International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2024/25 Volume 11, Issue 3, May – June (2024)

RESEARCH ARTICLE

Preserving Security in Terms of Authentication on Blockchain-Based Wireless Sensor Network (WSN)

Tejbir Singh
Department of Computer Science and Engineering, MM Engineering College, Maharishi Markandeshwar (Deemed to be University), Mullana, Ambala, Haryana, India.
✉ tejbirrana662@gmail.com

Rohit Vaid
Department of Computer Science and Engineering, MM Engineering College, Maharishi Markandeshwar (Deemed to be University), Mullana, Ambala, Haryana, India.
rohitvaid@mmumullana.org

Received: 18 October 2023 / Revised: 21 May 2024 / Accepted: 25 June 2024 / Published: 30 June 2024

Abstract – Sensor nodes in wireless sensor networks have limited resources such as computing power, storage space, and battery life. Since WSNs are often deployed in untrusted areas, they are vulnerable to a wide variety of threats. Given the impossibility of preventing security breaches in a WSN, its data quality is likewise called into doubt. The authentication method in WSNs allows for the verification of the authenticity of both resources and data. Authentication in WSNs safeguards the integrity of the original data by determining whether it came from a trusted source and only allowing modifications made by that source. Existing authentication systems, however, have certain security flaws, such as those vulnerable to Identity (ID) spoofing attacks. As another example of promising new technology, blockchain has shown great promise in the realm of cyber security. The blockchain's security features include its cryptographic protection, immutability, non-reputability, irrevocability, auditability, and verifiability. This research is motivated by a desire to implement blockchain capabilities in WSNs for data integrity, security, and efficiency. In this study, research developed a new blockchain-based authentication method specifically for WSNs. Sensor nodes and a blockchain were built into the study's system architecture with the help of users and a private blockchain. A full security audit was done on the data used in the study. Concurrently, the proposed model was deployed to a wireless sensor node (WiSeN) sensor node to analyze its performance. According to the simulation findings, the suggested optimized strategy outperforms the traditional non-optimized technique in terms of accuracy. Furthermore, MVO has greater accuracy than ACO and PSO. The advantages of this technology and the issues with the present authentication processes make it imperative that the WSN deploy it. Optimization strategies are tested to improve security in WSNs. PSO, ACO, and MVO boost precision, recall, and F1-score. These procedures are trustworthy and might improve network resilience and counter real-world challenges. Security solutions may improve with further study.

Index Terms – Blockchain, WSN, Security, WiSeN Sensor Node, Performance, Authentication Method.

1. INTRODUCTION

Scientists have built WSNs, which are wireless networks comprised of various sensor nodes, to keep tabs on the state of the planet. WSNs are used in a wide variety of contexts, including home automation, industrial automation, transportation, and more [1]. There are potentially hundreds of potential uses in each category. In the environmental field, for instance, several uses may be found, including monitoring agricultural land, gauging water contamination, and keeping an eye on forest fires. In confined spaces like gardens or stadiums, wireless sensor networks thrive. However, they are also used in applications like border patrol and fire prevention that take place in the wild.

Wireless sensor networks WSNs face challenges due to limited resources and vulnerability to threats [2]. Authentication methods, such as ID spoofing attacks, are insufficient. Blockchain technology offers promising security features like cryptographic protection, immutability, and auditability [3]. This study developed a new blockchain-based authentication method for WSNs, integrating sensor nodes and a private blockchain. A security audit was conducted on the data and the model was deployed to a WiSeN sensor node. The optimized strategy outperformed traditional non-optimized techniques, making it crucial for WSN deployment.Blockchain technology offers significant benefits beyond authentication in wireless sensor networks (WSNs). It provides an immutable, tamper-proof ledger, enhancing data integrity and security [4]. Blockchain distributes authentication processes across nodes, making it more resilient to cyber attacks. Its cryptographic protocols ensure secure data transmission and storage. It also improves efficiency by streamlining data management processes and reducing reliance on intermediaries. Smart contracts automate

RESEARCH ARTICLE

agreements between WSN nodes, reducing transaction costs and processing times [5]. Blockchain-based solutions can revolutionize applications like smart cities, supply chain management, precision agriculture, and industrial IoT, driving innovation and enabling new capabilities in wireless sensor networks.

1.1. Blockchain

A 'blockchain' is an unalterable ledger of transactions that are cryptographically connected. These keys or signatures are linked in distributed ledgers via a network of nodes or processes [6]. The network ensures that every node always has the most recent version of the whole chain. The distributed nature of blockchain digital ledgers and the impossibility of backdating transactions are two further benefits of this technology; blockchain technology provides various benefits [7].

To accomplish this objective, when a WSN user publishes (stores) the data on the blockchain, it makes it impossible for a challenger to change the data due to the immutability aspect of the blockchain technology [8]. In addition, due to the immutability of the blockchain, it is possible to identify both internal and external attackers by monitoring any changes that take place in the hash of the blocks. "Blockchain is a peer-to-peer (P2P) architecture that erodes the power of third-party intermediaries" via the use of decentralization [9] with fundamental properties, such as immutability, dependability, transparency, and security. Blockchains are digital ledgers that record and verify transactions between two or more peers. The individual blocks that make up a blockchain are linked to one another to create a distributed ledger. The previous block's hash is kept in a persistent location inside each block [10]. Even a one-bit variation in one block has a ripple effect in the hash of all the other blocks. The distinctive characteristics of blockchain technology that contribute to the enhancement of Wireless networks (WNs) are shown in Figure 1.

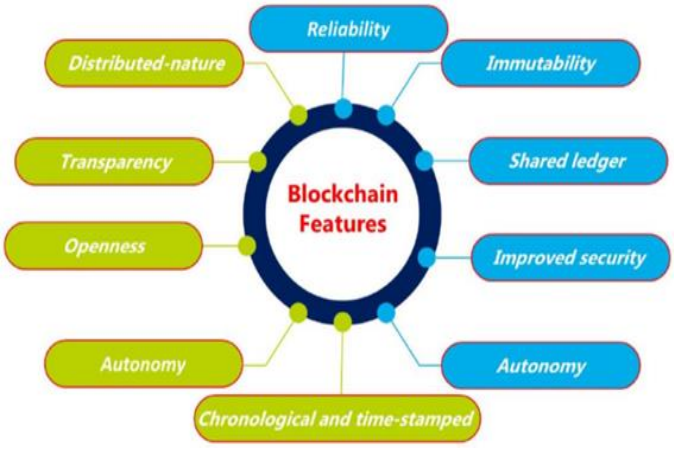

Figure 1 Feature of Blockchain [10]

1.2. Wireless Sensor Network (WSN)

A WSN is a self-configure ring, infrastructure-free network used to collect and transmit data from sensors measuring physical or environmental factors such as noise or vibration [11]. To keep tabs on the health of a system or its surrounding environment, a WSN, or wireless sensor network, may be set up using several wireless sensors [12]. WSNs are interconnected systems of sensors deployed across a region with the purpose of monitoring and reporting on environmental conditions. Some of the environmental factors that WSNs may track are temperature and wind speed.

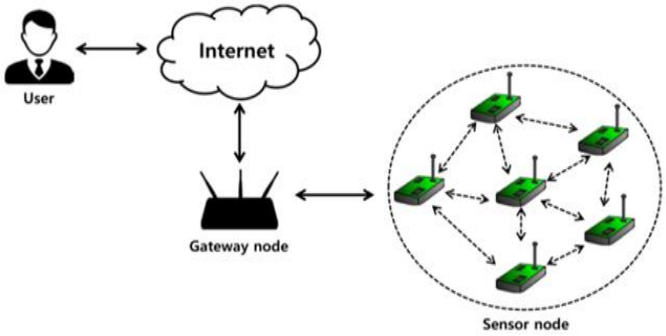

Figure 2 Wireless Sensor Network [12]

Figure 2 presents the WSNs. To allow wireless transmission of sensor data, they, like wireless ad hoc networks, rely on wireless connection and the spontaneous expansion of networks [13]. Environmental or physical elements are detected by WSNs and include temperature, sound, and pressure. Modern networks don't only operate as conduits for data collecting; they also enable the management and manipulation of sensor activity. The military's major goal for creating these networks is battlefield surveillance. From equipment health monitoring to industrial process control, these networks have many practical and consumer applications. Each 'node' in a WSN is a sensor node, and the total number of nodes in a WSN may range from a few to several thousand [14]. Each node has a radio transceiver with an antenna, a microprocessor, a power supply (usually a battery or an integrated form of energy harvesting), and an electrical circuit for connecting with the sensors.

1.3. Security

Encryption is the process of encoding data using cryptographic methods. Using this method, research can convert plaintext information into a cryptographic representation [15, 16]. To protect sensitive information, only authorized individuals should be able to interpret cipher letters. While encryption cannot stop data from being intercepted, it may prevent it from being interpreted by an unauthorized user [17]. For practical purposes, this technique creates a pseudo-random encryption key. A well-designed encryption technique requires a lot of computational power

RESEARCH ARTICLE

and expertise to decode the message without the key. The proposed study employs polynomial encryption and evaluates about existing methods for secure data storage, such as "RSA and AES [18].

1.3.1. RSA

RSA public-key cryptosystem" is one of the most used methods for ensuring the safety of data transfer. In addition to that, it is also one of the oldest. In symmetric-key cryptography, the shared keys are often sent through RSA [19]. These keys are subsequently utilized for widespread encryption and decryption. Key distribution describes this method.

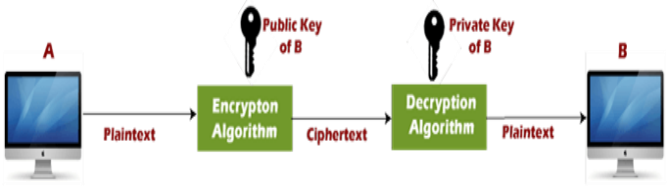

Figure 3 RSA Algorithms [19]

RSA Algorithms shown in Figure 3, the RSA cryptographic method requires both a public key and a private key for usage (that is, two distinct keys that are mathematically related to one another) [20]. In contrast to the public nature of a public key, the absolute secrecy of a private key means that it must never be shared with anybody.

1.3.2. AES

The U.S. NIST (National Institute of Standards and Technology) developed a standard for the encryption of digital data in 2001 called AES, formerly known by its original name, Rijndael [21]. During the AES selection process, two Belgian cryptographers proposed a variation of the Rijndael block cipher to NIST. When coupled with an NSA-approved cryptographic module, AES is the only publicly accessible cipher allowed for usage with secret information [22].

Offering advantages beyond authentication concerns improves the case for blockchain-based wireless sensor network solutions. Blockchain technology improves data integrity, security, and efficiency beyond authentication. Decentralized blockchains provide an immutable, tamper-proof ledger, ensuring data integrity [23]. All transactions and data updates are cryptographically linked to past records, making it very hard to change historical data without notice. This capability makes WSN data more reliable, which is important for healthcare, environmental monitoring, and industrial automation. Second, blockchain reduces data breaches and single points of failure. Cyber attacks on centralized servers or authentication servers may target traditional centralized authentication systems [24]. Blockchain is more resistant to assaults and unauthorized access since it spreads authentication over a network of nodes. Blockchain's cryptographic methods protect WSN data during transmission and storage. Blockchain streamlines data management and reduces middlemen, improving efficiency. Smart contracts, self-executing contracts with blockchain-encoded conditions, automate and enforce WSN node agreements, eliminating middlemen and lowering transaction costs and processing times. Decentralized blockchain allows peer-to-peer communication and data exchange, avoiding centralized servers and lowering network latency and congestion. Including these advantages in the argument shows blockchain's transformational potential beyond WSN authentication [25]. Blockchain-based solutions can transform smart cities, supply chain management, precision agriculture, and industrial IoT by improving data integrity, security, and efficiency, driving innovation, and enabling new wireless sensor network capabilities.

1.4. Role of Blockchain in WSN

Tactics, Techniques, and Procedures (TTP) are capable of describing the behavior of threat actors as well as a structured framework for executing a cyber attack. By eliminating the need for a TTP, a BWSN system improves upon the security and trust of traditional WSNs. A trustworthy distributed system for storing sensory data is provided by BWSN [26]. Therefore, the SPF issue does not arise. Blockchain technology has been researched in wireless networks, inspired by its successful use in cryptocurrencies since it enables previously unknown persons to engage with each other transparently [27]. Blockchain technology has several potential applications; one is the safe exchange of data in a wireless body area network as shown in Figure 4.

1.5. Authentication of Blockchain-Based WSN

Such security vulnerabilities may be avoided with the usage of authentication [28]. Authentication of data in sensor networks ensures that data has come from trusted sources and prevents tampering with the original data. For WSNs, authentication is crucial for a secure connection. During two-way communication between sensor nodes, authentication ensures that both parties are talking to genuine devices. Only approved sensor nodes will be able to connect to the network, and this is ensured via authentication. In this method, only approved users are allowed access to the network. In WSNs, user authentication may be accomplished in a few different ways.

1.6. Optimization Approach Comparison

Traditional optimization methods, such as gradient descent, are simple and general for simpler problems but struggle with complex, high-dimensional search spaces. Metaheuristic algorithms, such as Genetic Algorithms (GAs), Particle

RESEARCH ARTICLE

Swarm Optimization (PSO), and Ant Colony Optimization (ACO), offer more robust solutions for complex and non-linear optimization problems. These methods are flexible and do not require gradient information, making them suitable for a broader range of applications [29]. Hybrid approaches and nature-inspired algorithms combine the strengths of multiple algorithms to enhance performance. Combining PSO with local search techniques can improve convergence speed and accuracy. Nature-inspired algorithms, like the Firefly Algorithm and Rock Hyrax Swarm Optimization (RHSO), leverage natural phenomena to develop innovative search strategies. RHSO, for example, mimics the cooperative behavior of rock hyraxes to efficiently explore and exploit search spaces. Advanced optimization techniques often incorporate mechanisms to handle dynamic and uncertain environments, making them suitable for real-time applications. Techniques such as adaptive parameter control and multi-objective optimization further enhance their capability to solve complex problems that involve trade-offs between multiple conflicting objectives.

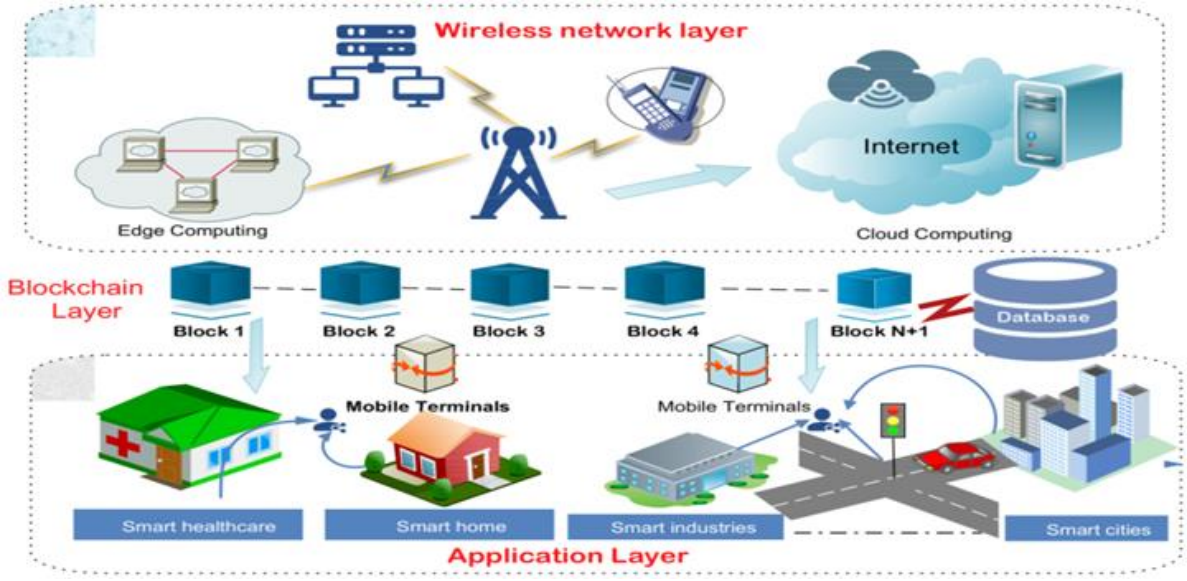

Figure 4 Role of Blockchain in WSN [27]

1.7. Challenges of Blockchain Integration

Blockchain technology is a promising solution for transforming various industries, but its integration faces several challenges. Scalability is a major hurdle, as traditional blockchains like Bitcoin and Ethereum struggle with limited transaction throughput and high latency, making them less suitable for high-frequency transactions [30]. Interoperability is another challenge, as different blockchain platforms operate on unique protocols, making it difficult to achieve seamless communication and data exchange.

Security and privacy concerns also pose significant challenges, as blockchain technology is inherently secure due to its decentralized nature but still has vulnerabilities. Regulatory and compliance issues complicate blockchain integration, as the legal status of blockchain and cryptocurrencies varies across jurisdictions.

Energy consumption is another pressing issue, particularly for proof-of-work-based blockchains like Bitcoin, which require significant computational power and raise environmental concerns and operational costs. Finally, user adoption and education are critical challenges, as blockchain technology is complex and difficult for end-users and developers to understand and use effectively. Addressing these issues requires collaboration between developers, industry stakeholders, and policymakers to realize the full potential of blockchain technology.

1.8. Proposed Blockchain-Based Authentication System

A blockchain-based authentication system is being proposed to enhance security in Wireless Sensor Networks (WSN) [31]. The system uses blockchain technology's immutability and distributed nature to record all authentication transactions. Sensor nodes generate public and private cryptographic keys, which are stored on the blockchain for tamper-proof verification.

The system can incorporate advanced cryptographic techniques like digital signatures and hash functions, and use smart contracts for real-time responses to security breaches. It addresses critical security concerns like unauthorized access, data integrity, and protection against attacks like man-in-the-middle, replay attacks, and node impersonation. The decentralized nature eliminates single points of failure, making the network more resilient against attacks.

RESEARCH ARTICLE

1.9. Security Benchmark

A security benchmark is a standardized evaluation framework used to assess the security posture of systems, networks, or applications. It involves testing and measuring various security parameters and practices against predefined criteria or industry best practices [32]. The primary objective is to identify vulnerabilities, weaknesses, and areas of improvement in the security infrastructure and establish a baseline for comparison with security standards or compliance requirements [33]. A security benchmark covers multiple aspects of security, including network security, endpoint security, data security, application security, identity and access management, incident response and management, and compliance and regulatory requirements. The process involves defining objectives, gathering information, selecting a suitable benchmark, conducting a comprehensive assessment, analyzing results, providing recommendations, and implementing continuous improvement processes. By following a structured security benchmarking process, organizations can gain valuable insights into their security posture, identify and mitigate potential risks, and strengthen their overall security defenses against evolving threats.

1.10. Real Word Application

A blockchain-based wireless sensor network (WSN) could be used to secure communication and data exchange among IoT devices and sensors in a smart city infrastructure project. Each sensor node is equipped with a unique identifier and cryptographic capabilities to authenticate and encrypt data transactions on the blockchain [34]. An authentication system is implemented to manage access control and identity verification for authorized users, devices, and applications [35]. The authentication process involves a multi-factor authentication process, which is securely recorded and time stamped on the blockchain ledger. Once authenticated, authorized devices and applications can securely exchange data with the WSN, ensuring confidentiality and integrity. The authentication system also generates real-time monitoring and alerts for suspicious activities, enabling prompt response and mitigation of security threats [36]. This system ensures compliance with data protection regulations and privacy laws, facilitating secure data sharing and collaboration among stakeholders [37].

1.11. Paper Organization

Section 1 focuses on the introduction part. it contains the definition and features of blockchain and WSN. it considers polynomial encryption and evaluates about existing methods for secure data storage along with the Role of Blockchain in WSN.

Section 2 surveyed on literature review considering existing research papers on Blockchain, WSN, Security, WiSeN sensor nodes, and Authentication Method. It contains research gaps for several approaches.

Section 3 presents the problem statement in existing research. Previous studies have not sufficiently considered how well their findings apply to situations that occur in the real world.

Section 4 considers the proposed work part which contains the research methodology. it is the Working of LSTM in the proposed work and the Technology used in the proposed work with its model. it presents the Integration of optimization with deep learning.

Section 5 implements the result and discussion part considering the proposed model of this research by comparing the accuracy and error rate of conventional mechanism, PSO, ACO, AND MVO integrated mechanism.

Section 6 focuses on the conclusion part. Simulation results conclude that the proposed optimized approach provides better accuracy as compared to the conventional non-optimized approach.

Section 7 considers the future scope of research. The goal of future research is to test out alternative digital signature algorithms and employ all currently available consensus techniques.

2. LITERATURE REVIEW

A. K. Gautam, et al.(2021) did research on the various methods used in WSNs for handling keys, authentication, and trust. In this article, research provides a primer on the several approaches to managing trust, authenticating users, and securing data that may be used in practice. Multiple methods have been offered to address WSN key management, authentication, and trust management; here, research takes a closer look at the strengths and weaknesses of each technique. This in-depth evaluation was performed to find the most adaptable security option for the application.[1]

M. A. Ferrag, et al.(2017) focused on the IoT with strong authentication protocols. In this study, they provide a thorough analysis of the authentication mechanisms currently in use for IoT. They analyze in depth more than forty authentication protocols used in these contexts. To begin, they look at all of the recent survey studies that have been published on IoT. They next examine IoT authentication protocol threat models, mitigation strategies, and formal security verification methods. they also give a table-based taxonomy and comparison of IoT authentication methods across five dimensions: network model, objectives, primary operations, computational complexity, and communication overhead.[2]

K. Salah, et al.(2018) reviewed IoT security in a retrospective with blockchain-based answers and unanswered questions. issues of key concern for IoT security were presented and

RESEARCH ARTICLE

examined. They examine and classify prevalent security concerns relating to the IoT's layered architecture, including the networking, communication, and management protocols. They describe IoT security needs, including the current assaults, threats, and cutting-edge solutions. They also compile a table of IoT security issues and a map of published remedies. They also talk about how blockchain, the technology behind Bitcoin, may be a crucial facilitator in addressing many of the security issues plaguing the IoT.[3]

M. T. Hammi, et al.(2018)introduced the bubbles of trust as a distributed authentication mechanism for IoT that uses the blockchain. To solve the problem of weak device authentication and identification, they offer a novel distributed approach termed bubbles of trust. Additionally, it safeguards both the availability and integrity of the data. To this end, their method makes use of blockchains' security features to build isolated networks (bubbles) of connected devices that know and trust one another. The findings demonstrate its effectiveness, efficiency, and cheap cost in meeting the security needs of IoT.[4]

T. Salman, et al.(2019)presented work on the safety measures provided by blockchain technology. The purpose of this article was to explain why and how security services are necessary for contemporary applications, detail the challenges these services offer, and then explain how blockchain technology might solve these problems. Additionally, several blockchain-based methods that provide these safety services are compared in detail. [5]

C. V. Nguyen, et al.(2021)proposed work on the pros and cons of using blockchain technology in WSNs.These days, civil and military applications aren't the only places where wireless sensor networks are being put to use. Even though WSNs provide many advantages, there are also some drawbacks. However, because of its centralized server/client approach, the WSN presents numerous difficulties when used in the real world, including security and storage. As a result, the WSN's infrastructure must adopt the distributed paradigm. Blockchain (BC) is one of the newest distributed technologies now in use. The use of Blockchain technology as a means to address WSN's security and distributed storage issues seems to be a promising direction to go. It may lead to new areas of study and distributed application development.[6]

C. H. Liu, et al.(2017) looked at a safe method of user identification for mobile medical sensor networks. This study presents an authentication strategy for users and a data transfer mechanism that safeguards users' privacy while allowing healthcare providers to quickly track patients' vitals and provide better, faster treatment. Only authorized medical staff was able to see sensitive patient data like temperature, and blood pressure thanks to their system's combination of smart cards and passwords. In addition, a safe cryptosystem was used to set up the system of sending data.[7]

R. Riaz, et al.(2019) focused on biometric user authentication systems for wireless sensor networks. Therefore, they provide a novel approach to WSN security. It improves network speed while also increasing security. The calculations and procedures in this solution are simple. In this paper, they assess the suggested method and compare it to similar approaches already in use. By decreasing network traffic, protecting against DOS assaults, and extending a node's battery life, this technique improves the network's overall performance.[8]

Y. Lu, et al.(2016)did research on a mixed-encryption wireless authentication centre for WSNs.WSNs have found usage in many different fields recently. Due to the potentially life-changing nature of the information sent by sensor networks, safety must be a top concern. Therefore, it was important to consider how to secure sensor nodes against assaults without increasing their processing capacity or energy usage. [9]

A. Sen, et al.(2016)looked at a watermark-based low-overhead node authentication technique for WSNs. They provide a scheme that uses digital watermarks to verify node identities. There are three parts to the proposed watermarking method: creation, embedding, and detection. The algorithm's strength was determined by how long it took and how likely it was to break. Using the results of the robustness study, they can determine the optimal watermark size for future designs. The scheme's efficiency was evaluated in terms of data storage, processing time, and network bandwidth use. They compare the analytical findings to two current systems, both of which reduce these kinds of overheads significantly.[10]

X. Zhang, et al.(2019)explained IoT devices through WSNs with anonymous users. IoT growth has been aided by the widespread availability of wireless networks and devices. In this research, they describe two models that work well in an IoT setting, and then they build authentication protocols for each model that are more secure and need less computing power to implement than other methods now in use.[11]

A. Arivarasi et al.(2021)focused on the adaptive trust sector-based authentication with the honey encryption technique in WSN to improve the anonymity of the source location. To determine the relationship between an item and its surrounding environment, scientists have developed wireless sensor networks. It takes up all the information it can and sends it back to the hub through wireless connections. However, there were obstacles to overcome in wireless sensor networks, such as the effective placement of sensor nodes. Energy scarcity, transmission capacity, range, data dispersion, data permanence, malfunctioning nodes, and data security

RESEARCH ARTICLE

redundancy are just a few of the problems that need to be solved.[12]

The integration of blockchain technology with IoT in healthcare has emerged as a promising solution to address challenges related to data security, privacy, and energy optimization. Alghamdi and Javaid (2024) explored the use of blockchain for energy optimization and secure storage in wireless sensor IoTs. Their study emphasizes the dual benefits of enhanced authentication and cost-effective storage solutions provided by blockchain, crucial for maintaining the integrity and efficiency of IoT networks in healthcare environments [13]. Similarly, Vatambeti et al. (2023) focused on the application of blockchain to secure medical data within IoT systems. They proposed an enhanced privacy-preserving blockchain technology that significantly improves data security, ensuring that sensitive health information is protected from unauthorized access and breaches [14].

Furthermore, Xiao et al. (2024) introduced a novel approach called BS-SCRM, which combines blockchain with swarm intelligence techniques to secure wireless sensor networks. This method not only fortifies network security but also leverages the decentralized nature of blockchain to enhance the robustness of IoT systems against cyber threats [15]. Additionally, de Jesus et al. (2024) examined the security implications of integrating blockchain with smart cyber-physical applications that rely on wireless sensor and actuator networks. Their comprehensive review highlighted the potential of blockchain to provide a secure foundation for the deployment of advanced IoT applications in healthcare, ensuring reliable and tamper-proof data exchange between devices [16].

Collectively, these studies underscore the critical role of blockchain technology in enhancing the security and efficiency of IoT in healthcare. By addressing key issues such as data privacy, authentication, and energy optimization, blockchain presents a robust framework for the development of secure and reliable healthcare IoT systems. These advancements pave the way for more resilient and trustworthy healthcare infrastructures, capable of meeting the growing demands of modern medical applications.

Table1 provides a snapshot of each reference, highlighting their algorithmic approaches, achieved results, and identified limitations based on the information available from the references. For detailed analysis, specific access to each paper would be required. Table 1 is presenting algorithm, remarks and limitation of related works.

Table 1 Summary of the Related Works

Ref	Algorithm	Remarks	Limitations
[1]	Adaptive trust sector-based authentication with a honey encryption algorithm	Improved source location privacy protection in WSN	Not explicitly stated in the provided summary
[2]	Deterministic K-means secure coverage clustering with periodic authentication	Enhanced security in wireless sensor networks (WSN) for coverage clustering	Lack of details on scalability and real-world deployment
[3]	Various authentication protocols for IoT	A comprehensive survey of authentication protocols for IoT	No new algorithm or implementation, survey-based
[4]	Review of IoT security and blockchain solutions	Overview of challenges and solutions in IoT security using blockchain	General review lacks specific algorithm or implementation details
[5]	Modified Neuro-Fuzzy Model	Estimating the reliability of component-based software systems	Application limited to software systems, not directly related to WSN
[6]	Various security services using blockchains	Survey of blockchain-based security services	Lack of specific new algorithm or implementation
[7]	Blockchain technology in WSN	Benefits and challenges of using blockchain in WSN	Theoretical discussion may lack practical deployment details
[8]	Secure user authentication scheme	Improved security for healthcare sensor networks	Potential limitations in scalability and real-time performance
[9]	SUBBASE authentication scheme based on user biometrics	Enhanced authentication in WSN	Biometric data security concerns, deployment challenges

RESEARCH ARTICLE

[10]	Mixed Encryption in WSN	Study of mixed encryption for authentication	Potential overhead due to mixed encryption approach
[11]	CK Metrics for object-oriented structure	Study on reliability using CK Metrics	Limited to software metrics, not specific to WSN
[12]	Anonymous user WSN authentication	Novel anonymous authentication approach	Practical feasibility and performance in real-world scenarios
[13]	Energy optimization with authentication using blockchain	Energy-efficient IoT using blockchain	Blockchain overhead on energy consumption, scalability
[14]	Enhanced privacy-preserving blockchain in IoT	Secure medical data management	Privacy concerns, blockchain scalability
[15]	BS-SCRM: Blockchain and swarm intelligence for WSN security	Novel approach for secure WSN using blockchain and swarm intelligence	Integration complexity, resource consumption
[16]	Security in blockchain-based smart cyber-physical applications	Security in smart applications using blockchain and WSN	Integration challenges, performance impact
[17]	Fuzzy-based secure authentication and clustering	Energy-efficient authentication and clustering in WSN	Fuzzy logic computational complexity
[18]	IoTChain: Three-tier blockchain-based IoT security architecture	Comprehensive IoT security using blockchain	Blockchain scalability and latency issues
[19]	Quality assurance of component-based software systems	Quality assurance in software systems	Not directly related to WSN or IoT
[20]	Improved blockchain-based authentication protocol for IoT network management	Enhanced authentication protocol for IoT networks	Scalability and blockchain overhead

2.1. Research Gap

The author has researched the several approaches used in WSNs for managing keys, authenticating users, and establishing trust. The author focuses on IoT with robust authentication protocols, which give a comprehensive review of the authentication techniques that are now in use for the IoT. The research analyzed the history of IoT security, providing both blockchain-based solutions and problems that remained unresolved. Concerns that are of primary concern about the safety of IoT were presented and investigated. The author presented the bubbles of trust, which is a decentralized authentication system for IoT that makes use of the blockchain. They propose a unique distributed strategy that they call bubbles of trust to overcome the issue of insufficient device authentication and identification. The author presented their research on the preventative measures offered by blockchain technology and advised more research on the benefits and drawbacks of using blockchain technology in WSNs. At this point, wireless sensor networks are finding utility in a variety of contexts in addition to their traditional civil and military uses. They looked for a foolproof method of user identification for mobile medical sensor networks, one that provides an authentication strategy for users and a data transfer mechanism that protects users' privacy while enabling medical professionals to quickly track patients' vitals and treat them more effectively and expediently.

The SUBBASE project's primary emphasis was on developing a biometric user authentication system for use with wireless sensor networks. As a result, they provided a fresh strategy for protecting WSNs and conducted research on a wireless mixed-encryption authentication center specifically designed for WSNs.WSN have lately found applications in a wide variety of industries. A watermark-based low-overhead node authentication approach was investigated for use in WSNs as part of the research. They provide a LoWaNA protocol that validates node IDs via the use of digital watermarks. It walked anonymous people through an explanation of IoT devices using WSNs.

RESEARCH ARTICLE

2.2. Challenges

Previous studies have not sufficiently considered how well their findings apply to situations that occur in the real world. Previous research only addressed a very little piece of the subject at hand. Within the realms of blockchain technology and WSN, there is an urgent need to enhance the accuracy and efficiency of their respective operations. In addition, the prior study did not consider the possibilities of merging WSN, security, and authentication in any way. In other words, past studies have not been able to properly apply the findings of their study in the actual environment where the research was conducted. The previous study only looked at a small part of much larger phenomena. Two features of WSN that need to be addressed are its accuracy and its efficiency. In addition, the earlier research didn't take into consideration the potential benefits that may be obtained by maintaining the security of authentication on blockchain-based WSN systems, therefore it missed out on those opportunities.

3. PROPOSED WORK

The suggested research is informed by the most up-to-date research in 6G and optimization. Current studies focus on"PSO, ACO, and MVO", three different kinds of optimization techniques. There are several problems with the suggested task that stem from the constraints of the optimization process and its accuracy and efficiency. Consider the PSO-MVO, the objective function, and the many parameters that need to be included in the suggested hybrid approach. Finally, researchers compare the time it takes and the number of mistakes made to the industry norm. Figure5 presents the research methodology.

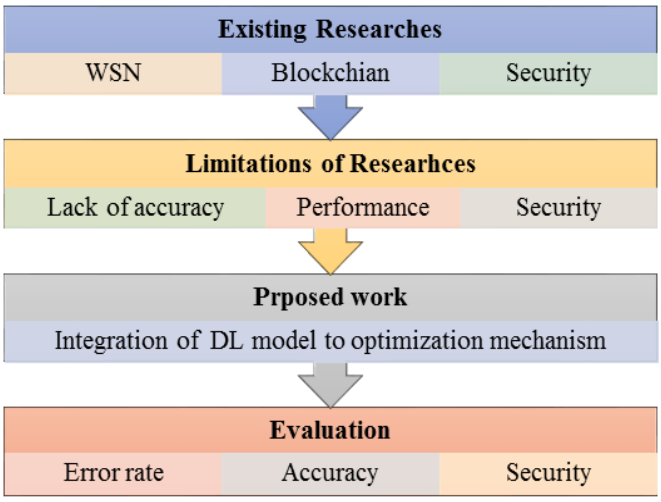

Figure 5 Research Methodologies

3.1. Technology Used in Proposed Work

Research work is considering MATLAB environment for simulation of accuracy and error rate. Java-based net beans environment has been used for GUI programming to program the sender and receiver modules. Moreover, data compression and encryption coding have been made in Java language. To perform data compression data replacement mechanisms have been used whereas data encryption has been performed by cryptography techniques. Blockchain mechanism has been used to store data securely after compression and cryptography. To categorize threats deep learning model has been used.

3.2. Working of LSTM in Proposed Work

"LSTM is a type of RNN architecture" that is particularly effective in handling sequences of data. LSTMs are widely used for data classification tasks, especially when the data has temporal dependencies or sequential patterns. Here's an overview of how an LSTM model works for data classification.

1. Data Preparation: The first step is to prepare the data. For data classification tasks, you typically have labeled data, where each example is associated with a specific class or category. This data is often divided into a training set, a validation set, and a test set.
2. Sequence Padding: If data consists of sequences of varying lengths, you may need to pad the sequences to make them uniform. This is important for batch processing, which LSTMs typically require.
3. Input Encoding: Convert the input data into a format that can be fed into the LSTM model. This often involves encoding categorical data or transforming text data into numerical vectors, such as word embeddings.
4. LSTM Architecture: Construct the LSTM model. The LSTM architecture consists of one or more LSTM layers. Each LSTM unit within a layer processes the input sequence step by step and retains a hidden state that captures information from previous time steps. LSTMs can be stacked to create deep architectures.
5. Training: Train the LSTM model using the training data. During training, the model learns to capture the temporal dependencies and patterns within the sequences. This is done through back propagation and gradient descent, where the model adjusts its weights and biases to minimize a loss function.
6. Dropout and Regularization: To prevent over fitting, dropout layers, and regularization techniques can be added to the LSTM model. This helps ensure that the model generalizes well to unseen data.
7. Loss Function: Use an appropriate loss function for classification tasks. For binary classification, binary cross-entropy is commonly used, while categorical cross-entropy is suitable for multi-class classification.

RESEARCH ARTICLE

8. Optimization: Select an optimization algorithm, such as stochastic gradient descent (SGD), Adam, or RMSprop,Optimization: Select an optimization algorithm, such as stochastic gradient descent (SGD), Adam, or RMSprop,to update the model's parameters during training.
9. Validation: Continuously evaluate the model's performance on the validation set during training to monitor for overfitting and adjust hyper parameters as needed.
10. Prediction: Once the model is trained, you can use it to make predictions on new, unseen data. The LSTM processes input sequences and provides class predictions or probability scores for each class.
11. Evaluation: Measure how successfully the model classifies data using the test set using tools like accuracy, precision, recall, F1-score, and the confusion matrix.

LSTM models (Figure 6) excel at handling sequential data, making them suitable for a wide range of applications, including NLP, time series analysis, speech recognition, and more. By capturing long-term dependencies and patterns in data, LSTMs have demonstrated their effectiveness in various data classification tasks.

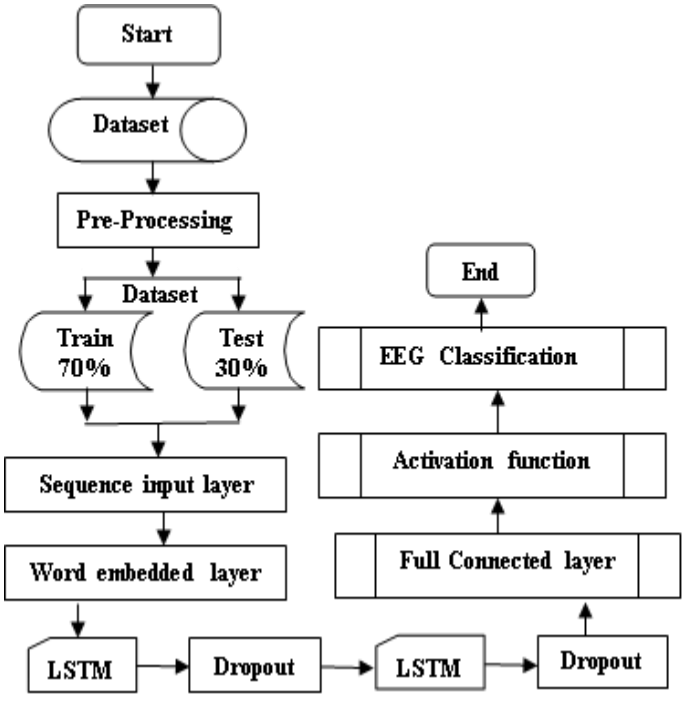

Figure 6 LSTM Model

3.3. Integration of Optimization with Deep Learning

Simulating Optimization with deep learning can be a powerful approach to enhance the optimization process and improve convergence towards optimal solutions. In this integration, deep learning techniques can be used to enhance different aspects of the optimizer, such as initialization, fitness function estimation, and swarm behavior. Here's a general overview of how you can simulate PSO with deep learning.

1) Initialization with Deep Learning

- Use deep learning models to intelligently initialize the positions and velocities of particles in the optimization algorithm.
- Deep learning models can analyze the problem's characteristics and suggest better starting points for the particles.

2) Adaptive Parameters: Train deep learning models to adaptively adjust the parameters of the optimization algorithm during optimization.

3) Fitness Function Estimation: Replace or augment the conventional fitness function with a deep learning model that estimates the fitness value of solutions. This can be particularly useful when evaluating the fitness function is computationally expensive.

4) Swarm Behavior Enhancement

- Utilize deep reinforcement learning to enhance the decision-making behavior of particles. Train agents that control particle movements and interactions in a way that accelerates convergence.
- Reinforcement learning can help particles adapt to changing problem landscapes and swarm dynamics.

5) Hybridization with Deep Learning: Combine optimization with deep learning in a hybrid approach.

6) Dynamic Parameter Tuning: Implement deep learning-based controllers that continuously tune the parameters of optimization, adapting them to the specific characteristics of the optimization problem.

7) Stopping Criteria: Train a deep learning model to predict the termination point for the optimization process based on the current state and progress. This can help avoid unnecessary computation when the optimization is likely to converge.

8) Parallel and Distributed Optimization: Utilize deep learning for orchestrating parallel and distributed optimization processes during collaboration and efficient sharing of information efficiently.

9) Transfer Learning: Use transfer learning techniques to apply knowledge learned from previous optimization problems to new and similar problems, accelerating convergence in previously unoptimized areas.

RESEARCH ARTICLE

These approaches demonstrate the potential of combining optimization and deep learning to create more intelligent and adaptive optimization algorithms. The integration of deep learning techniques allows for improved problem-solving capabilities and faster convergence to optimal solutions in complex and high-dimensional spaces. However, it's important to note that the success of this integration depends on careful problem analysis and parameter tuning.

4. RESULT AND DISCUSSION

To establish which of the cluster's nodes will act in the capacity of cluster head based on the data that has been provided, the environment of MATLAB simulates several different scenarios that include the total number of nodes that make up the cluster. Investigations were conducted into a variety of scenarios including 100 nodes. The simulation accounted for different assault volumes, which resulted in a rise in the number of lost packets and a drop in the number of packets delivered. Before it was possible to conduct an assessment of the system's security, the various types of threats were categorized, and blockchain technology was utilized to implement security measures. Several tables have been used to provide a summary of the categorization analysis. It is essential to keep in mind that attacks might result in the loss of packets, which can subsequently impede the delivery of packets if there are sufficient numbers of them. For this reason, it is very necessary to take into consideration these variables when determining the level of overall security provided by the system. The MATLAB simulation seems to be a comprehensive way of evaluating the system's ability to withstand a range of different forms of assault. The capacity of the system to provide the nodes with a high degree of security and reliability is improved by the use of blockchain technology. Section 4.1 is focused on proposed work algorithm.

4.1. Proposed Algorithm

There is a proposed work algorithm that is expressed step by step:

1. Initialization: Initialize the blockchain network with all sensor nodes and their corresponding identities. Set up smart contracts to govern authentication and access control policies.
2. Data Transmission: Sensor nodes collect data and transmit it securely to neighboring nodes within the WSN. Each data transmission is time stamped and recorded on the blockchain ledger.
3. Authentication Process: When a sensor node receives data from another node, it verifies the sender's identity using the blockchain. Smart contracts are executed to enforce authentication policies, ensuring that only authorized nodes can access and transmit data.
4. Accuracy Calculation: Keep track of successful authentication events and unauthorized access attempts. Calculate accuracy as the ratio of successful authentications to the total number of authentication attempts.

$$\text{Accuracy} = \frac{\text{Authentication Successful}}{\text{Total Authentication}} \times 100\%$$

5. Error Rate Calculation: Identify and record instances of authentication errors, including false positives (authorized nodes misidentified) and false negatives (unauthorized nodes granted access). Calculate the error rate as the ratio of authentication errors to the total number of authentication attempts.

$$\text{Error Rate} = \frac{\text{Authentication Error}}{\text{Total Authentication}} \times 100\%$$

6. Continuous Monitoring and Evaluation: Continuously monitor authentication processes and record any deviations or anomalies. Evaluate accuracy and error rate periodically to assess the effectiveness of the authentication system.
7. Security Analysis: Conduct a security analysis to identify potential vulnerabilities or weaknesses in the authentication system. Address any security issues discovered through updates, patches, or policy revisions.
8. Feedback and Improvement: Gather feedback from network stakeholders, including sensor node operators and administrators. Use feedback to refine the authentication algorithm and enhance security measures.
9. Documentation and Reporting: Maintain detailed records of authentication events, accuracy, and error rates. Generate periodic reports to communicate performance metrics and security status to stakeholders.
10. Adaptive Learning: Implement adaptive learning mechanisms to improve the authentication algorithm over time. Use machine learning algorithms to analyze authentication patterns and adjust parameters dynamically.

4.2. Comparison Analysis of Accuracy

Students to perform in the future are shown in Table 2. The conventional process has been proven to be less exact than the suggested method, which is more precise. In the case of 100 nodes, 6-time attacks have been made that are influencing accuracy in the outcomes of an inventory taking about the precision of the work that was finished and the tasks that were suggested for the case of conventional and proposed work. Taking into consideration the information in Table 2, researchers are now able to demonstrate in Figure 7 how much more accurate the optimized version of the Deep Learning Mechanism is in contrast to the non-optimized version.

RESEARCH ARTICLE

Table 2 Comparative Analysis of Accuracy

Attacks	Conventional Mechanism	PSO integrated mechanism	ACO integrated Mechanism	MVO integrated mechanism
1	91.86%	94.01%	94.68%	94.92%
2	91.60%	93.96%	94.89%	94.26%
3	91.99%	94.11%	95.14%	95.03%
4	91.38%	93.39%	94.80%	94.43%
5	91.69%	93.03%	94.79%	95.44%
6	91.06%	93.70%	94.98%	94.57%

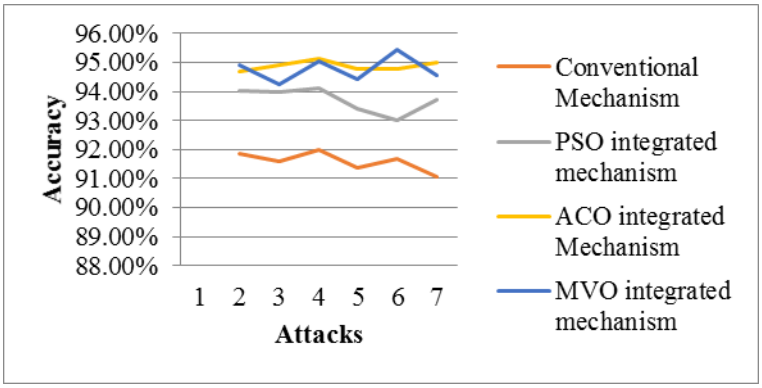

Figure 7 Comparative Analysis of Accuracy

4.3. Comparison Analysis of Error Rate

The findings of analyzing the mistake rate of finished work and the suggested further work for each of the three classes are shown in Table 3, which may be found. The conventional process has been proven to be less exact than the suggested method, which is more precise. In the case of 100 nodes, 6-time errors have been made that are influencing accuracy in the case of conventional and proposed work.

Taking into consideration the information shown in Table 3, researchers are now able to provide, in Figure 8, a comparison of the error rate produced by the Proposed Mechanisms that considers different optimization techniques and the Conventional one. The simulation presents that the error rate is high for conventional as accuracy is low for the proposed work.

Table 3 Comparative Analysis of Error Rate

Attacks	Conventional Mechanism	PSO integrated mechanism	ACO integrated Mechanism	MVO integrated mechanism
1	8.14%	5.99%	5.32%	5.08%
2	8.40%	6.04%	5.11%	5.74%
3	8.01%	5.89%	4.86%	4.97%
4	8.62%	6.61%	5.20%	5.57%
5	8.31%	6.97%	5.21%	4.56%
6	8.94%	6.30%	5.02%	5.43%

RESEARCH ARTICLE

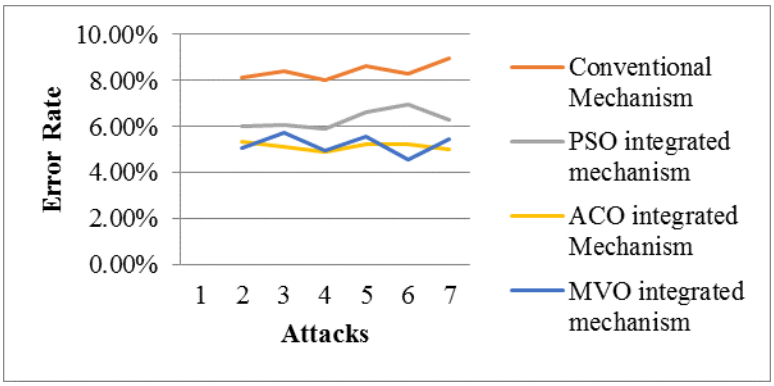

Figure 8 Comparative Analysis of Error Rate

4.4. Comparison Analysis of Precision

The comparison analysis of precision across different attacks reveals interesting insights into the performance of various mechanisms that is shown in table 4. Conventional mechanism consistently achieves a respectable level of precision across all attacks, with precision values ranging from 0.9106 to 0.9199 in table 4.

Upon integration with PSO, ACO, and MVO mechanisms, there is a notable improvement in precision across most attacks. Particularly, the ACO and MVO integrated mechanisms demonstrate the highest precision values, consistently outperforming both the conventional mechanism and the PSO integrated mechanism.

Table 4 Comparative Analysis of Precision

Attacks	Conventional Mechanism	PSO integrated mechanism	ACO integrated Mechanism	MVO integrated mechanism
1	0.9186	0.9401	0.9468	0.9492
2	0.916	0.9396	0.9489	0.9426
3	0.9199	0.9411	0.9514	0.9503
4	0.9138	0.9339	0.948	0.9443
5	0.9169	0.9303	0.9479	0.9544
6	0.9106	0.937	0.9498	0.9457

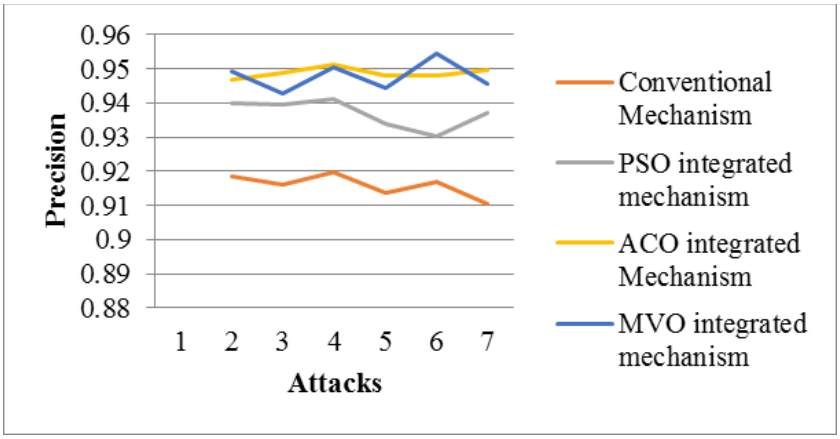

Figure.9 Comparative Analysis of Precision

RESEARCH ARTICLE

Figure 9 visualizes this comparative analysis, illustrating the precision values achieved by each mechanism across different attacks. Overall, the findings suggest that integrating optimization mechanisms such as ACO and MVO enhances the precision of the system, potentially indicating their effectiveness in mitigating security threats in the context of the analyzed attacks.

4.5. Comparison Analysis of Recall Value

The comparison analysis of recall value across various attacks provides valuable insights into the performance of different mechanisms in table 5. The conventional mechanism exhibits consistent recall values across all attacks, ranging from 0.918802 to 0.923075 in table 5.

Upon integration with PSO, ACO, and MVO mechanisms, there is a noticeable improvement in recall value across most attacks. Particularly, the ACO and MVO integrated mechanisms demonstrate the highest recall values, consistently outperforming both the conventional mechanism and the PSO integrated mechanism.

Table 5 Comparative Analysis of Recall Value

Attacks	Conventional Mechanism	PSO integrated mechanism	ACO integrated Mechanism	MVO integrated mechanism
1	0.923075	0.944934	0.952294	0.950082
2	0.921807	0.941377	0.955076	0.945947
3	0.922349	0.948814	0.95742	0.959002
4	0.919498	0.936911	0.951656	0.953434
5	0.918802	0.931107	0.948112	0.958583
6	0.919686	0.941323	0.955689	0.950807

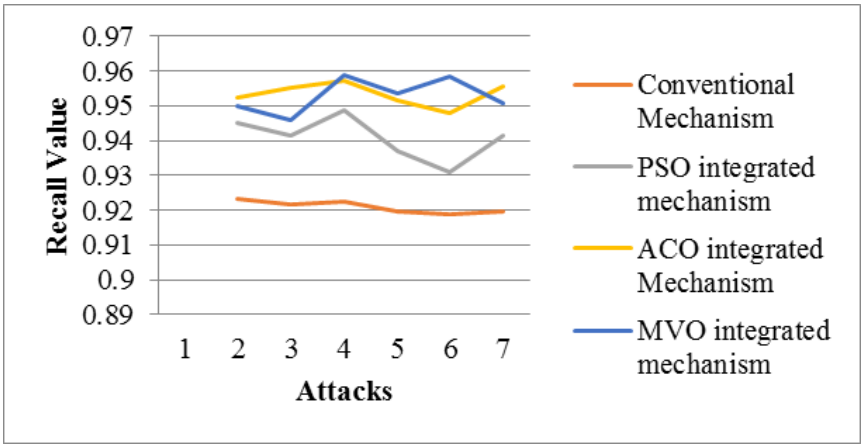

Figure 10 Comparative Analysis of Recall Value

Figure 10 illustrates this comparative analysis, showcasing the recall values achieved by each mechanism across different attacks. Overall, the results suggest that integrating optimization mechanisms such as ACO and MVO enhances the recall performance of the system, indicating their effectiveness in detecting and recalling instances of attacks in the analyzed scenarios.

4.6. Comparison Analysis of F1-Score

The comparison analysis of the F1-score provides a comprehensive evaluation of the overall performance of different mechanisms in terms of precision and recall in table 6. Across various attacks, the conventional mechanism demonstrates relatively stable F1 scores, ranging from 0.911451 to 0.91774 in table 6.

Upon integration with optimization mechanisms such as PSO, ACO, and MVO, there is a notable improvement in the F1 score across most attacks. Particularly, the ACO and MVO integrated mechanisms consistently exhibit the highest F1 scores, indicating a balanced performance in terms of precision and recall.

RESEARCH ARTICLE

Table 6 Comparative Analysis of F1-Score

Attacks	Conventional Mechanism	PSO integrated mechanism	ACO integrated Mechanism	MVO integrated mechanism
1	0.91774	0.942013	0.949921	0.944557
2	0.917939	0.933965	0.94936	0.940701
3	0.912602	0.946948	0.951153	0.952373
4	0.912989	0.929922	0.942246	0.948649
5	0.91376	0.931049	0.946031	0.958056
6	0.911451	0.933987	0.950731	0.941913

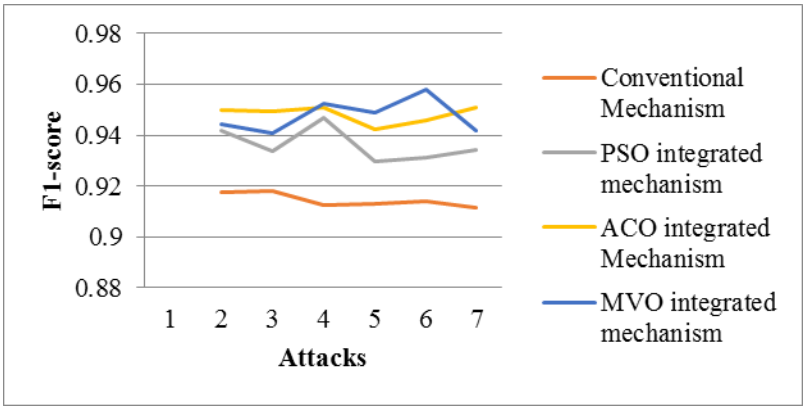

Figure 11 Comparative Analysis of F1-Score

Figure 11 visualizes this comparative analysis, illustrating the F1 scores achieved by each mechanism across different attacks. Overall, the results suggest that integrating optimization mechanisms, especially ACO and MVO, enhances the overall performance of the system in terms of achieving a balance between precision and recall, thereby improving its effectiveness in detecting and mitigating attacks in the analyzed scenarios.

5. CONCLUSION

Simulation results conclude that the proposed optimized approach provides better accuracy as compared to the conventional nonoptimized approach. Moreover, the accuracy of MVO is better than PSO and ACO. There is an emphasis on the need to implement this technology in the WSN because of the problems with the current authentication procedures and the benefits it offers. However, several obstacles must be overcome to successfully deploy blockchain in WSN. However, the WSN has limited capacity nodes and blockchain requires a lot of processing power and energy. As more and more transactions are processed, the size of the blocks grows, necessitating substantial space on the blockchain. Despite this, more work has to be done to incorporate the highly secure features of blockchain technology into WSN applications that need such features. To that end, a new authentication system built on the blockchain has been created for use in highly sensitive WSN applications. Both security and efficiency analyses showed the suggested protocol to be effective. In addition to providing a high level of safety, this research demonstrates efficiency in terms of accuracy. The study evaluates the integration of optimization techniques in wireless sensor networks (WSNs) to enhance security. Results show that Particle Swarm Optimization, Ant Colony Optimization, and Multi-Verse Optimization improve system performance, resulting in higher precision, recall, and F1-score values. These mechanisms are robust and reliable, suggesting their potential for enhancing network resilience and addressing real-world threats. Further research could lead to more efficient security solutions.

6. FUTURE SCOPE

The goal of future research is to test out alternative digital signature algorithms and employ all currently available consensus techniques. The need to use blockchain technology in the WSN is emphasized due to the drawbacks of the current authentication procedures in the WSN and the benefits it

RESEARCH ARTICLE

offers. However, several obstacles must be overcome to successfully deploy blockchain in WSN. However, the WSN has limited capacity nodes and blockchain requires a lot of processing power and energy. As more and more transactions are processed, the size of the blocks grows, necessitating substantial space on the blockchain. Despite this, more work has to be done to incorporate the highly secure features of blockchain technology into WSN applications that need such features. To that end, a new authentication system built on the blockchain has been created for use in highly sensitive WSN applications. Both security and efficiency analyses showed the suggested protocol to be effective. In addition to providing a high level of safety, this research demonstrates efficiency in terms of latency, energy, and memory use. The goal of future research is to test out other digital signature algorithms and employ all available consensus methods.

REFERENCES

[1] A. Arivarasi and P. Ramesh, "RETRACTED ARTICLE: An improved source location privacy protection using adaptive trust sector-based authentication with honey encryption algorithm in WSN," Journal of Ambient Intelligence and Humanized Computing, vol. 13, no. S1. Springer Science and Business Media LLC, pp. 9–9, Mar. 14, 2021. doi: 10.1007/s12652-021-03021-2.

[2] M. Bala Krishna and M. N. Doja, "Deterministic K- means secure coverage clustering with periodic authentication for wireless sensor networks," International Journal of Communication Systems, vol. 30, no. 4. Wiley, Sep. 24, 2015. doi: 10.1002/dac.3024.

[3] M. A. Ferrag, L. A. Maglaras, H. Janicke, J. Jiang, and L. Shu, "Authentication Protocols for Internet of Things: A Comprehensive Survey," Security and Communication Networks, vol. 2017. Hindawi Limited, pp. 1–41, 2017. doi: 10.1155/2017/6562953.

[4] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," Future Generation Computer Systems, vol. 82, pp. 395–411, May 2018, doi: 10.1016/j.future.2017.11.022.

[5] R. K. Sharma and Dr. P. Gandhi, "Estimate reliability of component-based software system using modified neuro-fuzzy model," International Journal of Engineering & Technology, vol. 6, no. 2. Science Publishing Corporation, p. 45, May 24, 2017. doi: 10.14419/ijet.v6i2.7722.

[6] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security Services Using Blockchains: A State of the Art Survey," IEEE Communications Surveys & Tutorials, vol. 21, no. 1. Institute of Electrical and Electronics Engineers (IEEE), pp. 858–880, 2019. doi: 10.1109/comst.2018.2863956.

[7] C. V. Nguyen, M. T. Nguyen, T. T. H. Le, T. A. Tran, and D. T. Nguyen, "Blockchain Technology in Wireless Sensor Network: Benefits and Challenges," *ICSES Trans. Comput. Netw. Commun.*, pp. 1-4, 2021.

[8] C. H. Liu and Y. F. Chung, "Secure user authentication scheme for wireless healthcare sensor networks," *Comput. Electr. Eng.*, pp. 250-261, 2017.

[9] R. Riaz, N. A. Gillani, S. Rizvi, S. Shokat, and S. L. Kwon, "SUBBASE: An Authentication Scheme for Wireless Sensor Networks Based on User Biometrics," *Wirel. Commun. Mob. Comput.*, pp. 6370742, 2019.

[10] Y. Lu, J. Zhai, R. Zhu, and J. Qin, "Study of Wireless Authentication Center with Mixed Encryption in WSN," *J. Sens.*, vol. 2016, article 9297562, 2016.

[11] R. K. Sharma and P. Gandhi, "Study of Reliability of Object-Oriented Structure Consuming CK Metrics," in *2019 6th International Conference on Computing for Sustainable Global Development (INDIACom)*, pp. 828-831, Mar. 2019.

[12] X. Zhang and F. Wen, "A novel anonymous user WSN authentication for Internet of Things," *Soft Comput.*, vol. 23, pp. 5683-5691, 2019.

[13] T. A. Alghamdi and N. Javaid, "Energy optimization with authentication and cost-effective storage in the wireless sensor IoTs using blockchain," Computational Intelligence, vol. 40, no. 1. Wiley, Feb. 2024. doi: 10.1111/coin.12630.

[14] R. Vatambeti, E. S. P. Krishna, M. G. Karthik, and V. K. Damera, "Securing the medical data using enhanced privacy preserving based blockchain technology in the Internet of Things," Cluster Computing, vol. 27, no. 2. Springer Science and Business Media LLC, pp. 1625–1637, Jun. 02, 2023. doi: 10.1007/s10586-023-04056-0.

[15] J. Xiao, C. Li, Z. Li, and J. Zhou, "BS-SCRM: a novel approach to secure wireless sensor networks via blockchain and swarm intelligence techniques," Scientific Reports, vol. 14, no. 1. Springer Science and Business Media LLC, Apr. 27, 2024. doi: 10.1038/s41598-024-60338-6.

[16] M. A. de Jesus et al., "Security in Blockchain- Based Smart Cyber- Physical Applications Relying on Wireless Sensor and Actuators Networks," Applying Artificial Intelligence in Cybersecurity Analytics and Cyber Threat Detection. Wiley, pp. 279–310, Mar. 22, 2024. doi: 10.1002/9781394196470.ch14.

[17] Sureshkumar, C.; Sabena, S. Fuzzy-Based Secure Authentication and Clustering Algorithm for Improving the Energy Efficiency in Wireless Sensor Networks. Wirel. Pers. Commun. 2020, 112, pp. 1517–1536.

[18] Bao, Z.; Shi, W.; He, D.; Choo, K.R. IoTChain: A Three-Tier Blockchain-based IoT Security Architecture. arXiv 2018, arXiv:1806.02008v2.

[19] Sharma, R. K., & Gandhi, P. (2016, March). Quality assurance of component-based software systems. In 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom) (pp. 3850-3854). IEEE.

[20] Yavari, M.; Safkhani, M.; Kumari, S.; Kumar, S.; Chen, C.M. An Improved Blockchain-Based Authentication Protocol for IoT Network Management. Secure. Commun. Netw. 2020, 2020, 8836214.

[21] Alan, C.H.L.; Yeung, K.H.; Yan, F. Blockchain-based authentication in IoT networks. In Proceedings of the 2018 IEEE Conference on Dependable and Secure Computing (DSC), Kaohsiung, Taiwan, 10–13 December 2018; pp. 1–8.

[22] Uddin, M.A.; Stranieri, A.; Gondal, I.; Balasubramanian, V. A Lightweight Blockchain Based Framework for Underwater IoT. Electronics 2019, 8, 1552.

[23] Gandhi, P., Khan, M. Z., Sharma, R. K., Alhazmi, O. H., Bhatia, S., &Chakraborty, C. (2022). Software Reliability Assessment Using Hybrid Neuro-Fuzzy Model. Computer Systems Science & Engineering, 41(3).

[24] Dong, S.; Yang, H.; Yuan, J.; Jiao, L.; Yu, A.; Zhang, J. Blockchain-based cross-domain authentication strategy for trusted access to mobile devices in the IoT. In Proceedings of the 2020 International Wireless Communications and Mobile Computing (IWCMC), Limassol, Cyprus, 15–19 June 2020; pp. 1–3.

[25] Goyat, R.; Kumar, G.; Saha, R.; Conti, M.; Rai, M.K.; Thomas, R.; Alazab, M.; Hoon-Kim, T. Blockchain-based Data Storage with Privacy and Authentication in Internet-of-Things. IEEE Internet Things J. 2020, 9, 14203–14215.

[26] Yazdinejad, A.; Parizi, R.M.; Srivastava, G.; Dehghantanha, A.; Choo, K.K.R. Energy efficient decentralized authentication in the internet of underwater things using blockchain. In Proceedings of the 2019 IEEE Globecom Workshops (GC Wkshps), Waikoloa, HI, USA, 9–13 December 2019; pp. 1–6.

[27] Hong, S. P2P networking-based Internet of Things (IoT) sensor node authentication by blockchain. Peer-Peer Netw. Appl. 2020, 13, pp. 579–589.

[28] Almadhoun, R.; Kadadha, M.; Alhemeiri, M.; Alshehhi, M.; Salah, K. A User Authentication Scheme of IoT Devices using Blockchain-enabled Fog Nodes. In Proceedings of the 2018 IEEE/ACS 15th International Conference on Computer Systems and Applications (AICCSA), Aqaba, Jordan, 28 October–1 November 2018; pp. 1–8.

RESEARCH ARTICLE

[29] Rathod, T.; Jadav, N.K.; Alshehri, M.D.; Tanwar, S.; Sharma, R.; Felseghi, R.-A.; Raboaca, M.S. Blockchain for Future Wireless Networks: A Decade Survey. Sensors 2022, 22, 4182, https://doi.org/10.3390/s22114182.

[30] K. Suresh Kumar, R. Rajeswari, Ch Vidyadhari, and B. Santhosh Kumar. "Mathematical modeling approaches for blockchain technology." In IOP conference series: materials science and engineering, vol. 981, no. 2, p. 022001. IOP Publishing, 2020.

[31] Sharma C, Vaid R. "Analysis of existing protocols in WSN based on key parameters" In Proceedings of 2nd international conference on communication, computing and networking, Volume16, PP.165171, ISSN (electronic):2367-3389.Springer, Singapore,2019.

[32] Sharma C, Vaid R." A Novel Sybil Attack Detection and Prevention Mechanism for Wireless Sensor Network. In 2021 6th International Conference on Signal Processing, Computing and Control (ISPCC) 2021 Oct 7 pp.340-345.IEEE.

[33] Sharma C.Vaid R "Energy –Efficient and Secure Data Forwarding Mechanism for Balancing Cluster Lifetime for Huge Size Wireless Sensor Network' Journal of Computational and Theoretical Nanoscience, Volume 16, No 9, pp. 3961-3964, ISSN (Online):1546-1955, September 2019.

[34] Sharma C., Vaid R. and Gupta K "KDS: Keyless Data Security in Wireless Sensor Networks" 3rd International Conference on 'Mobile Radio Communications & 5G Network (MRCN-2022) in University Institute of Engineering &Technology, Kurukshetra University, Volume588, pp 613-624, Springer, Singapore. https://doi.org/10.1007/978-981-19-7992-8_51.

[35] Tejbir Singh, Rohit Vaid, and Avinash Sharma. "Security Issues in Blockchain Integrated WSN: Challenges and Concerns." In 2022 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES), DOI:10.1109/ICSES55317.2022.9914006 pp. 1-5. IEEE, 2022.

[36] Mohd Younus Dar and Tejbir Singh. "Study of Security to Block Chain under Wireless Sensor Network (WSN)". International Journal of Wireless Network Security, Volume 7, Issue 2, PP. 1-7, Journal Pub, 2021.

[37] Singh, T., Vaid, R. (2023). Enigmas of Various Techniques to Implementing Authentication and Integrity in Blockchain-Based Wireless Sensor Networks. Lecture Notes in Electrical Engineering, vol 1040. Springer, Singapore. https://doi.org/10.1007/978-981-99-2271-0_29.

Authors

Mr. Tejbir Singh has received his Bachelor of Science from BDCB ,Saharanpur, Uttar Pradesh ,India and completed his M.Tech degree from Department of Computer Science & Engineering, MM Engineering College, Maharishi Markandeshwar (Deemed to be University) Mullana, Ambala, Haryana, India. He is a research scholar at Computer Science & Engineering, MM Engineering College, Maharishi Markandeshwar (Deemed to be University) Mullana, Ambala, Haryana, India. Currently, he is working as Assistant Professor in Maharishi Markandeshwar (Deemed to be University) Mullana, Ambala, Haryana, India. His interests lie in the areas of Blockchain and Wireless Sensor Network. He has published 15 research papers in International Journals and Conferences.

Dr. Rohit Vaid is working as an Associate Professor in the Department of computer Science & Engineering, M.M Engineering College, M. M. (Deemed to University), Mullana, Ambala. He received his Ph. D degree in year 2016 and M. Tech (Gold Medalist) degree in 2009 both from Maharishi Markandeshwar University, Mullana, Ambala (Haryana) respectively. He supervised 34 M. Tech and 3 Ph.D candidates. One of his research scholar has submit her Ph.D thesis in the month of May 2024. Currently he is supervising 4 Ph.D research scholars. He has about 34 publications in International Journals and Conferences. His research area includes Wireless Communications, Mobile Ad hoc & Sensor based Networks Security and Block Chain Technology.

How to cite this article:

Tejbir Singh, Rohit Vaid, "Preserving Security in Terms of Authentication on Blockchain-Based Wireless Sensor Network (WSN)", International Journal of Computer Networks and Applications (IJCNA), 11(3), PP: 390-406, 2024, DOI: 10.22247/ijcna/2024/25.