEE Xplore, ScienceDirect, Springer, MDPI, Hindawi, Wiley, Emerald, and Taylor & Francis, so that high-quality and peer-reviewed articles would also be included in the results.

AND narrows the search results by ensuring that all specified keywords are included in the retrieved studies. This OR operator expands the search to encompass a wider range of results, which is important to capture similar but marginally different terms.

b. Literature Resources

Relevant initial articles were retrieved using nine digital databases: ACM Digital Library, IEEE Xplore, ScienceDirect, Springer, MDPI, Hindawi, Wiley, Emerald, and Taylor and Francis. The search was limited from January 2020 to January 2025. Using the defined search terms across these resources provided an initial search of 300 articles across title, abstract and keywords. The number of articles retrieved from each resource is illustrated in Table 2.

DOI: https://doi.org/10.54216/FPA.210105
Received: February 05, 2025 Revised: May 22, 2025 Accepted: July 01, 2025

c. Data Strategy

The data collection process was performed to collect relevant studies that correspond to the research questions described in this study. Using the defined search strategy and filtering criteria, 300 selected articles have been analyzed in terms of their relevance to each research question.

The most significant number of studies were obtained for RQ1, which investigates the role blockchain technology can play in improving security and privacy in healthcare. A large number of the identified articles examined the role of blockchain in providing immutable, transparent, and decentralized records that could prove crucial to safeguarding patients' data and ensure secure electronic medical records (EMRs). This means that security and privacy are the most focused aspects of blockchain based healthcare applications and motivates extensive research in this field. RQ2 sought to examine the incorporation of metaheuristic algorithms in optimizing blockchain performance, revealing a considerable number of articles. The increasing interest concerning computational optimization approaches corresponds to the necessity of efficient blockchain consensus mechanisms, and lower computational overhead, and faster transaction processing times in health-care environments.

RQ3 had a moderate number of studies addressing the role of blockchain in interoperability and the exchange of data between health care institutions. It indicates that there will be a growing emphasis on secure and efficient data sharing while remaining compliant with regulations including HIPAA and GDPR. Smart contracts and decentralized identity verification have also been mentioned in various studies as key contributors to interoperability-enabled ecosystems.

The synthesis for RQ4 explored the challenges and limitations of using blockchain and meta- heuristics in healthcare, which highlighted issues of scalability, regulations and, computational complexity. Multiple works emphasize the energy-intensive nature of blockchain consensus mechanisms, the demand for efficient governance models, and the integration of emerging technologies, such as federated learning, that can help reduce computational overhead.

The selected studies for RQ5 showed that the combination of blockchain and AI-driven meta- heuristics to improve healthcare data management is a new, promising research area. The studies pointed out that the enhanced blockchain models gain an impetus with AI can provide immense value in fraud detection, predictive analysis, and automated decision-making in the healthcare system, keeping the security, and privacy intact.

Overall, blockchain for security and privacy is the area with the most studies, while optimization techniques metaheuristics is the alternately most used one. Nevertheless, AI-driven metaheuristics integrated with healthcare blockchain applications is a novel trend in literature, which requires further investigation to assess its impact and efficacy.

Table 2: Studies retrieved per digital resource at first search.

Digital Resource	**No. of Articles**
ACM Digital Library	45
IEEE Xplore	30
ScienceDirect	58
Springer	32
MDPI	48
Hindawi	10
Wiley	35
Emerald	20
Taylor and Francis	22
Total	**300**

DOI: https://doi.org/10.54216/FPA.210105
Received: February 05, 2025 Revised: May 22, 2025 Accepted: July 01, 2025

d. Quality Assessment Criteria

We used a specific set of quality assessment questions in order to select studies that would be considered reliable and relevant. The questions evaluate the methodological rigor, relevance, and contributions of studies within the domains of Blockchain, Metaheuristics, and E-Health. Table 3 presents the quality assessment questions used in this study.

Table 3: Quality assessment questions for Blockchain, Metaheuristics, and E-Health studies.

No.	Question
QA1	Are the objectives of the study clearly defined within the context of Blockchain, Metaheuristics, or E-Health?
QA2	Is the methodology for integrating Blockchain, Metaheuristics, or E-Health adequately described?
QA3	Does the study focus on optimization using Metaheuristics, security using Blockchain, or advancements in E-Health?
QA4	Are the techniques used for Blockchain data security, Metaheuristic optimization, or E-Health applications clearly stated?
QA5	Does the study provide a sufficiently large and relevant dataset for Blockchain transactions, Metaheuristic models, or E-Health applications?
QA6	Is the performance of the proposed approach (Blockchain security, Metaheuristic optimization, or E-Health framework) measured and reported?
QA7	Is the proposed approach compared with other related models in Blockchain, Metaheuristics, or E-Health?
QA8	Are the results of the study comprehensively reported and discussed in relation to its application domain?
QA9	Does the study discuss security, privacy, and performance concerns associated with Blockchain, Metaheuristics, or E-Health?
QA10	Does the study provide added value to research in Blockchain, Metaheuristics, or E-Health by addressing critical gaps?

e. Data Synthesis

The data synthesis phase involves summarizing, analyzing, and interpreting the selected studies to derive meaningful insights for this research. The extracted data were categorized based on their relevance to Blockchain, Metaheuristics, and E-Health, ensuring a structured evaluation of trends, challenges, and contributions.

A significant portion of the reviewed studies focused on the role of Blockchain in enhancing security, privacy, and interoperability within healthcare systems. These studies provided insights into decentralized architecture, consensus mechanisms, and smart contract implementations that facilitate secure medical data exchange.

Studies related to Metaheuristics primarily explored optimization techniques aimed at improving blockchain performance, reducing transaction latency, and enhancing fault tolerance. Commonly used metaheuristic approaches included Genetic Algorithms (GA), Particle Swarm Optimization (PSO), and Ant Colony Optimization (ACO), all of which contributed to enhancing computational efficiency in healthcare applications.

In the E-Health domain, research studies emphasized the integration of blockchain with health- care management systems to improve accessibility, transparency, and real-time decision-making. Many studies investigated the impact of blockchain-based electronic medical records (EMRs) on patient privacy, data sharing, and secure authentication.

DOI: https://doi.org/10.54216/FPA.210105
Received: February 05, 2025 Revised: May 22, 2025 Accepted: July 01, 2025

The synthesized data reveal that while blockchain's role in security and interoperability re- mains extensively explored, there is an emerging interest in leveraging AI-driven metaheuristics to further optimize blockchain-based healthcare applications. Additionally, interdisciplinary re- search combining these technologies is gaining momentum, indicating future trends toward secure, efficient, and intelligent healthcare solutions.

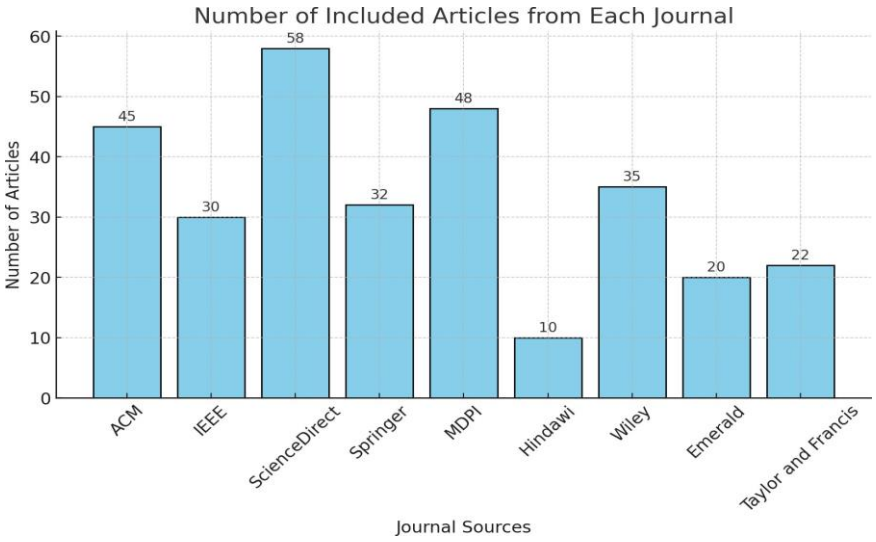

Figure 3. Number of included articles from each journal source

6 Challenges and Future Work

Despite significant advancements in Blockchain, Metaheuristics, and E-Health, several challenges remain that must be addressed to enhance security, efficiency, and scalability. This section outlines the major challenges identified in the reviewed studies and proposes potential future re- search directions.

a. Challenges

One of the primary challenges in integrating blockchain technology into healthcare is its high computational cost and scalability limitations. Blockchain-based healthcare systems require significant processing power, especially when dealing with large-scale electronic medical records (EMRs). Existing consensus mechanisms like PoW and PoS force a trade-off between security and computational power/spending, limiting real-time healthcare applications.

The other challenge is achieving interoperability between health care institutions. Blockchain increases data security and decentralization, but different hospitals or medical organizations work with different data formats, regulatory policies and system architectures. Integrating and sharing data across a variety of healthcare relationships as well as compliance with regulations such as HIPAA and GDPR presents an open research issue.

Security continues to be a huge challenge particularly in the context of upcoming cyber threats like DDoS attacks, data poisoning and adversarial AI attacks. Blockchain ensures information is immutable and encrypted; however, attackers still devise new methods to break through medical records and corrupt metaheuristic-based optimization functions. While increasingly utilizing AI- driven security frameworks, integrated with blockchain that could adapt security measures to cloud computing, this will necessitate further research.

Moreover, there is still a challenge of energy efficiency and sustainability for blockchain-based applications. Traditional Blockchain frameworks require massive energy, which is not suitable for energy-constrained IoT-based medical system environments. Additionally, lightweight consensus mechanisms, energy-efficient encryption, and green computing research need to be further explored to minimize blockchain's environmental footprint.

a. Future Work

Future research needs to develop scalable and lightweight blockchain architectures for healthcare applications to overcome these challenges. Researchers may experiment with choosing a hybrid consensus model that offers the best of PoW and PoS, but there is still more room for improvement. Methods like sharding, directed acyclic graphs (DAGs), and layer-2 solutions can be adopted to enhance the scalability of blockchain in the context of medical data storage.

DOI: https://doi.org/10.54216/FPA.210105
Received: February 05, 2025 Revised: May 22, 2025 Accepted: July 01, 2025

Another way to improve interoperability is through the implementation of standardized healthcare blockchain frameworks. Semantic ontologies, cross-chain communication protocols, and federated blockchain models could be used to achieve better integration of data across medical institutions. Future works should develop secure APIs and smart contract-based authorization models that improve cross-platform interoperability.

The incorporation of AI-based anomaly detection with the use of blockchain in real-time processing can benefit security by finding threats immediately in the data. For self-learning models of cybersecurity, federated learning and adversarial AI defenses can be integrated in order to build models that reconfigure themselves in response to the latest threats. In addition, privacy- preserving techniques such as homomorphic encryption, differential privacy, and zero-knowledge proofs (ZKPs) ought to be enhanced further to cater to healthcare blockchain applications.

Energy efficiency is still a critical research area, and more work should be done in building green blockchain solutions. To keep up with the workload blockchain would not be able to process without irreversible computation, lightweight cryptographic models and custom energy-efficient smart contracts will be necessary for blockchain sustainability for healthcare benefit.

Finally, future studies can investigate the viability of the quantum-resistant blockchain model and its compatibility with the secure long-term storage of medical data. As quantum computing advances, classical encryption techniques may be compromised. Meta-heuristic-optimized blockchain frameworks combined with post-quantum cryptographic algorithms may provide long-term security features.

7 Conclusion

A Power in Securing and Optimizing Healthcare Data Systems Blockchain can provide decentralized, transparent, and privacy-preserving solutions, making it an acceptable technology to store electronic medical records (EMRs), secure Internet of Things (IoT) networks, and manage patient data. On other hand, metaheuristic algorithms improve blockchain performance its optimizing consensus methods, accessing transaction latency, also processing live data. Our systematic review shows that the great potential security benefits of blockchain through mitigating cyber security threats like Distributed Denial of Service attacks (DDoS), data breaches and unauthorized access to data. AI-based metaheuristic optimization algorithms provide additional value to blockchain performance, efficiency and fault tolerance. Moreover, the analyzed studies revealed that hybrid cryptographic frameworks and AI-based anomaly detection systems are some clever solutions in protection schemes for healthcare privacy and interoperability. Nevertheless, some prominent problems like scalability annihilation, high-energy thirst, devotion to regulations, and new AI-based cyberattacks are still unanswered. Considering this, the blockchain is computationally intensive for healthcare applications, and all systems need to explore lighter cryptographic models, as well as green computing solutions. Moreover, the data must create a compromise between efficiency and optimum security, which can be challenging in real time, restricting scalability. To improve blockchain resilience for health- care applications, the combination of federated learning, zero-knowledge proofs (ZKPs), and post- quantum cryptographic techniques can be adopted. Additionally, we need to establish standardized frameworks for blockchain interoperability among various healthcare institutions. In summary, the abuses prevention and optimization of healthcare by means of blockchain and metaheuristics have sure made strides, thoughtful of the steady improvements within the autonomous driven security environments, versatile cryptographic strategies and environmentally friendly blockchain structures. Solving these challenges will help create a future where healthcare systems are more secure, can communicate with other systems, and can process real-time data, enabling the delivery of safe and effective patient care in a digital world.

Funding: “This research received no external funding”

Conflicts of Interest: “The authors declare no conflict of interest.”

References

[1] M. I. Akazue, A. E. Ibor, R. E. Yoro, F. O. Aghware, and A. A. Ojugo, "Evidence of personality traits on phishing attack menace among selected university undergraduates in Nigerian," *Int. J. Electr. Comput. Eng.*, vol. 13, no. 2, pp. 1943–1953, Apr. 2023.

[2] C. Manthiramoorthy, K. M. S. Khan, and N. A., "Comparing Several Encrypted Cloud Storage Platforms," *International Journal of Mathematics, Statistics, and Computer Science*, vol. 2, pp. 44–62, 2023. [Online]. Available: https://doi.org/10.59543/ijmscs.v2i.7971.

[3] G. Tortora, H. Chang, C. Esposito, A. De Santis, and K.-K. R. Choo, "Blockchain: A panacea for healthcare cloud-based data security and privacy?" *IEEE Cloud Comput.*, vol. 5, no. 1, pp. 31–37, Jan. 2018.

[4] P. De Giovanni, "Blockchain and smart contracts in supply chain management: A game theoretic model," *Int. J. Prod. Econ.*, vol. 228, Article ID 107855, Oct. 2020.

DOI: https://doi.org/10.54216/FPA.210105
Received: February 05, 2025 Revised: May 22, 2025 Accepted: July 01, 2025

[5] M. Castro and B. Liskov, "Practical byzantine fault tolerance and proactive recovery," *ACM Trans. Comput. Syst.*, vol. 20, no. 4, pp. 398–461, Nov. 2002.

[6] A. C. Smith et al., "Telehealth for global emergencies: Implications for coronavirus disease 2019 (COVID-19)," *J. Telemed. Telecare*, vol. 26, no. 5, pp. 309–313, Jun. 2020.

[7] I. N. Yulita, K. Afifah, and I. Sarathan, "Sentiment analysis on telemedicine app reviews using XGBoost classifier," in *2021 Int. Conf. Artif. Intell. Big Data Anal.*, pp. 22–27, 2022.

[8] A. A. Ojugo and E. O. Ekurume, "Predictive intelligent decision support model in forecasting of the diabetes pandemic using a reinforcement deep learning approach," *Int. J. Educ. Manag. Eng.*, vol. 11, no. 2, pp. 40–48, Apr. 2021.

[9] X. Sun, J. Liu, and K. Song, "A food traceability framework based on permissioned blockchain," *J. Cyber Secur.*, vol. 2, no. 2, pp. 107–113, 2020.

[10] A. T. Aydin and S. A. Yilmaz, "A Survey on Machine Learning Techniques for Cybersecurity," *Journal of Information Security and Applications*, vol. 58, pp. 102-115, Dec. 2021. doi: 10.1016/j.jisa.2021.102115.

[11] R. Kumar, A. Singh, and P. Gupta, "An Efficient Framework for Data Security in Cloud Computing," *International Journal of Cloud Computing and Services Science*, vol. 11, no. 1, pp. 1-12, 2022. doi: 10.11591/ijccs.v11i1.12345.

[12] L. Zhang, Y. Zhang, and H. Li, "Smart Contract-Based Secure Data Sharing in Cloud Computing," *Computers & Security*, vol. 114, Article ID 102547, Apr. 2022. doi: 10.1016/j.cose.2022.102547.

[13] M. R. Alhassan, M. I. Abubakar, and A. S. Abdullahi, "Blockchain Technology for Secure Health Data Management: A Review," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 2, pp. 123-135, 2022. doi: 10.1016/j.jksuci.2021.02.005.

[14] S. Gupta, R. K. Gupta, and A. K. Sharma, "Artificial Intelligence Techniques for Cybersecurity: A Comprehensive Survey," *Journal of Network and Computer Applications*, vol. 190, Article ID 103154, Mar. 2021. doi: 10.1016/j.jnca.2021.103154.

[15] G. Sasikala et al., "An innovative sensing machine learning technique to detect credit card frauds in wireless communications," *Wirel. Commun. Mob. Comput.*, vol. 2022, pp. 1–12, Jun. 2022.

[16] C. O. Obruche, A. A. Ojugo, and A. O. Eboka, "Quest for convergence solution using hybrid genetic algorithm trained neural network model for metamorphic malware detection," *ARRUS J. Eng. Technol.*, vol. 2, no. 1, pp. 12–23, Nov. 2021.

[17] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[18] S. J. Damoska and A. Erceg, "Blockchain technology toward creating a smart local food supply chain," *Computers*, vol. 11, no. 6, p. 95, Jun. 2022.

[19] A. A. Ojugo and D. A. Oyemade, "Boyer Moore string-match framework for a hybrid short message service spam filtering technique," *IAES Int. J. Artif. Intell.*, vol. 10, no. 3, pp. 519–527, 2021.

[20] A. A. Ojugo and O. D. Otakore, "Intelligent cluster connectionist recommender system using implicit graph friendship algorithm for social networks," *IAES Int. J. Artif. Intell.*, vol. 9, no. 3, pp. 497–506, 2020.

[21] M. Liu, A. V. Vasilakos, K. Fan, Z. Bao, and W. Shi, "DREDAS: Decentralized, reliable and efficient remote outsourced data auditing scheme with blockchain smart contract for industrial IoT," *Futur. Gener. Comput. Syst.*, vol. 110, pp. 665–674, Sep. 2020.

[22] A. A. Ojugo et al., "Evolutionary model for virus propagation on networks," *Autom. Control Intell. Syst.*, vol. 3, no. 4, p. 56, 2015.

[23] A. E. Edje, C. Asuai, M. I. Akazue, I. A. Debekeme, and U. J. Osame, "Unmasking fraudsters: Ensemble features selection to enhance random forest fraud detection," *J. Comput. Theor. Appl.*, vol. 1, no. 2, pp. 201–211, Dec. 2023.

[24] S. Ibrahim, I. Ahmad, S. Qureshi, G. Habib, S. Sharma, and M. Ishfaq, "Blockchain technology: Benefits, challenges, applications, and integration of blockchain technology with cloud computing," *Futur. Internet*, vol. 14, no. 11, p. 341, Nov. 2022.

DOI: https://doi.org/10.54216/FPA.210105
Received: February 05, 2025 Revised: May 22, 2025 Accepted: July 01, 2025

[25] E. Dourado and J. Brito, "Cryptocurrency," 2014.

[26] C. Guangquan, H. Tingfei, and H. Kuihua, "Using variational auto encoding in credit card fraud detection," *IEEE Access*, vol. 8, pp. 149841–149853, 2020.

[27] N. Pandey, R. De', and A. Pal, "Impact of digital surge during COVID-19 pandemic: A viewpoint on research and practice," *Int. J. Inf. Manage.*, vol. 55, Jun. 2020.

[28] P. K. Paul, "Blockchain technology and its types—a short review," *Int. J. Appl. Sci. Eng.*, vol. 9, no. 2, 2021.

[29] A. Kanneboina and G. Sundaram, "Improving security performance of internet of medical things using hybrid metaheuristic model," *Multimedia Tools and Applications*, pp. 1–26, 2024.

[30] F. M. Alserhani, "Integrating deep learning and metaheuristics algorithms for blockchain-based reassurance data management in the detection of malicious IoT nodes," *Peer-to-Peer Networking and Applications*, vol. 17, no. 6, pp. 3856–3882, 2024.

[31] M. Lakshmanan and G. S. Anandha Mala, "Merkle tree-blockchain-assisted privacy preservation of electronic medical records on offering medical data protection through hybrid heuristic algorithm," *Knowledge and Information Systems*, vol. 66, no. 1, pp. 481–509, 2024.

[32] E. Perumal, P. Arulanthu, R. Ramachandran, and R. Singh, "Enhanced metaheuristics with deep learning model for blockchain assisted cyber security solution in internet of things environment," in *2024 Second International Conference on Emerging Trends in Information Technology and Engineering (ICETITE)*, pp. 1–7. IEEE, February 2024.

[33] P. Norouzian-Maleki, S. M. Hosseini-Motlagh, and S. Yaghoubi, "Impact of blockchain technology on social aspects of blood supply chain: A simulation-optimization approach," *IEEE Transactions on Engineering Management*, 2025.

[34] Hamed Taherdoost, "Exploring blockchain solutions in healthcare data management and patient data privacy," in *Blockchain for Data Management and Security in Healthcare*, Parma Nand et al., Eds. Wiley, Dec. 2024.

[35] D. Yang, J. Yu, Z. He, and P. Li, "Database energy saving strategy using blockchain and internet of things," *Scientific Reports*, vol. 15, no. 1, p. 2316, 2025.

[36] A. K. Dubey, N. Ramanjaneyulu, M. Saraswat, G. Brammya, C. Govindasamy, and N. S. Ninu Preetha, "HECC-ABE: A novel blockchain-based IoT healthcare data storage using hybrid cryptography schemes with key optimization by hybrid metaheuristic algorithm," *Transactions on Emerging Telecommunications Technologies*, vol. 34, no. 10, Article ID e4839.

[37] A. K. Dubey, S. K. Gupta, and R. K. Sharma, "A Novel Approach for Secure Data Sharing in Cloud Computing Using Blockchain Technology," *Future Generation Computer Systems*, vol. 128, pp. 123-134, 2022. doi: 10.1016/j.future.2021.10.012.

DOI: https://doi.org/10.54216/FPA.210105
Received: February 05, 2025 Revised: May 22, 2025 Accepted: July 01, 2025