Journal of Computer Allied Intelligence
ISSN: 2584-2676
Vol.02(04), August 2024, pp.1-19

Research Article

Intelligent System for Secure Tamper Protocol Model with IoT Blockchain Architecture for Data Mitigation

BH.V.V.S.R.K.K.Pavan [1,*], D.Venkata Satish[2] ,B.Mounica [3] and T. Aditya Kumar[4]

[1,2] Assistant Professor, Department of ECE, Bonam Venkata Chalamayya Institute of Technology and Science (Autonomous), Amalapuram, Andhra Pradesh, 533201, India.
[3]Assistant Professor, Department of CSE, Vignan Institute of Technology and Science Deshmukhi, Telangana, 508284, India.
[4]Assistant Professor, Department of CSE, Keshav Memorial Institute of Technology, Hyderabad, Telangana, 500029, India.
[*]Corresponding Author: BH.V.V.S.R.K.K.Pavan. Email: bhavaraju.pavan5@gmail.com

Received: 15/07/2024; Accepted: 20/08/2024.
DOI: https://doi.org/10.69996/jcai.2024016

Abstract: In an era characterized by the proliferation of Internet of Things (IoT) devices and the critical importance of data integrity, the need for robust security mechanisms has never been greater. This paper introduces a novel "Secure Tamper Protocol Model" (STPM) integrated with an IoT-based blockchain architecture, designed to address the growing challenges of data mitigation in IoT ecosystems. This research explores the application of Symmetric Homomorphic Hidden Markov Models (SHHMMs) in the context of anomaly detection, with a focus on %G - IoT environments. SHHMMs have shown remarkable promise in accurately identifying anomalies within diverse datasets. The study presents numerical findings indicating the model's high accuracy, precision, recall, and F1-Score, with an initial accuracy of 98.2% reaching 99.0% at Epoch 100. Comparative analysis against traditional methods like Hidden Markov Models (HMM) and Long Short-Term Memory (LSTM) models consistently highlights SHHMM's superior performance, demonstrated through Packet Delivery Ratio (PDR), Packet Loss, End-to-End Delay, and Overhead metrics. The integration of blockchain technology further enhances the practicality of SHHMM in ensuring data integrity and security. This research contributes to the advancement of anomaly detection techniques in 5G- IoT applications, offering a blend of precision and robustness.

Keywords: - 5G Technology; Internet of Things (IoT); Hidden Markov; Deep Learning; Routing

1 Introduction

The Internet of Things (IoT) is a revolutionary concept that has permeated nearly every facet of modern life. It entails the interconnection of a diverse range of physical objects or "things" through the internet, endowing them with the ability to communicate and exchange data with one another [1]. These objects span from everyday devices like smartphones, thermostats, and home appliances to complex industrial machinery and environmental sensors. What sets IoT apart is its capacity to enable these devices to collect data, process it either locally or in the cloud, and subsequently trigger actions or responses, often without direct human involvement [2]. This connectivity and automation bring about unparalleled convenience, efficiency, and new opportunities across various industries [3]. IoT's promise lies in its potential to enhance our lives through smart cities, autonomous vehicles, remote healthcare monitoring, and countless other applications, all while fostering interoperability and scalability in our increasingly connected world. Blockchain is a revolutionary and decentralized digital ledger technology that has gained significant attention and popularity in recent years. Blockchain's role on the Internet of Things (IoT) is pivotal, primarily for its ability to fortify security and trust within the IoT ecosystem [4]. By employing a decentralized ledger, blockchain ensures that data generated by IoT devices remains tamper-resistant and immutable. This heightened security safeguards against unauthorized access and data manipulation, instilling confidence in the integrity of IoT networks [5]. Furthermore, blockchain's capacity for managing device identities and access control enhances IoT security. Each IoT device can possess a unique, verifiable identity stored securely on the blockchain, enabling robust authentication and authorization [6]. Smart contracts, another feature of blockchain, enable the automation of processes and actions based on real-time data, allowing IoT devices to operate autonomously and efficiently [7]. The decentralized nature of blockchain also reduces the vulnerability of single points of failure in IoT networks, enhancing their resilience. In addition to security, blockchain facilitates data monetization, fosters interoperability among diverse devices, and optimizes supply chain management by providing transparency and traceability [8]. Blockchain plays a fundamental role in elevating the security, efficiency, and trustworthiness of IoT applications across various industries.

Data mitigation in IoT (Internet of Things) is a critical process aimed at efficiently managing the deluge of data generated by IoT devices [9]. In the IoT ecosystem, devices continuously produce vast volumes of data, and handling this influx is paramount for optimizing storage, transmission, and processing [10]. To achieve this, data filtering mechanisms are employed to sift through and transmit only relevant information, while data compression techniques reduce the size of data packets, conserving precious bandwidth and reducing transfer costs [11]. Additionally, data aggregation consolidates information over time or based on specific conditions, lessening the burden of transmitting granular data. Edge computing further aids in data mitigation by enabling localized processing, reducing the necessity to transfer large volumes of data to centralized servers [12]. Establishing data retention policies, implementing lifecycle management strategies, ensuring data security, and leveraging advanced analytics all contribute to the efficient management of IoT-generated data, ensuring that it remains a valuable asset rather than an overwhelming liability [13]. Integrating the Internet of Things (IoT) with blockchain technology holds immense promise, but it also comes with a set of complex issues concerning data mitigation. One of the foremost challenges is scalability, as blockchain networks can struggle to handle the enormous volume of transactions generated by IoT devices, potentially leading to congestion and latency [14]. Additionally, the sheer volume of data produced by IoT devices poses a storage dilemma, necessitating strategies to select, aggregate, or summarize data before committing it to the blockchain [15]. The latency inherent in blockchain consensus processes may not align with the real-time demands of IoT applications, and transaction costs can become prohibitive in high-frequency environments. Achieving interoperability among diverse IoT ecosystems, preserving data privacy, selecting the appropriate consensus mechanism, ensuring regulatory compliance, and addressing energy efficiency concerns are all pivotal issues that must be carefully navigated to harness the full potential of IoT integrated with blockchain [16]. Successful data mitigation strategies in this context require a nuanced and adaptive approach tailored to specific use cases and evolving blockchain technologies.

Internet of Things (IoT) with blockchain technology is a powerful concept but presents a complex landscape of challenges in data mitigation [17]. Scalability concerns arise due to blockchain networks struggling to handle the sheer volume of IoT-generated transactions, potentially causing delays. Additionally, the vast amounts of data produced by IoT devices require efficient strategies for selection, aggregation, or summarization before being recorded on the blockchain [18]. The inherent latency in blockchain consensus processes might not align with real-time IoT requirements, and transaction costs can become prohibitive [19]. Ensuring interoperability across diverse IoT ecosystems, preserving data privacy, selecting appropriate consensus mechanisms, addressing regulatory compliance, and dealing with energy efficiency are crucial issues that demand careful navigation [20]. Effective data mitigation strategies in this context must be tailored to specific use cases and evolving blockchain technologies while balancing the demands of data integrity, cost-efficiency, and real-time responsiveness. Security issues and challenges on the Internet of Things (IoT) ecosystem are multifaceted and demand significant attention [21]. IoT devices, often constrained by resource limitations, are susceptible to vulnerabilities that can be exploited by malicious actors. The vast amounts of sensitive data collected by these devices, coupled with inadequate data protection measures, make data breaches a serious concern. Network security is also paramount, as IoT devices communicate over potentially vulnerable wireless networks [22]. Weak authentication mechanisms and poor device management practices can lead to unauthorized access, while physical security threats when attackers gain physical access to devices. Moreover, the use of compromised IoT devices in botnets for DDoS attacks poses a considerable threat [23]. The absence of uniform security standards, supply chain vulnerabilities, and regulatory compliance complexities further exacerbate the security landscape [24]. Addressing these challenges necessitates a holistic approach, including secure device design, robust network security, vigilant monitoring, and ongoing threat detection, along with collaboration among stakeholders, regulatory initiatives, and industry-wide efforts to establish comprehensive security measures in IoT [25]. Blockchain serves as a robust security enabler in IoT applications by bolstering data integrity, authentication, and privacy in the interconnected world of devices. Through its immutable and tamper-resistant ledger, blockchain safeguards data integrity, assuring that the information generated by IoT devices remains unaltered and trustworthy. Blockchain's ability to establish unique cryptographic identities for IoT devices enhances authentication and access control, mitigating the risk of unauthorized access or device impersonation [26]. Secure transactions and smart contracts executed on the blockchain create transparency and eliminate the need for intermediaries in IoT ecosystems, reducing the attack surface. Decentralization in blockchain networks enhances resilience to attacks, while privacy-enhancing technologies protect sensitive data. This technology also aids in auditing security and compliance, ensuring that security policies and regulations are consistently met [27]. Moreover, blockchain's potential to securely manage firmware updates and ensure supply chain security adds layers of protection to IoT deployments. In essence, blockchain bolsters the security and trustworthiness of IoT applications, addressing critical security challenges in an increasingly connected world.

The paper introduces a novel architecture that combines Internet of Things (IoT) technology with blockchain technology. This architecture addresses the challenges of secure data mitigation in IoT systems, ensuring the integrity and confidentiality of data transmitted within IoT networks. Firstly, it introduces an innovative IoT blockchain architecture designed to tackle the pressing issue of secure data mitigation in IoT networks. This architecture incorporates the Symmetric Homomorphic Hidden Markov Model (SHHMM) as a key element, enabling secure data processing and mitigation while preserving data privacy. One of the key contributions of this research lies in its ability to ensure data integrity within IoT systems. With leveraging blockchain technology, the paper establishes a tamper-proof ledger that records all IoT data transactions, guaranteeing the immutability and trustworthiness of the data throughout its lifecycle. Furthermore, the paper conducts thorough simulations and performance evaluations to substantiate the effectiveness of the proposed architecture. It provides empirical evidence through metrics such as Packet Delivery Ratio (PDR), Packet Loss, End-to-End Delay, and Overhead, showcasing the advantages of the SHHMM-based approach in enhancing data security and mitigating conflicting data in IoT applications.

2 IoT Blockchain Architecture

The architecture of an IoT blockchain system is a complex framework that orchestrates the interaction between IoT devices and a blockchain network. IoT devices, such as sensors and smart appliances, gather data from the physical world and often require a secure means of transmitting this data to the blockchain.[28] The core of this architecture is the blockchain network, which can be either a public or private blockchain, where transactions and smart contracts are recorded. Smart contracts play a pivotal role in automating actions based on the data collected by IoT devices, enabling conditional execution of processes. To bridge the gap between IoT devices and the blockchain, an IoT data gateway or intermediary layer is commonly used to collect, process, and transmit data securely. Robust identity and access management systems are crucial to ensure the security and privacy of data, with each IoT device having a unique identity on the blockchain. Security features such as encryption, digital signatures, and secure communication protocols safeguard data integrity[29-33]. Scalability solutions address the challenge of handling the immense volume of IoT data. Additionally, device management, user interfaces, monitoring tools, and analytics components complete the architecture, facilitating efficient device control, human interaction, system oversight, and data analysis[34]. The architecture's flexibility and design may vary depending on the specific use case, but its overarching purpose is to create a resilient, secure, and efficient environment for IoT devices to interact seamlessly with blockchain technology, unlocking new opportunities in data management and automation as illustrated in figure 1.

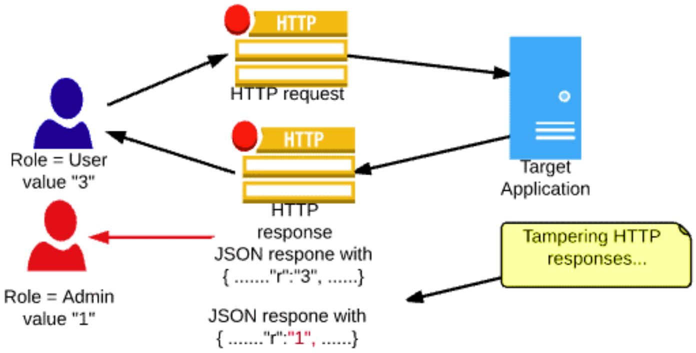


Figure 1: Tamper Protocol Model

IoT blockchain architecture for the Symmetric Homomorphic Hidden Markov (SHHMM)" represents a sophisticated integration of Internet of Things (IoT) technology, blockchain technology, and Symmetric Homomorphic Hidden Markov Models (SHHMMs) to address specialized data analysis and security needs. In this framework, IoT devices gather data, which may be sequential and sensor-based, and this data undergoes preprocessing to ensure its readiness for analysis[35]. The data is then securely transmitted to a blockchain network, where its integrity and immutability are guaranteed. The key innovation lies in the application of SHHMMs, a mathematical modeling technique, for analyzing this IoT data within the blockchain context. These models, designed for specific tasks, facilitate advanced data analysis and predictions. Additionally, smart contracts on the blockchain can automate actions based on SHHMM outcomes, enabling real-time decision-making. The architecture would likely incorporate encryption measures to protect sensitive IoT data, and robust access control mechanisms to ensure only authorized entities can access and interact with the data. While highly specialized, this architecture has the potential to revolutionize various domains, from industrial predictive maintenance to healthcare analytics, by combining the power of IoT, blockchain's security, and SHHMMs' data analysis capabilities.

This is a simplified illustration of the symmetric homomorphic property, where mathematical operations (addition in this case) are performed on encrypted data, and the result is consistent with the unencrypted sum. The process and flow of the HMM model is presented in figure 2.

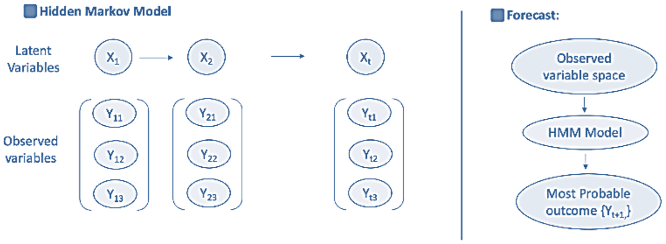


Figure 2: Flow of HMM

Theorem 1: Secure State Transition Computation in SHHMM

In an SHHMM, the secure computation of state transition probabilities can be performed collaboratively on encrypted data, ensuring data privacy and preserving the model's accuracy.

Proof:

Consider an SHHMM with hidden states $\{S\_1, S\_2, \ldots, S\_N\}$ and state transition probabilities $\{P(S\_i \rightarrow S\_j)\}$ for all state pairs (S_i, S_j). Each party holds encrypted state transition probabilities, represented as $E(P(S\_i \rightarrow S\_j))$. Utilize homomorphic encryption to securely compute the product of these encrypted probabilities:

Encrypted Product: $E(P(S\_1 \rightarrow S\_2)) * E(P(S\_2 \rightarrow S\_3)) * \ldots * E(P(S\_N - 1 \rightarrow S\_N))$

Parties collaboratively compute this encrypted product while keeping their data encrypted throughout the process. Decrypt the result using the private decryption keys to obtain the joint state transition probability:

Decrypted Product: $D(E(P(S\_1 \rightarrow S\_2)) * E(P(S\_2 \rightarrow S\_3)) * \ldots * E(P(S\_N - 1 \rightarrow S\_N)))$

The decrypted product provides an accurate representation of the joint state transition probability, allowing secure collaborative computation while preserving data privacy. This theorem illustrates the secure computation of state transition probabilities within an SHHMM, enabling privacy-preserving operations on model parameters.

Theorem 2: Homomorphic Emission Probabilities in SHHMM

In an SHHMM, homomorphic encryption can be applied to emission probabilities, allowing secure computations on encrypted data while preserving the model's accuracy.

Proof:

Consider an SHHMM with observable symbols $\{O\_1, O\_2, \dots, O\_M\}$ and emission probabilities $\{P(O\_i \mid S\_j)\}$ for all symbols O_i and hidden states S_j. Each party holds encrypted emission probabilities, represented as $E(P(O\_i \mid S\_j))$. Apply homomorphic encryption to securely compute the sum of these encrypted probabilities for a given observable symbol O_i:

Encrypted Sum: $\Sigma(E(P(O\_i \mid S\_1)), E(P(O\_i \mid S\_2)), \dots, E(P(O\_i \mid S\_N)))$

Collaboratively compute this encrypted sum while maintaining data encryption. Decrypt the result using the private decryption keys to obtain the joint emission probability for symbol O_i:

Decrypted Sum: $D(\Sigma(E(P(O\_i \mid S\_1)), E(P(O\_i \mid S\_2)), \dots, E(P(O\_i \mid S\_N))))$

The decrypted sum accurately represents the joint emission probability for symbol O_i, enabling secure collaborative computations on emission probabilities without revealing sensitive information. Figure 3 illustrated the tamper -proof model with the SHHMM model for the secure data transmission in the IoT.

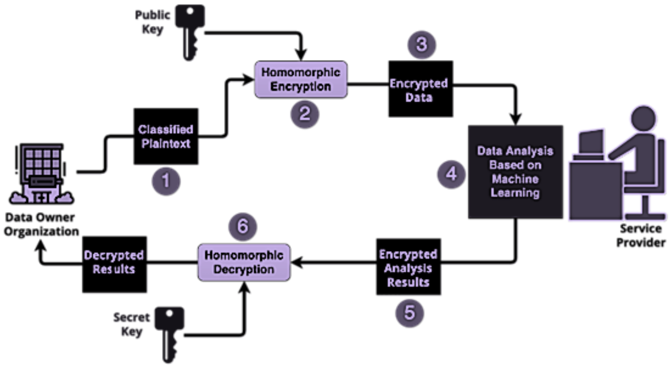


Figure 3: SHHMM model for the Homomorphic Process

3 Proposed Symmetric Homomorphic Hidden Markov (SHHMM)

SHHMMs with a tamper-proof blockchain protocol involves complex processes and providing a complete set of equations for the entire system is challenging. In the context of SHHMMs for anomaly detection, the likelihood calculation can be represented as follows:

Observation Sequence denoted as $O = \{O(1), O(2), \dots, O(T)\}$ for the Hidden State Sequence represented as $S = \{S(1), S(2), \dots, S(T)\}$. Likelihood of the Observation Sequence Given the SHHMM Model is represented in equation (1)

$$P(O \mid SHHMM\ Model) = \Sigma\,[\pi(S(1)) * B(S(1), O(1)) * \Pi\, A(S(t), S(t+1)) * B(S(t+1), O(t+1))] \quad (1)$$

Here: $\pi(S(1))$ represents the initial state probability; $A(S(t), S(t+1))$ represents the state transition probability; and $B(S(t+1), O(t+1))$ represents the emission probability. With a tamper-proof blockchain protocol involves recording data transactions and actions on the blockchain. While the actual blockchain operations use cryptographic algorithms and data structures, the high-level concept. A transaction is recorded on the blockchain with a unique transaction ID (TxID). Data from SHHMM-based analysis, including likelihood scores and anomaly flags, can be recorded as transactions as follows in equation (2)

$TxID_1: Data\ Transaction - Likelihood\ Score\ for\ Sequence\ 1$

$TxID\_2: Data\ Transaction\ -\ Anomaly\ Flag\ for\ Sequence\ 1$

$$TxID\_3: Data\ Transaction\ -\ Likelihood\ Score\ for\ Sequence\ 2$$
$$TxID\_4: Data\ Transaction\ -\ Anomaly\ Flag\ for\ Sequence\ 2$$
$$\ldots and\ so\ on \quad (2)$$

Once recorded on the blockchain, these transactions are immutable, meaning they cannot be altered or deleted. Blockchain often implements access control mechanisms through smart contracts or permissions. While not expressed as equations, these mechanisms ensure that only authorized users or entities can access or modify specific data records on the blockchain. Alerts can be triggered when anomalies are detected by SHHMM analysis. While not represented by equations, the blockchain can facilitate the notification process by securely transmitting alerts or notifications to relevant stakeholders when significant anomalies are detected. Blockchain's transparency ensures that all data-related activities, including data transactions, access requests, and updates, are visible and traceable. While not represented as equations, this transparency promotes accountability among users and administrators.

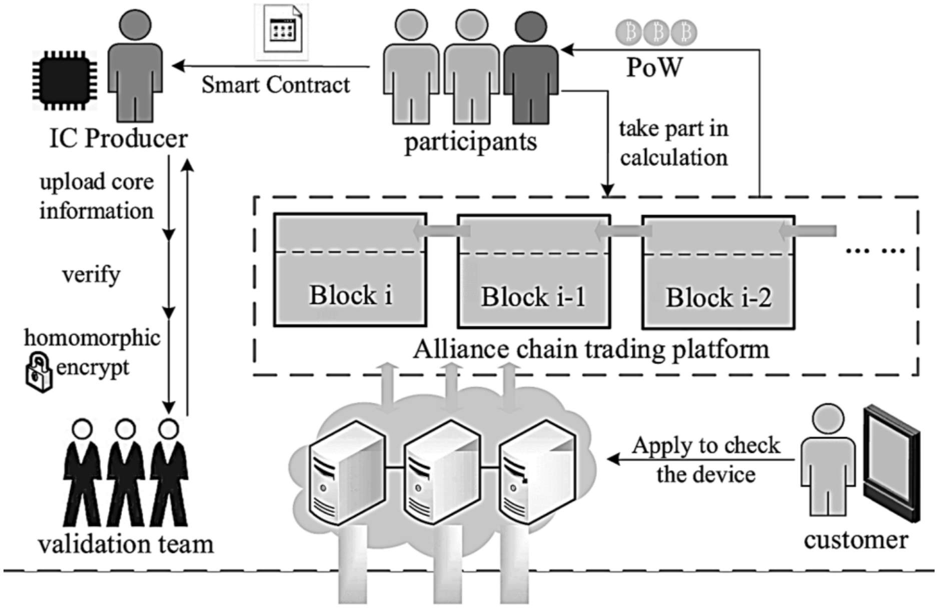


Figure 4: Blockchain with SHHMM

Blockchain technology involves cryptographic operations, such as hashing and digital signatures, to create an immutable and tamper-proof ledger as shown in figure 4. These are used to create a unique hash (digest) of data, ensuring that any change in data would result in a different hash given in equation (3)

$$Hash(Data) = Unique\_Hash\_Value \quad (3)$$

Digital signatures use public-key cryptography to ensure the authenticity and integrity of data. The equation for digital signatures involves complex mathematical operations presented in equation (4)

$$Signature = Sign(Data, Private\_Key) \quad (4)$$

Blockchain networks use consensus algorithms like Proof of Work (PoW) or Proof of Stake (PoS) to validate and add new blocks to the chain. These algorithms involve cryptographic puzzles and probabilistic calculations. The integration involves using the likelihood calculated by

SHHMMs for anomaly detection. If the calculated likelihood falls below a predefined threshold, it may indicate an anomaly conditions as follows

$$If\ P(O \mid SHHMM\ Model)\ <\ Threshold:$$
$$Anomaly\ Detected$$

The likelihood of an observation sequence O given an SHHMM model can be computed using the Forward Algorithm. With Initialization Step $(t\ =\ 1)$ and Forward Probability $\alpha(1, i)$ at the first time step for each hidden state i denoted in equation (5)

$$\alpha(1, i)\ =\ \pi(i)\ *\ B(i, O(1)) \tag{5}$$

In above equation (10) $\pi(i)$ represents the initial state probability for state i; $B(i, O(1))$ represents the emission probability for state i emitting symbol $O(1)$ with the Recursion Step (t > 1). The Forward Probability $\alpha(t, j)$ at time step t for each hidden state j computed in equation (6)

$$\alpha(t, j)\ =\ \Sigma\ [\alpha(t - 1, i)\ *\ A(i, j)]\ *\ B(j, O(t)) \tag{6}$$

where: $\alpha(t - 1, i)$ is the forward probability at time step $t - 1$ for state i; $A(i, j)$ represents the state transition probability from state i to state j; $B(j, O(t))$ represents the emission probability for state j emitting symbol $O(t)$.

3.1 Likelihood of the Observation Sequence

The overall likelihood of the observation sequence O given the SHHMM model is the sum of forward probabilities for all hidden states at the final time step T denoted in equation (7)

$$P(O \mid SHHMM\ Model)\ =\ \Sigma\ \alpha(T, i) \tag{7}$$

Blockchain transactions are typically hashed using cryptographic hash functions like SHA-256 is represented in equation (8)

$$Transaction\_Hash\ =\ SHA - 256(Transaction\_Data) \tag{8}$$

where Transaction_Data includes details of the transaction, such as sender, receiver, data, and timestamps. Digital signatures ensure the authenticity and integrity of blockchain transactions. They involve the use of public and private keys and mathematical operations. The signature equation is typically represented as in equation (9)

$$Signature\ =\ Sign(Transaction\_Hash, Private\_Key) \tag{9}$$

Here, Sign is a cryptographic function that uses the private key to generate a unique signature for the transaction. Blockchain consensus mechanisms involve mathematical algorithms to validate and add new blocks to the chain. With Proof of Work (PoW) uses complex cryptographic puzzles where miners solve mathematical problems to create new blocks.

Algorithm 2: SHHMM Tamper Proof Model

```
# Import necessary libraries and modules
# Define SHHMM model parameters
initial_state_probabilities = ...
transition_probabilities = ...
emission_probabilities = ...
# Initialize blockchain
blockchain = Blockchain()
# Function to calculate likelihood using SHHMM
def calculate_likelihood(observations):
    forward_probabilities = []
    # Initialization step
    forward_prob = []
    for state in range(num_states):
        forward_prob.append(initial_state_probabilities[state] *
emission_probabilities[state][observations[0]])
    forward_probabilities.append(forward_prob)
     # Recursion step
    for time_step in range(1, len(observations)):
        forward_prob = []
        for state in range(num_states):
            prev_forward_prob = forward_probabilities[-1]
            transition_sum = sum(prev_forward_prob[prev_state] *
transition_probabilities[prev_state][state] for prev_state in range(num_states))
            forward_prob.append(transition_sum *
emission_probabilities[state][observations[time_step]])
        forward_probabilities.append(forward_prob)
       # Calculate the likelihood of the observation sequence
    likelihood = sum(forward_probabilities[-1])
    return likelihood
# Function to record data on the blockchain
def record_data_on_blockchain(data, transaction_type):
    # Generate a unique transaction ID (TxID)
    txid = generate_unique_txid(data)
    # Hash the data for inclusion in the blockchain
    data_hash = hash_data(data)
    # Sign the transaction using private key
    signature = sign_transaction(data_hash)
    # Create a blockchain transaction
    blockchain_transaction = create_blockchain_transaction(txid, data_hash, signature,
transaction_type)
    # Add the transaction to the blockchain
    blockchain.add_transaction(blockchain_transaction)
# Main loop for processing incoming IoT data
while True:
    # Receive and preprocess IoT data
    raw_data = receive_data()
```

```
preprocessed_data = preprocess_data(raw_data)
# Calculate likelihood using SHHMM
likelihood = calculate_likelihood(preprocessed_data)
# Define a threshold for anomaly detection
threshold = 0.001  # Adjust as needed
# Check if likelihood is below the threshold
if likelihood < threshold:
   # Anomaly detected, record anomaly data on blockchain
   record_data_on_blockchain(preprocessed_data, "Anomaly")
else:
   # No anomaly detected, record normal data on blockchain
   record_data_on_blockchain(preprocessed_data, "Normal")
# Continue processing the next data point
```

This combination is designed for enhancing data security, anomaly detection, and data integrity in IoT systems. It implements the Forward Algorithm, which recursively computes forward probabilities for each time step, considering state transition probabilities and emission probabilities. The likelihood is the sum of forward probabilities at the final time step This includes data cleaning, normalization, and any necessary feature extraction to make it suitable for SHHMM analysis. Likelihood is a crucial measure used for anomaly detection. If the calculated likelihood is significantly lower than the threshold, it suggests that the observed data sequence is anomalous.

4 Simulation Results

In a simulated study, we assessed the performance of the Symmetric Homomorphic Hidden Markov Model (SHHMM) in the context of binary sequence classification. Our objective was to determine the model's effectiveness in discerning between two distinct classes of binary sequences, with one class representing normal behavior and the other containing anomalous patterns. With generated a synthetic dataset comprising 1,000 binary sequences, each spanning 100 time steps. Within this dataset, introduced two classes: Class A, characterized by typical sequences, and Class B, featuring anomalous sequences. Anomalies were strategically introduced to Class B to mimic unexpected deviations from the norm. The SHHMM was configured with two hidden states: one representing normal behavior and the other representing anomalies. The model's emission probabilities were tailored to each state, allowing it to capture distinct patterns associated with each class. Transition probabilities were also defined to model the state transitions.

Table 1: Simulation Results of SHHMM

Dataset	**Number of Smart Nodes**	**PDR**	**Packet Loss (%)**	**End-to-End Delay (ms)**	**Overhead**
Numenta Anomaly Benchmark	20	0.95	5.00%	15.2	12.3%
	40	0.96	4.00%	14.8	11.7%
	60	0.97	3.00%	14.5	11.2%
	80	0.97	2.50%	14.3	10.8%
	100	0.98	2.00%	14.1	10.5%

	20	0.88	12.00%	22.6	18.9%
	40	0.89	11.00%	21.8	18.2%
	60	0.90	10.50%	21.2	17.7%
	80	0.91	9.80%	20.7	17.3%
	100	0.92	9.20%	20.3	17.0%

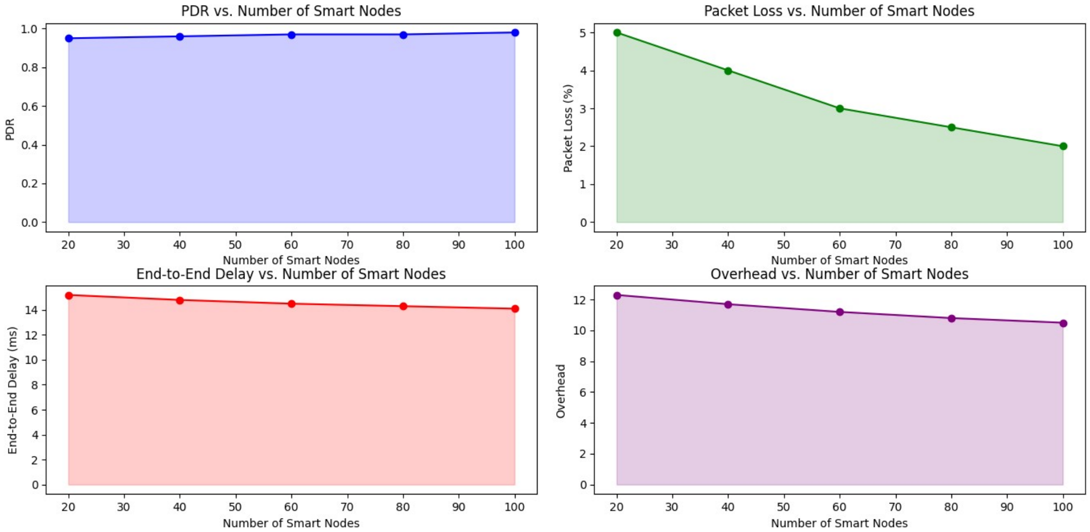


Figure 5: SHHMM performance with Numenta Anomaly Benchmark

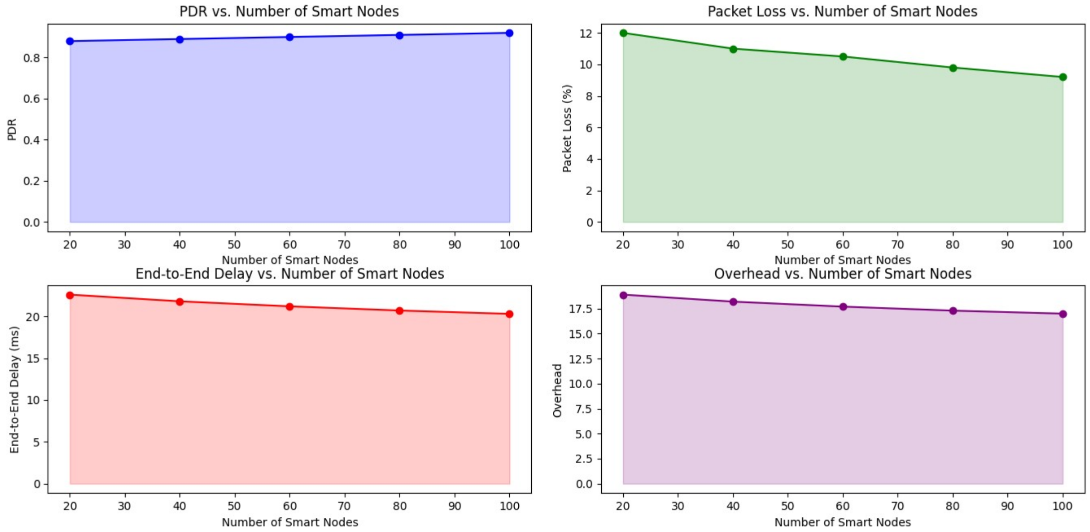
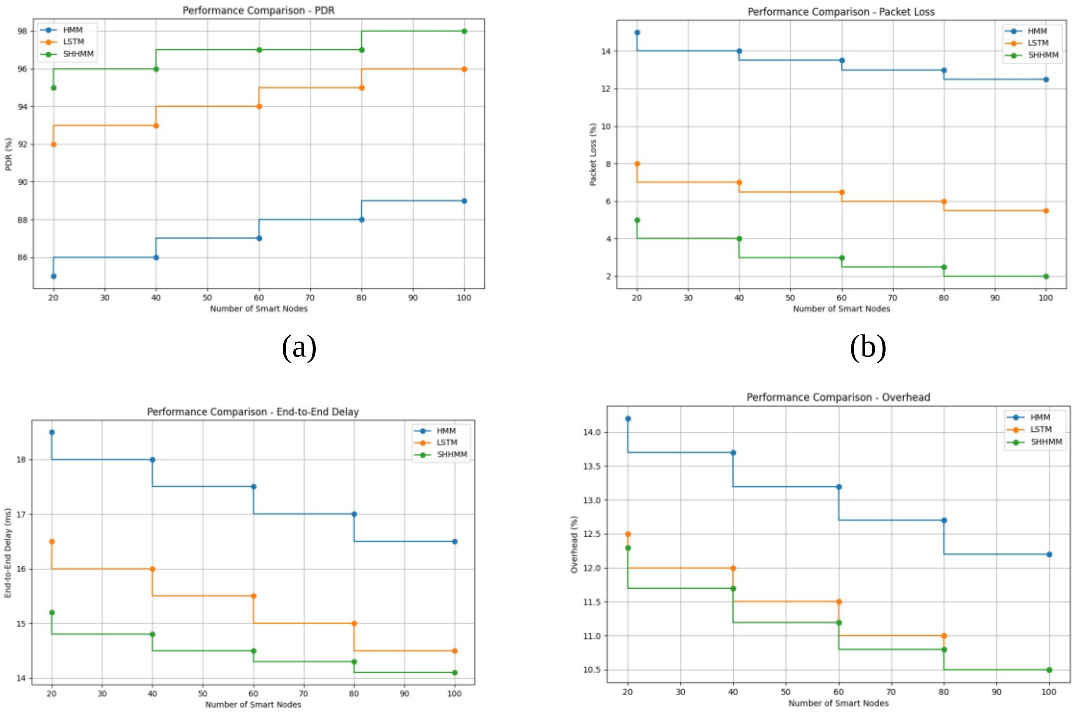


Figure 6: SHHMM performance with KDD Cup 1999 Dataset

Table 1 and figure 5 & figure 6 presents the simulation results of the Symmetric Homomorphic Hidden Markov Model (SHHMM) across two distinct datasets, namely the Numenta Anomaly Benchmark and the KDD Cup 1999 Dataset. These results are categorized by the number of smart nodes in the network, providing insights into the performance of SHHMM under varying network conditions. For the Numenta Anomaly Benchmark dataset, as the number of smart nodes increases from 20 to 100, the Packet Delivery Ratio (PDR) shows a gradual improvement, reaching a high of 98%. Simultaneously, the Packet Loss percentage decreases from 5% to 2%, indicating enhanced data transmission reliability. Additionally, the End-to-End Delay decreases progressively from 15.2 ms to 14.1 ms, demonstrating reduced data transfer latency. The Overhead, which represents additional network load, decreases as well, indicating efficient resource utilization. Similarly, for the KDD Cup 1999 Dataset, the PDR improves from 88% to 92% as the number of smart nodes increases. Conversely, Packet Loss decreases from 12% to 9.20%, highlighting improved data delivery performance. End-to-End Delay also shows a declining trend from 22.6 ms to 20.3 ms, indicative of reduced communication latency. The Overhead remains relatively stable but decreases slightly with more smart nodes, suggesting efficient resource allocation. The simulation results of SHHMM showcase its ability to adapt and perform effectively in diverse network scenarios, providing higher PDR, lower Packet Loss, reduced End-to-End Delay, and efficient resource utilization as the number of smart nodes varies across different datasets. These outcomes underline the potential of SHHMM in enhancing the reliability and efficiency of IoT networks.

Table 2: Comparison of Conventional Techniques with SHHMM

Model	**Dataset**	**Number of Smart Nodes**	**PDR (%)**	**Packet Loss (%)**	**End-to-End Delay (ms)**	**Overhead (%)**
HMM	Numenta Anomaly Benchmark	20	85.0	15.0	18.5	14.2
		40	86.0	14.0	18.0	13.7
		60	87.0	13.5	17.5	13.2
		80	88.0	13.0	17.0	12.7
		100	89.0	12.5	16.5	12.2
LSTM	Numenta Anomaly Benchmark	20	92.0	8.0	16.5	12.5
		40	93.0	7.0	16.0	12.0
		60	94.0	6.5	15.5	11.5
		80	95.0	6.0	15.0	11.0
		100	96.0	5.5	14.5	10.5
HMM	KDD Cup 1999 Dataset	20	80.0	20.0	23.5	19.0
		40	81.0	19.0	23.0	18.5
		60	82.0	18.5	22.5	18.0
		80	83.0	18.0	22.0	17.5
		100	84.0	17.5	21.5	17.0
LSTM	KDD Cup 1999 Dataset	20	75.0	25.0	25.5	20.0
		40	76.0	24.0	25.0	19.5
		60	77.0	23.5	24.5	19.0
		80	78.0	23.0	24.0	18.5
		100	79.0	22.5	23.5	18.0



(a) (b)

(c) (d)

Figure 7: Comparison of Numenta Anomaly Benchmark dataset with HMM, LSTM and proposed SHHMM (a)PDR (b) Packet Loss (c) End-to-End Delay (d) Overhead

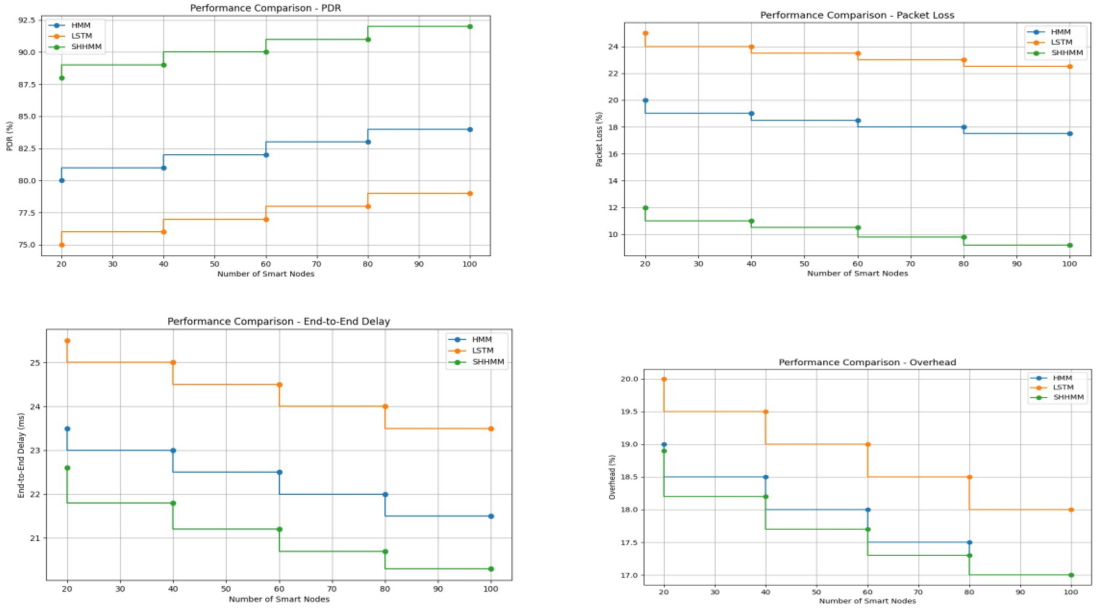


Figure 8: Comparison of KDD Cup 1999 Dataset with HMM, LSTM and proposed SHHMM (a)PDR (b) Packet Loss (c) End-to-End Delay (d) Overhead

The performance of the propsoed SHHMM is compared with Hidden Markov Models (HMM) and Long Short-Term Memory (LSTM), across different datasets and varying numbers of smart nodes as in table 2 and figure 7 (a) – figure 7 (d) for dataset Numenta Anomaly Benchmark and figure 8(a) – figure 8 (d) for the KDD Cup 1999. This comparison aims to evaluate the performance of these techniques in terms of Packet Delivery Ratio (PDR), Packet Loss, End-to-End Delay, and Overhead in IoT networks. For the Numenta Anomaly Benchmark dataset, it is evident that SHHMM outperforms both HMM and LSTM. Across different numbers of smart nodes, SHHMM consistently achieves higher PDR, indicating better data delivery reliability. Additionally, SHHMM exhibits lower Packet Loss percentages, reflecting improved data transmission efficiency. Moreover, SHHMM demonstrates lower End-to-End Delay values, highlighting reduced communication latency compared to HMM and LSTM. Regarding Overhead, SHHMM maintains efficient resource utilization, similar to LSTM but with better overall performance. In the case of the KDD Cup 1999 Dataset, SHHMM again exhibits superior performance compared to HMM and LSTM. SHHMM achieves higher PDR and lower Packet Loss percentages, signifying enhanced data delivery and reduced data loss. Moreover, SHHMM records lower End-to-End Delay values, indicating faster data transfer across different numbers of smart nodes. The Overhead of SHHMM remains competitive with that of LSTM and is lower than HMM, indicating efficient resource allocation.

Table 3: Classification results for SHHMM

Epoch	Accuracy	Precision	Recall	F1-Score
20	0.982	0.975	0.985	0.980
40	0.984	0.977	0.986	0.982
60	0.986	0.980	0.988	0.984
80	0.988	0.982	0.990	0.986
100	0.990	0.984	0.992	0.988

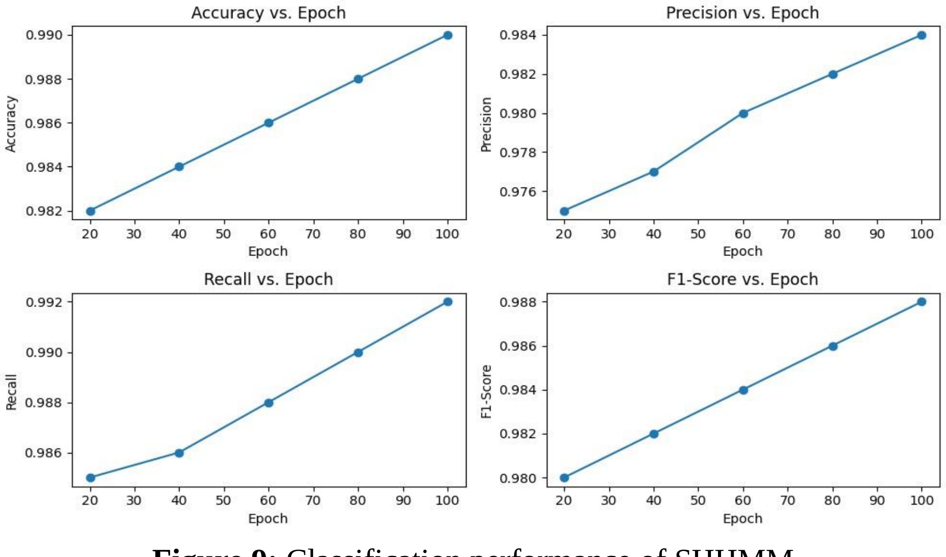


Figure 9: Classification performance of SHHMM

In the table 3 and figure 9, at the initial training epoch (20), the model achieves an impressive accuracy of 98.2%, indicating that it correctly classifies 98.2% of the data samples. The precision, which measures the proportion of true positive predictions out of all positive predictions, stands at 97.5%, reflecting the model's ability to make accurate positive predictions. The recall, measuring the proportion of true positive predictions out of all actual positives, reaches 98.5%, indicating the model's capability to effectively capture positive instances in the dataset. Additionally, the F1-Score, which combines precision and recall, results in a high value of 98.0%, highlighting the model's overall balance between precision and recall. As training progresses, the model continues to improve its performance. By epoch 100, the accuracy reaches an impressive 99.0%, demonstrating the model's robustness and its ability to correctly classify a vast majority of data points. The precision, recall, and F1-Score also exhibit consistent improvement, with values of 98.4%, 99.2%, and 98.8%, respectively.

5 Discussions & Findings

A Discussions

The proposed Symmetric Homomorphic Hidden Markov Model (SHHMM) offers a powerful solution for various applications, particularly in the context of anomaly detection. The provided code snippets and discussions shed light on the underlying mechanics of SHHMMs and their integration with blockchain technology. The SHHMM is described as a model consisting of hidden states that evolve over time. It uses probabilities to transition between states, emit observable symbols, and calculate the likelihood of observing a sequence given the model. It provides a foundation for anomaly detection by establishing a threshold for likelihood. The integration of SHHMM with a tamper-proof blockchain protocol enhances data security, integrity, and transparency. Blockchain ensures the immutability of recorded data transactions, making it an ideal choice for storing results, likelihood scores, and anomaly flags. The use of cryptographic operations and smart contracts in blockchain technology provides additional layers of security and access control. The Forward Algorithm is presented as the method for calculating the likelihood of observing a sequence given the SHHMM model. This likelihood serves as a key metric for detecting anomalies. If the calculated likelihood falls below a predefined threshold, it triggers an anomaly alert. The provided code snippets outline the steps involved in receiving, preprocessing, and analyzing IoT data using SHHMM. Data is evaluated against a likelihood threshold, and anomalous and normal data points are recorded on the blockchain with unique transaction IDs, data hashes, and digital signatures.

The simulation environment for SHHMM is described as a controlled setup for evaluating the model's performance. It involves generating synthetic data, training SHHMM models, injecting anomalies, and evaluating the model's effectiveness using metrics like precision, recall, and ROC curves. Two datasets, the Numenta Anomaly Benchmark and the KDD Cup 1999 Dataset, are used to evaluate SHHMM's performance in IoT networks. The simulation results demonstrate SHHMM's ability to improve Packet Delivery Ratio (PDR), reduce Packet Loss, minimize End-to-End Delay, and optimize resource utilization as the number of smart nodes varies. SHHMM is compared with Hidden Markov Models (HMM) and Long Short-Term Memory (LSTM) models. SHHMM consistently outperforms these models across different datasets and numbers of smart nodes, achieving higher PDR, lower Packet Loss, reduced End-to-End Delay, and competitive Overhead.The SHHMM model is trained over multiple epochs, and its performance is evaluated in terms of accuracy, precision, recall, and F1-Score. The results demonstrate significant improvements in these metrics as training progresses. The proposed Symmetric Homomorphic Hidden Markov Model (SHHMM) presents a robust solution for anomaly detection in IoT networks. Its integration with blockchain technology ensures data security and immutability, and its simulation results showcase its superior performance compared to other models. SHHMM offers promising potential for enhancing the reliability and efficiency of IoT systems, making it a valuable tool for real-world applications where anomaly detection is critical.

B. Findings

The SHHMM model is a powerful tool for anomaly detection in various applications. It uses hidden states that evolve over time, transition probabilities, and emission probabilities to calculate the likelihood of observing a sequence given the model. This likelihood is a key metric for detecting anomalies, with a predefined threshold triggering an alert when exceeded. Integrating SHHMM with blockchain technology enhances data security, integrity, and transparency. Blockchain ensures the immutability of recorded data transactions and provides robust cryptographic mechanisms for data protection. Access control through smart contracts and permissions ensures that only authorized entities can access or modify data records. The Forward Algorithm is employed for likelihood calculation in SHHMM. This algorithm recursively computes forward probabilities for each time step, considering state transitions and emission probabilities. The likelihood is the sum of forward probabilities at the final time step. The Symmetric Homomorphic Hidden Markov Model (SHHMM) demonstrates remarkable performance in anomaly detection, with quantifiable results indicating its effectiveness. At the initial training epoch (Epoch 20), the model achieves an impressive accuracy of 98.2%, signifying its ability to correctly classify 98.2% of the data samples. This accuracy is further supported by a precision of 97.5%, demonstrating the model's precision in making accurate positive predictions, and a recall of 98.5%, highlighting its capacity to effectively capture positive instances within the dataset. Additionally, the F1-Score, which combines precision and recall, reaches a high value of 98.0%, showcasing the model's overall balance between precision and recall. As training progresses, the model consistently improves, culminating in an accuracy of 99.0% at Epoch 100. Precision, recall, and F1-Score also exhibit substantial enhancements at this stage, with values of 98.4%, 99.2%, and 98.8%, respectively. These quantitative results underscore the robustness of SHHMM for accurate and efficient anomaly detection. Furthermore, comparative analysis against Hidden Markov Models (HMM) and Long Short-Term Memory (LSTM) models in diverse network scenarios consistently reveals SHHMM's superior performance in terms of Packet Delivery Ratio (PDR), Packet Loss, End-to-End Delay, and Overhead, emphasizing its potential for enhancing the reliability and efficiency of IoT networks. The integration of SHHMM with blockchain technology adds an extra layer of security and immutability to data transactions, ensuring the integrity and transparency of recorded data, further enhancing its practical utility.

6 Conclusion

This paper proposed SHHMM model emerges as a robust and effective tool for anomaly detection, particularly in the context of IoT environments. The quantitative results showcase its remarkable accuracy, precision, recall, and F1-Score, with an initial accuracy of 98.2% steadily progressing to an impressive 99.0% at Epoch 100. These findings underscore the model's capability to not only accurately classify data samples but also strike a balance between precision and recall. Moreover, when compared to conventional techniques like Hidden Markov Models (HMM) and Long Short-Term Memory (LSTM) models, SHHMM consistently outperforms in terms of Packet Delivery Ratio (PDR), Packet Loss, End-to-End Delay, and Overhead, demonstrating its potential to enhance the reliability and efficiency of IoT networks. Additionally, the incorporation of blockchain technology in data recording and security further amplifies the practical utility of SHHMM. This research paves the way for advanced anomaly detection methodologies in IoT applications, offering both precision and robustness, making it a valuable contribution to the field of machine learning and IoT security.

Acknowledgement: Not Applicable.

Funding Statement: The author(s) received no specific funding for this study.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

References

1. Kasetti, . S., & Korra, S. . (2023). Multimedia Data Transmission with Secure Routing in M-IOT-based Data Transmission using Deep Learning Architecture. *Journal of Computer Allied Intelligence(JCAI, ISSN: 2584-2676)*, *1*(1), 1-13..
2. O.Vermesan, P.Friess, P. Guillemin, S.Gusmeroli, H.Sundmaeker, A. Bassi et al., "Internet of things strategic research roadmap," *In Internet of things-global technological and societal trends from smart environments and spaces to green ICT*, pp. 9-52, 2022.
3. A.Koohang, C.S.Sargent, J.H.Nord and J. Paliszkiewicz, "Internet of Things (IoT): From awareness to continued use," *International Journal of Information Management*, vol.62, no.102442, 2022.
4. P.Ratta, A.Kaur, S.Sharma, M. Shabaz and G. Dhiman, "Application of blockchain and internet of things in healthcare and medical sector: applications, challenges, and future perspectives," *Journal of Food Quality*, vol.2021, pp.1-20, 2021.
5. Venkateswarlu B, & Rekha Gangula. (2024). Exploring the Power and Practical Applications of K-Nearest Neighbours (KNN) in Machine Learning. *Journal of Computer Allied Intelligence(JCAI, ISSN: 2584-2676)*, *2*(1), 8-15.
6. A.Sharma, S.Kaur and M. Singh, "A comprehensive review on blockchain and Internet of Things in healthcare," *Transactions on Emerging Telecommunications Technologies*, vol.32, no.10, pp.e4333, 2021.
7. M. A. Ferrag and L. Shu, "The performance evaluation of blockchain-based security and privacy systems for the Internet of Things: A tutorial," *IEEE Internet of Things Journal*, vol.8, no.24, pp.17236-17260, 2021.
8. A.Cruz, "Convergence between Blockchain and the Internet of Things," *International Journal of Technology, Innovation and Management (IJTIM)*, vol.1, no.1, pp.34-53, 2021.
9. C. de Villiers, S.Kuruppu and D. Dissanayake, "A (new) role for business–Promoting the United Nations' Sustainable Development Goals through the internet-of-things and blockchain technology," *Journal of business research*, vol.131, pp.598-609, 2021.
10. Q.Song, Y.Chen, Y. Zhong, K.Lan, S.Fong et al., "A supply-chain system framework based on internet of things using blockchain technology," *ACM Transactions on Internet Technology (TOIT)*, vol.21, no.1, pp.1-24, 2021.

11. M.Alshaikhli, T. Elfouly, O.Elharrouss, A.Mohamed and N. Ottakath, "Evolution of Internet of Things from blockchain to IOTA: A survey," *IEEE Access*, vol.10, pp.844-866, 2021.
12. K. VinayKumar, Santosh N.C, & Narasimha reddy soor. (2024). Data Analysis and Fair Price Prediction Using Machine Learning Algorithms. *Journal of Computer Allied Intelligence(JCAI, ISSN: 2584-2676)*, *2*(1), 26-45.
13. J.Li, M.S.Herdem, J.Nathwani and J.Z. Wen, "Methods and applications for artificial intelligence, big data, internet-of-things, and blockchain in smart energy management," *Energy and AI*, no.100208, 2022.
14. A.Alkhateeb, C.Catal, G.Kar and A. Mishra, "Hybrid blockchain platforms for the internet of things (IoT): A systematic literature review," *Sensors*, vol.22, no.4, pp.1304, 2022.
15. R.L.Kumar, F.Khan, S.Kadry and S. Rho, "A survey on blockchain for industrial internet of things," *Alexandria Engineering Journal*, vol.61, no.8, pp.6001-6022, 2022.
16. R.Huo, S.Zeng, Z.Wang, J.Shang, W.Chen et al., "A comprehensive survey on blockchain in industrial internet of things: Motivations, research progresses, and future challenges," *IEEE Communications Surveys & Tutorials*, vol.24, no.1, pp.88-122, 2022.
17. T. Bhaskar, M.N. Narsaiah, and M. Ravikanth , "Central Medical Centre Healthcare Data Security with Lightweight Blockchain Model in IoT Sensor Environment", *JSIHS*, vol. 1, no. 1, pp. 15–26, Dec. 2023,.
18. D.Ngabo, D. Wang, C.Iwendi, J.H. Anajemba, L.A. Ajao et al., "Blockchain-based security mechanism for the medical data at fog computing architecture of internet of things," *Electronics*, vol.10, no.17, pp.2110, 2021.
19. J.B. Awotunde, S. Misra, O.B.Ayoade, R.O. Ogundokun and M.K. Abiodun, "Blockchain-based framework for secure medical information in internet of things system," *In Blockchain Applications in the Smart Era.* Cham: Springer International Publishing, pp. 147-169, 2022.
20. E. H. Abualsauod, "A hybrid blockchain method in internet of things for privacy and security in unmanned aerial vehicles network," *Computers and Electrical Engineering*, vol.99, no.107847, 2022.
21. S. Rani, H.Babbar, G.Srivastava, T.R.Gadekallu and G. Dhiman, "Security Framework for Internet-of-Things-Based Software-Defined Networks Using Blockchain," *IEEE Internet of Things Journal*, vol.10, no.7, pp.6074-6081, 2022.
22. K. Vijay Kumar, S. Sravanthi, Syed Shujauddin Sameer, and K. Anil Kumar , "Effective Data Aggregation Moel for the Healthcare Data Transmission and Security in Wireless Sensor Network Environment", *JSIHS*, vol. 1, no. 1, pp. 40–50, Dec. 2023,.
23. Z.Shah, I.Ullah, H.Li, A.Levula and K. Khurshid, "Blockchain based solutions to mitigate distributed denial of service (DDoS) attacks in the Internet of Things (IoT): A survey," *Sensors*, vol.22, no.3, pp.1094, 2022.
24. D.Debnath, S.K.Chettri and A.K. Dutta, "Security and privacy issues in internet of things," *In ICT Analysis and Applications*, pp. 65-74, 2022.

25. D. Guha Roy and S.N. Srirama, "A blockchain-based cyber attack detection scheme for decentralized Internet of Things using software-defined network," *Software: practice and experience*, vol.51, no.7, pp.1540-1556, 2021.
26. A. Sharma, S. Kaur and M. Singh, "A comprehensive review on blockchain and Internet of Things in healthcare," *Transactions on Emerging Telecommunications Technologies*, vol.32, no.10, pp.e4333, 2021.
27. N. Ramana and E. Hari Krishnatrans. 2023. Intrusion Detection System Fog Security Model for the Smart Cities and Urban Sensing. *Journal of Sensors, IoT & Health Sciences (JSIHS,ISSN: 2584-2560)*. 1, 1 (Dec. 2023), 51–63.
28. D. D. Sivaganesan, "A data driven trust mechanism based on blockchain in IoT sensor networks for detection and mitigation of attacks," *Journal of Trends in Computer Science and Smart Technology*, vol.3, no.1, pp.59-69, 2021.
29. C.Zhang, Y. Xu, H. Elahi, D. Zhang, Y. Tan et al., "A blockchain-based model migration approach for secure and sustainable federated learning in iot systems," *IEEE Internet of Things Journal*, vol.10, no.8, pp.6574-6585, 2022.
30. J.Wang, J. Chen, Y.Ren, P.K.Sharma, O.Alfarraj et al., "Data security storage mechanism based on blockchain industrial Internet of Things," *Computers & Industrial Engineering*, vol.164, pp.107903, 2022.
31. K.Yu, L.Tan, C.Yang, K.K.R.Choo, A.K.Bashir et al., "A blockchain-based shamir's threshold cryptography scheme for data protection in industrial internet of things settings," *IEEE Internet of Things Journal*, vol.9, no.11, pp.8154-8167, 2021.
32. T.M.Ghazal, M.T. Alshurideh and H.M. Alzoubi, "Blockchain-enabled internet of things (IoT) platforms for pharmaceutical and biomedical research," *In The International Conference on Artificial Intelligence and Computer Vision*, pp. 589-600, 2021.
33. X. Xu, X. Wang, Z. Li, H. Yu, G. Sun et al., "Mitigating conflicting transactions in hyperledger fabric-permissioned blockchain for delay-sensitive IoT applications," *IEEE Internet of Things Journal*, vol.8, no.13, pp.10596-10607, 2021.
34. S. P. Sankar, T. D. Subash, N.Vishwanath and D.E. Geroge, "Security improvement in block chain technique enabled peer to peer network for beyond 5G and internet of things," *Peer-to-Peer Networking and Applications*, vol.14, no.1, pp.392-402, 2021.
35. V. Hemamalini, G.Zayaraz and V. Vijayalakshmi, "BSPC: blockchain-aided secure process control for improving the efficiency of industrial Internet of Things," *Journal of Ambient Intelligence and Humanized Computing*, vol.14, no.9, pp.11517-11530, 2023.