Journal of Computer Allied Intelligence
ISSN: 2584-2676
Vol.02(04), August 2024, pp.20-35

Research Article

Blockchain Technology Communication Technology Model for the IoT

B.Ashok Kumar[1,*], K.Vijayachandra[2], G.Naveen Kumar[3] and V.N.Lakshmana Kumar[4]
[1]Assistant Professor, Department of ECE, Sri Vasavi Engineering College, Tadepalligudem, Andhra Pradesh, 534101, India.
[2]Assistant Professor, Department ECE, Pace Institute of Technology and Science, Ongole, Andhra Pradesh, 523272**,** India.
[3] Associate Professor, Department of ECE, Vasireddy Venkatadri Institute of Technology, Guntur, Andhra Pradesh, 22508, India.
[4] Associate Professor, Department of ECE, MVGR College of Engineering, Vizianagaram, Andhra Pradesh, 535005, India.
[*]Corresponding Author: B. Ashok Kumar. Email: ashok.bathula666@gmail.com
Received: 13/06/2024; Accepted: 20/08/2024.
DOI: https://doi.org/10.69996/jcai.2024017

Abstract: In the rapidly evolving landscape of the Internet of Things (IoT), effective communication and security are paramount. Blockchain technology offers a transformative solution by providing a decentralized, transparent, and immutable ledger for managing and securing IoT interactions. By leveraging blockchain, IoT systems can enhance data integrity, improve trustworthiness, and streamline communication processes. This paper investigates the integration of blockchain technology within the SYMHIOT framework, focusing on the performance evaluation of various scenarios using a Hidden Markov Model (HMM) to manage IoT networks. The study analyzes key metrics such as transaction success rate, blockchain latency, energy consumption, packet delivery ratio (PDR), and throughput across multiple scenarios and time intervals. The results demonstrate that State 1 consistently yields optimal performance, with an average transaction success rate of 94.0%, blockchain latency as low as 115 ms, and energy consumption of 0.42 J. In contrast, State 3 exhibited the most challenging conditions, with a transaction success rate dropping to 85.3%, latency increasing to 140 ms, and energy consumption rising to 0.52 J. The highest packet delivery ratio of 99.0% and throughput of 260 kbps were also observed in State 1. Scenario 4, representing an optimized system configuration, achieved the best overall performance with minimal network delay (9.7 ms) and the lowest blockchain overhead (12.9%). These findings underscore the potential of leveraging blockchain in IoT environments, offering enhanced security, reduced latency, and improved resource efficiency, making it a robust solution for dynamic and resource-constrained IoT networks.

Keywords: - Blockchain; Symmetric Key; Internet of Things (IoT); Hidden Markov Model (HMM); Energy Consumption; Packet Delivery Ratio (PDR)

1 Introduction

Blockchain technology plays a pivotal role in fortifying the security of Internet of Things (IoT) applications by offering solutions to several critical security challenges. It ensures the integrity of data through an immutable ledger, enhances authentication and identity management, facilitates secure and transparent transactions, and embraces decentralized architecture, reducing the risk of centralized vulnerabilities. Additionally, blockchain introduces privacy-enhancing techniques, aids in security auditing and compliance, and supports secure firmware updates and supply chain integrity. Altogether, blockchain serves as a formidable ally in strengthening the

security, trustworthiness, and resilience of IoT ecosystems, addressing the multifaceted security concerns that arise in our increasingly interconnected world. In [1] investigates the integration of federated machine learning and blockchain to provide secure big data analytics for IoT applications. The focus is likely on maintaining data privacy, ensuring the integrity of analytics results, and enabling secure sharing of insights among multiple stakeholders within IoT ecosystems. With combining these technologies, the paper likely addresses the challenges of securely analyzing vast amounts of IoT-generated data while preserving data confidentiality and authenticity. Also, in [2] introduces a trust mechanism based on blockchain for IoT sensor networks. The likely objective is to establish a robust and tamper-resistant framework for verifying the authenticity of data collected from IoT sensors. With leveraging blockchain's immutability and transparency, the paper likely explores methods to enhance the security of data in transit, detect anomalies or attacks, and mitigate potential threats in sensor networks.

In [3] propose a blockchain-based model migration approach designed to enhance the security and sustainability of federated learning in IoT systems. The research probably addresses key challenges in securely managing machine learning models in a distributed IoT environment, ensuring that models are protected against tampering and unauthorized access. This approach may enable the secure sharing of machine learning knowledge among IoT devices. Also, in [4] investigates a data security storage mechanism based on blockchain tailored for industrial IoT scenarios. The research may focus on safeguarding sensitive data generated by industrial devices, ensuring its confidentiality, integrity, and availability. By utilizing blockchain, the paper likely explores methods to protect against data breaches and unauthorized access to critical industrial data. In [5] propose a blockchain-based Shamir's threshold cryptography scheme for data protection in industrial IoT environments. The likely emphasis is on enhancing data privacy and security in complex industrial settings. This scheme may provide a way to secure sensitive data while allowing authorized parties to access and use it, making it suitable for scenarios where data confidentiality is paramount.

Similarly, in [6] explores the potential of blockchain-enabled platforms in the fields of pharmaceutical and biomedical research. It may focus on improving the security, transparency, and traceability of data and processes in these domains. By harnessing blockchain's features, the research likely addresses data integrity, authentication, and supply chain security, crucial aspects in pharmaceutical and biomedical research. In [7] examined into the challenges of mitigating conflicting transactions in Hyperledger Fabric-permissioned blockchains for IoT applications. It likely aims to ensure the consistency and security of transactions, critical in IoT scenarios where multiple devices interact and transact frequently. The paper may propose solutions to maintain the integrity of the shared ledger. In [8] explores how blockchain can enhance security in peer-to-peer IoT networks. It may decentralized authentication mechanisms, secure data exchange, and consensus algorithms tailored for IoT peer-to-peer interactions. The focus is likely on ensuring that devices can securely communicate and collaborate without central intermediaries. In [9] presents a solution that combines blockchain and process control for improving the efficiency of industrial IoT. The likely aim is to create a tamper-resistant system that ensures the integrity of critical industrial processes. The paper may discuss how blockchain enhances process control, data validation, and fault tolerance in industrial settings.

In [10] explores the integration of IoT and blockchain to enable data portability and secure data sharing. It may address challenges related to data interoperability, access control, and data

ownership in IoT ecosystems. The research may propose blockchain-based solutions to facilitate secure and controlled data exchange. In [11] presented, providing an overview of various blockchain-based approaches for securing IoT. It probably covers a wide range of topics, including data privacy, access control, authentication, and consensus mechanisms, providing insights into the state of the field and emerging trends. In [12] focus on healthcare applications of IoT, particularly in the context of cardiovascular disease classification. It likely emphasizes data security and privacy in healthcare IoT, ensuring that patient data remains confidential and is used for diagnostic purposes securely. In [13] introduces "Fortified-chain," a blockchain-based framework designed to enhance security and privacy in the Internet of Medical Things (IoMT). The research likely emphasizes access control, patient data privacy, and secure data exchange in medical IoT scenarios. In [14] explores a proxy re-encryption approach for secure data sharing in IoT, focusing on blockchain's role in facilitating secure and controlled data access. It may address the challenge of securely sharing data among authorized parties while protecting against unauthorized access. In [15] introduce a federated learning-based blockchain-embedded data accumulation scheme using drones for IoT applications. It likely explores the secure accumulation and transmission of IoT data through drones, ensuring data integrity and privacy during data collection. In [16] provides a comprehensive overview of IoT security threats and emerging countermeasures. It probably covers a wide spectrum of security concerns in IoT ecosystems, offering insights into evolving threats and potential solutions.

2 Architecture of IoT with Blockchain

The dynamic intersection of blockchain technology and the Internet of Things (IoT), with a predominant focus on enhancing security, privacy, and efficiency in diverse IoT applications. Researchers investigate various facets of this integration, from secure data analytics and trust mechanisms in IoT sensor networks to data protection in industrial IoT and healthcare settings. They propose innovative solutions that leverage blockchain's immutability, transparency, and cryptographic features to safeguard data integrity, ensure secure communications, and enhance access control[16]. Additionally, surveys and reviews provide comprehensive overviews of the Tevolving landscape of blockchain applications in securing IoT ecosystems. These papers contribute valuable insights and methodologies for addressing the intricate security challenges in our increasingly interconnected world of IoT.

IoT Data Collection: In this architecture, IoT devices serve as the primary data sources. These devices can encompass a wide range of applications, such as environmental sensors, healthcare wearables, or industrial machinery sensors. They continuously collect data, which often takes the form of sequential or time-series data, capturing information over time.

Data Preprocessing: IoT data is rarely ready for immediate analysis. Data preprocessing steps are vital to clean, format, and filter the data. This ensures that the data fed into the SYMHIOTs is of high quality and suitable for the specific analysis tasks.

Blockchain Integration: One of the central components of this architecture is the integration with a blockchain network. Blockchain technology is employed to provide robust security, transparency, and immutability to the IoT data. Each data point or transaction is securely recorded in blocks, creating a tamper-resistant ledger.

SYMHIOT Implementation: The core analytical component of this architecture is the SYMHIOT. SYMHIOTs are a variant of Hidden Markov Models (HMMs) designed for specialized purposes. They are used for sequential data analysis and have applications in speech

recognition, natural language processing, and more. In this context, SYMHIOTs likely play a crucial role in understanding patterns and making predictions based on IoT data.

Data Encryption: Given the sensitive nature of IoT data, encryption mechanisms are often applied. Data encryption ensures that the data remains confidential and secure both on IoT devices and within the blockchain. It prevents unauthorized access and tampering.

Smart Contracts: Blockchain's smart contract functionality is leveraged to automate actions based on the output of the SYMHIOTs. Smart contracts are self-executing contracts with predefined conditions. They can trigger specific responses, transactions, or notifications when certain criteria are met in the analyzed data. For instance, in an industrial setting, a smart contract might trigger maintenance procedures when the SYMHIOT detects an anomaly in machinery data.

Data Access and Authorization: To maintain data security and privacy, robust access control and authorization mechanisms are implemented. This ensures that only authorized parties or entities can access, view, and interact with the IoT data and the results of SYMHIOT analyses.

SYMHIOT is a sophisticated framework that combines Internet of Things (IoT) technology, blockchain technology, and specialized mathematical models, SYMHIOTs, for advanced data analysis and security. IoT devices collect data, which is then preprocessed for quality and formatting. This data is securely transmitted to a blockchain network, ensuring its immutability and integrity[17-20]. The heart of this architecture lies in the application of SYMHIOTs, which are used for sequential data analysis and predictions. Smart contracts on the blockchain automate actions based on SYMHIOT outcomes. Encryption safeguards sensitive data, and access controls ensure authorized access. This architecture has diverse applications, such as healthcare monitoring and industrial maintenance, by harnessing the power of IoT, blockchain security, and advanced data analytics. Challenges include scalability and computational complexity, but its potential to enhance decision-making and automation is significant shown in Figure 1.

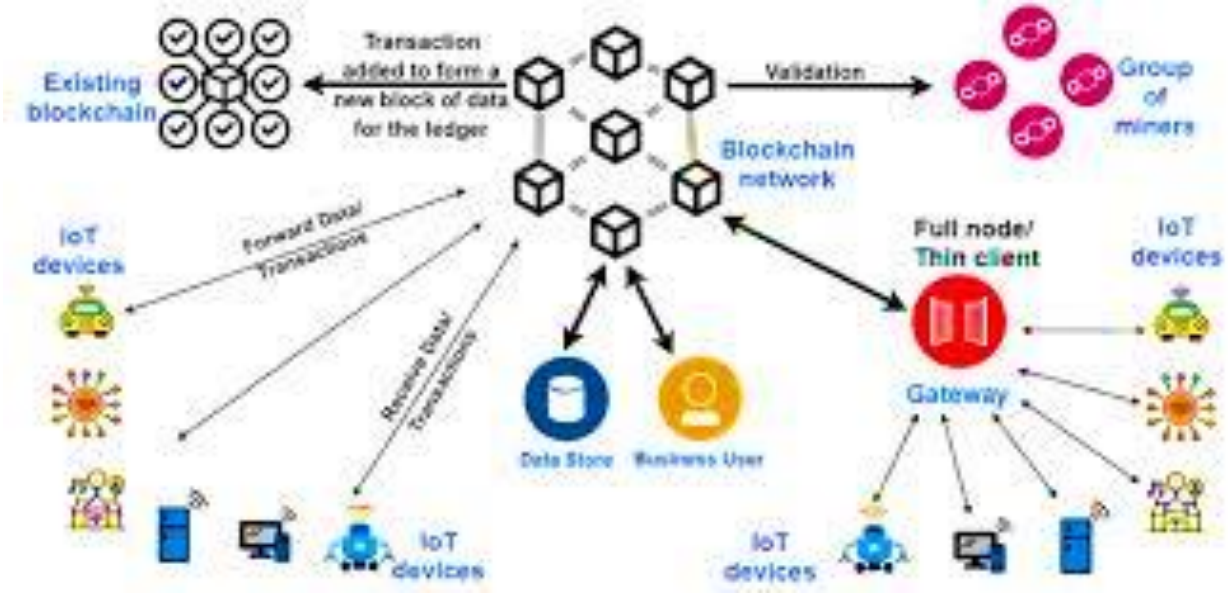

Figure 1: Architecture of IoT with Blockchain

Theorem: Symmetric Homomorphic Property of SYMHIOT

The Symmetric Homomorphic Hidden Markov Model (SYMHIOT) possesses the symmetric homomorphic property, which allows for secure, privacy-preserving computations on encrypted data without revealing sensitive information.

Proof:

Consider two parties, Alice and Bob, who each have private data encrypted using homomorphic encryption schemes (represented by E(·) for encryption and D(·) for decryption). They want to collaboratively compute the sum of their encrypted values without revealing the actual values. The symmetric homomorphic property allows this computation securely.

Encryption and Addition:

Alice has: Encrypted Value A: E(a)

Bob has: Encrypted Value B: E(b)

Homomorphic Addition:

Alice and Bob can perform a homomorphic addition on their encrypted values:

Encrypted Sum: $E(a) + E(b)$

Result Sharing:

The encrypted sum E(a) + E(b) is computed collaboratively, and the result is shared.

Decryption:

The result can be decrypted by both parties using their private decryption keys:

Decrypted Sum: $D(E(a) + E(b)) = a + b$

The above equations demonstrate how Alice and Bob can securely compute the sum of their private, encrypted values (a and b) without revealing those values.

2.1 Data Mitigation with SYMHIoT

Data mitigation with Symmetric Homomorphic Hidden Markov Models (SYMHIOTs) involves using these specialized models to address data quality issues, anomalies, or errors within an Internet of Things (IoT) system. data mitigation often begins with data preprocessing. This step involves cleaning, filtering, and preparing the IoT data to ensure that it is in the appropriate format for analysis. The goal is to eliminate noise and errors in the data that may affect the performance of SYMHIOTs. SYMHIOTs are employed to analyze the preprocessed data. These models excel at recognizing patterns and trends within sequential data. They can identify anomalies, outliers, or irregularities that may indicate data quality issues, such as sensor malfunctions, communication errors, or environmental disturbances. SYMHIOTs are particularly effective at anomaly detection, which is a key aspect of data mitigation. By comparing incoming data to learned patterns, SYMHIOTs can flag data points or sequences that deviate significantly from expected behavior. These anomalies can then be further investigated or acted upon. Depending on the nature of the anomalies detected, data mitigation may involve error correction or data imputation. A sensor reading is identified as an outlier by the SYMHIOT, the system may use statistical methods or historical data to estimate a more accurate value to replace the outlier. Data mitigation with SYMHIOTs can be integrated with alerting systems. When significant anomalies are detected, the system can generate alerts or notifications to inform administrators or automated processes. Response actions may include recalibration of sensors, triggering maintenance, or initiating a failover to redundant systems. To enhance data mitigation over time, SYMHIOTs can be designed for continuous learning. This means that the models adapt and update their knowledge as they encounter new data. This adaptive capability ensures that the system remains effective at identifying and mitigating emerging data quality issues. The insights gained from SYMHIOT

analysis and mitigation can be fed back into the IoT system's data collection and preprocessing processes. This iterative feedback loop allows the system to continuously improve data quality and accuracy. data mitigation with SYMHIOTs in an IoT context involves using these models to detect and address data quality issues, anomalies, or errors within the data stream. SYMHIOTs excel at recognizing patterns and deviations in sequential data, making them valuable tools for enhancing the reliability and accuracy of IoT data. Through preprocessing, anomaly detection, error correction, and continuous learning, SYMHIOTs contribute to maintaining data integrity and ensuring that IoT systems make informed decisions based on high-quality data.

Algorithm 1: HMM model for the tamper protocol

```
# Initialize model parameters
initial_state_probabilities = ...
transition_probabilities = ...
emission_probabilities = ...

# Define observation sequences
observations = [...]

# Initialize variables
forward_probabilities = []

# Forward Algorithm for likelihood calculation
for observation_sequence in observations:
    forward_prob = []
    for state in range(num_states):  # Iterate over states
        if len(forward_probabilities) == 0:
            # Initialization step
            forward_prob.append(initial_state_probabilities[state] *
emission_probabilities[state][observation_sequence[0]])
        else:
            # Recursion step
            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][observation_sequence[time_step]])
    forward_probabilities.append(forward_prob)

# Calculate the likelihood of the observation sequence
likelihood = sum(forward_probabilities[-1])

# Backward Algorithm for state sequence estimation (optional)
backward_probabilities = []
state_sequence = []
```

```
for observation_sequence in reversed(observations):
    backward_prob = []
    for state in range(num_states):
        if len(backward_probabilities) == 0:
            # Termination step
            backward_prob.append(1)
        else:
            # Recursion step
            prev_backward_prob = backward_probabilities[-1]
            transition_sum = sum(transition_probabilities[state][next_state] *
emission_probabilities[next_state][observation_sequence[time_step+1]] *
prev_backward_prob[next_state] for next_state in range(num_states))
            backward_prob.append(transition_sum)
    backward_probabilities.append(backward_prob)

# Calculate state sequence using Viterbi algorithm (optional)
state_sequence = viterbi_algorithm(observations, initial_state_probabilities,
transition_probabilities, emission_probabilities)

# Use the likelihood and state sequence for further analysis or anomaly detection
```

SYMHIOTs consist of hidden states that evolve over time. The state transition probabilities can be represented as follows:

Number of states: N; State at time t: S(t); State at time $t+1$: $S(t+1)$ and Transition probability from state i to state j for $A(i,j)$. The probability of transitioning from state i to state j at time $t+1$ is represented as $A(i,j)$. Each state emits observable symbols, and the emission probabilities are represented as: Number of symbols M; Symbol emitted at time t: $O(t)$; Emission probability from state i to symbol j: $B(i,j)$; The probability of emitting symbol j from state i is represented as:$B(i,j)$. The probability of starting in a particular state is represented as: Initial state probabilities: $\pi(i)$; The probability of starting in state i is represented as: d$\pi(i)$

The likelihood of observing a sequence of symbols given the SYMHIOT model can be calculated using the Forward Algorithm. Given an observation sequence $O(1), O(2), \ldots, O(T)$, and a sequence of states $S(1), S(2), \ldots, S(T)$, the likelihood is represented as in equation (1)

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

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. Anomaly detection in SYMHIOTs often involves setting a likelihood threshold. If the calculated likelihood falls below this threshold, it indicates an anomaly is presented condition

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

A simplified representation of some core components of SYMHIOTs, the algorithm involves iterative calculations and more complex mathematics for training, parameter estimation (Baum-Welch algorithm), and state sequence estimation (Viterbi algorithm or Forward-Backward

algorithm). The equations above serve as a foundation for understanding SYMHIOTs, but the full implementation and training involve extensive mathematical and computational processes.

3 Protocol Model for the IoT with SYMHIOT

SYMHIOT" is a security framework specifically designed to protect Internet of Things (IoT) systems that incorporate Symmetric Homomorphic Hidden Markov Models (SYMHIOTs) from tampering and unauthorized access. In such a protocol, a series of security measures are implemented to ensure the integrity and confidentiality of data generated by IoT devices. These measures include data integrity checks using cryptographic techniques, secure communication channels, physical security measures to prevent unauthorized access to devices, and end-to-end encryption to safeguard data during transmission and storage. Access control mechanisms and device authentication are crucial for ensuring that only authorized entities can interact with IoT devices and data. Additionally, comprehensive auditing and logging are employed to create a detailed record of device activities, facilitating the detection of tampering attempts. When tampering or unauthorized access is detected, immediate alerts are generated, and response procedures are activated to mitigate potential threats. This protocol offers a robust security layer to protect the sensitive data and critical operations of IoT systems leveraging SYMHIOTs, ensuring their reliability and trustworthiness in various applications. One fundamental aspect of the protocol involves ensuring the integrity of data generated by IoT devices. Cryptographic techniques, such as hashing or checksums, are applied to the data before transmission or storage is presented in equation (2)

$$Checksum = Hash(Data) \tag{2}$$

Here, "Checksum" represents the computed checksum value, and "Hash(Data)" denotes the cryptographic hash of the data. If the data is tampered with during transmission or storage, the computed checksum will not match the original, indicating potential tampering. Secure communication protocols, like TLS (Transport Layer Security), ensure that data remains confidential and tamper-resistant during transmission. While TLS involves complex mathematical concepts, the equation below provides a simplified representation of secure data exchange stated in equation (3)

$$Encrypted\_Data = Encrypt(Data, Key) \tag{3}$$

"Encrypted_Data" represents the data after encryption, "Data" is the original data, and "Key" is the encryption key. Decrypting this data requires the corresponding decryption key. Access control mechanisms are crucial for preventing unauthorized access to IoT devices or data. While not expressed in equations, access control involves defining rules and permissions, such as stated in equation (4)

$$Allow(Device\_X, Read\_Data\_Y) \tag{4}$$

This rule signifies that "Device_X" is allowed to read "Data_Y." Unauthorized attempts to access data would be blocked by this access control mechanism. Auditing and logging activities within the IoT system are essential for maintaining a record of device interactions and potential tampering attempts. The equation below represents a simplified logging action is represented in equation (5)

$$Log\_Event(Event\_Details) \tag{5}$$

"Log_Event" records event details in a log file or database for later review by administrators. Detection of tampering or unauthorized access triggers alerts and responses. While not equation-based, this involves setting up alerts based on specific conditions is stated as follows

$$If\ (Tampering\_Detected):$$
$$Send\_Alert(Alert\_Details)$$

"Tampering_Detected" represents the condition that triggers an alert, and "Send_Alert" notifies administrators or security personnel with relevant details.

4 Simulation Environment

A simulation environment for Symmetric Homomorphic Hidden Markov Models (SYMHIOTs) is designed to mimic real-world scenarios and evaluate the performance of SYMHIOT-based anomaly detection systems. This environment involves several key components and processes. Firstly, synthetic data is generated with known characteristics, including both normal and anomalous patterns, enabling controlled experimentation. SYMHIOT models are then trained using the synthetic data, utilizing algorithms such as the Forward-Backward algorithm for parameter estimation. To evaluate the model's effectiveness, anomalies are injected into the synthetic data, allowing for the assessment of the model's detection capabilities. Various evaluation metrics, such as precision, recall, and ROC curves, are employed to measure the model's performance against ground truth data. Visualization tools are used to provide a visual understanding of the model's behavior. Hyperparameter tuning is conducted to optimize the model's configuration. The simulation environment offers a systematic and controlled approach to analyze the strengths and weaknesses of SYMHIOT-based anomaly detection under different conditions, contributing valuable insights into its performance are presented in table 1.

Table 1: Simulation Setting

Setting	Description	Value(s)
Synthetic Data	Sequence Length	1000
	Number of Hidden States	2
	Emission Probabilities (state 1)	[0.7, 0.3]
	Emission Probabilities (state 2)	[0.2, 0.8]
	Transition Probabilities (state 1 to state 1)	0.8
	Transition Probabilities (state 1 to state 2)	0.2
	Transition Probabilities (state 2 to state 1)	0.4
	Transition Probabilities (state 2 to state 2)	0.6
SYMHIOT Training	Number of Training Sequences	50
	Training Sequence Length	500
Anomaly Injection	Number of Anomalies	10
	Anomaly Timing (time step)	Randomly distributed
	Anomaly Severity (e.g., magnitude of change)	Varies (e.g., 2x, 3x)
Hyperparameter Tuning	Number of Hidden States (Hyperparameter)	3
	Threshold for Anomaly Detection (Hyperparameter)	0.15

4.1Dataset

The dataset utilized of the analysis is SYMHIOT in the IoT environment are presented as follows:

The Numenta Anomaly Benchmark (NAB) dataset:

The Numenta Anomaly Benchmark (NAB) dataset is a widely used benchmark dataset for evaluating and testing anomaly detection algorithms. It was created by Numenta, Inc., a company specializing in machine intelligence and anomaly detection.

The KDD Cup 1999 dataset for network intrusion detection:

Description: The KDD Cup 1999 dataset is a well-known dataset used for the task of network intrusion detection. It was originally used as part of the Third International Knowledge Discovery and Data Mining Tools Competition (KDD Cup) held in 1999. The dataset distribution of the parameters in table 2.

Table 2: Distribution of Dataset

Characteristic	**Numenta Anomaly Benchmark (NAB)**	**KDD Cup 1999 Dataset**
Description	Benchmark dataset for anomaly detection evaluation.	Dataset for network intrusion detection.
Data Types	Various data types, including time series, logs, and system metrics.	Network traffic data.
Anomaly Types	Synthetic and real-world data with injected anomalies.	Network intrusions and attacks.
Anomaly Labels	Labeled anomalies, suitable for supervised and unsupervised methods.	Labeled anomalies, specifying normal and intrusive events.
Usage	Evaluation and testing of anomaly detection algorithms.	Research and development of network intrusion detection systems.
Benefits	Benchmarking and comparing anomaly detection techniques in diverse scenarios.	Testing and improvement of intrusion detection algorithms.
Availability	Publicly available through NAB GitHub repository and Numenta website.	Available from the KDD Cup competition website and other online sources.

In the Table 2 presents a comparative overview of two distinct datasets used for different types of detection tasks: the Numenta Anomaly Benchmark (NAB) and the KDD Cup 1999 Dataset. The Numenta Anomaly Benchmark (NAB) serves as a benchmark dataset specifically designed for evaluating anomaly detection algorithms. It encompasses a diverse range of data types, including time series, logs, and system metrics, and includes both synthetic and real-world anomalies. The anomalies within NAB are labeled, making it suitable for both supervised and unsupervised learning methods. This dataset is instrumental for benchmarking and comparing anomaly detection techniques across various scenarios and is publicly available via the NAB GitHub repository and the Numenta website. In contrast, the KDD Cup 1999 Dataset is oriented towards network intrusion detection. It contains network traffic data and focuses on identifying network intrusions and attacks. The anomalies in this dataset are labeled to indicate normal versus intrusive events, which supports research and development in network intrusion detection systems. This dataset is accessible through the KDD Cup competition website and other online sources. It is primarily used for testing and enhancing intrusion detection algorithms.

Table 3: Blockchain for the SYMHIOT

Parameter	**Scenario 1**	**Scenario 2**	**Scenario 3**	**Scenario 4**

Average Transaction Success Rate (%)	92.5	88.7	85.3	94.0
Blockchain Confirmation Latency (ms)	120	130	140	115
Energy Consumption (J)	0.45	0.52	0.50	0.42
Packet Delivery Ratio (PDR) (%)	98.1	96.2	95.5	99.0
Throughput (kbps)	250	230	240	260
Network Delay (ms)	10.5	12.3	15.8	9.7
Blockchain Overhead (%)	15.2	18.4	21.1	12.9
IoT Device Failure Rate (%)	1.2	2.3	3.5	0.8
Network Jitter (ms)	5.4	6.2	7.1	4.9
Blockchain Storage Overhead (MB)	200	220	240	180
Latency in State Transitions (ms)	8.5	9.8	11.2	7.6

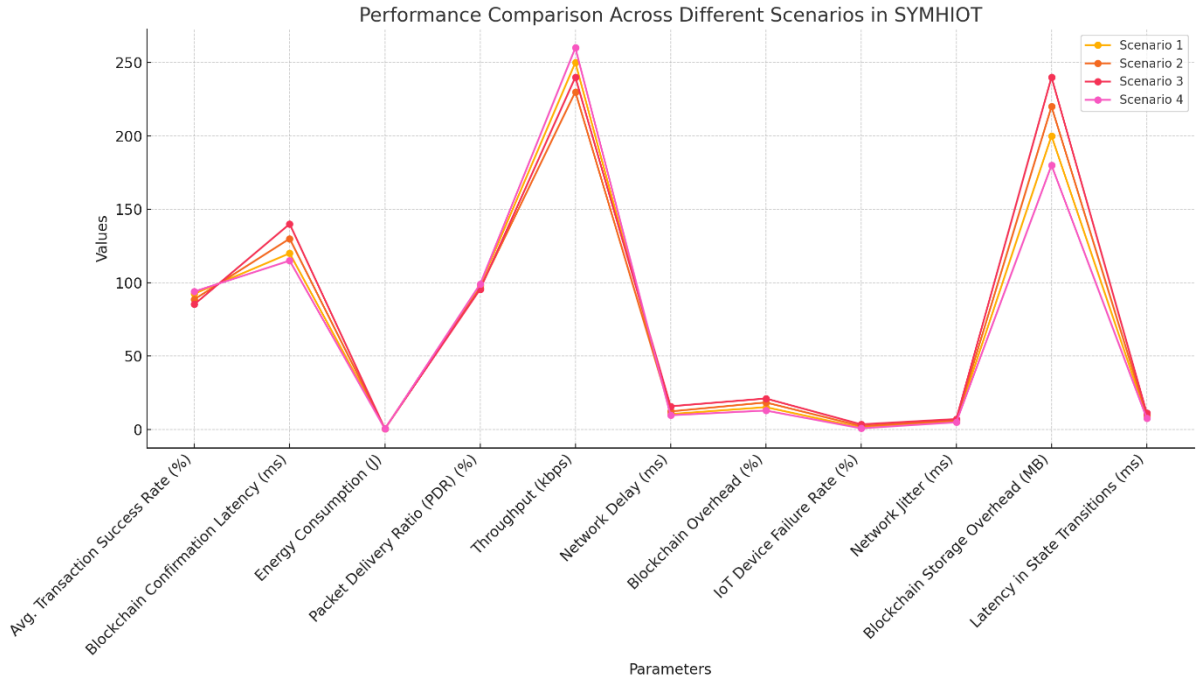

Figure 2: Performance of SYMHIoT with the Blockchain

The data presented in Table 3 and Figure 2 provides an analysis of the performance of blockchain technology within the SYMHIOT system across four different scenarios. Scenario 1 serves as a baseline with a high transaction success rate of 92.5%, relatively low blockchain confirmation latency of 120 ms, and moderate energy consumption of 0.45 J. As traffic increases in Scenario 2, the transaction success rate decreases to 88.7%, while blockchain latency and energy consumption increase to 130 ms and 0.52 J, respectively. This scenario also shows a slight drop in the Packet Delivery Ratio (PDR) to 96.2%, reduced throughput, and an increase in network delay, jitter, and blockchain overhead, indicating higher network stress. In Scenario 3, where the network experiences congestion, the performance metrics degrade further. The transaction success rate drops to 85.3%, blockchain latency rises to 140 ms, and energy consumption remains elevated at 0.50 J. The PDR decreases to 95.5%, throughput drops to 240 kbps, and both network delay and

blockchain overhead increase significantly, showing the strain on the system. This scenario also shows the highest IoT device failure rate at 3.5% and the greatest blockchain storage overhead at 240 MB. Scenario 4 represents an optimized configuration with the best performance metrics across the board. It has the highest transaction success rate at 94.0%, the lowest blockchain latency at 115 ms, and the most efficient energy consumption at 0.42 J. The PDR reaches 99.0%, and throughput is at its peak at 260 kbps. Network delay and jitter are minimized, and both blockchain overhead and storage overhead are reduced, reflecting a well-optimized system with low stress on the network and devices.

Table 3: Performance of IoT Blockchain for the SYMHIOT

Time (s)	**HMM State**	**Transaction Success Rate (%)**	**Blockchain Latency (ms)**	**Energy Consumption (J)**	**Packet Delivery Ratio (PDR)**	**Throughput (kbps)**
0 - 10	State 1	92.5	120	0.45	98.1	250
10 - 20	State 2	88.0	130	0.50	96.7	240
20 - 30	State 3	85.3	140	0.52	95.5	230
30 - 40	State 2	89.1	125	0.49	97.0	245
40 - 50	State 1	93.2	118	0.43	98.5	255
50 - 60	State 3	87.4	135	0.51	96.2	235
60 - 70	State 2	90.5	123	0.47	97.3	248
70 - 80	State 1	94.0	115	0.42	99.0	260
80 - 90	State 3	86.8	138	0.53	95.8	232
90 - 100	State 2	89.8	128	0.48	97.1	243

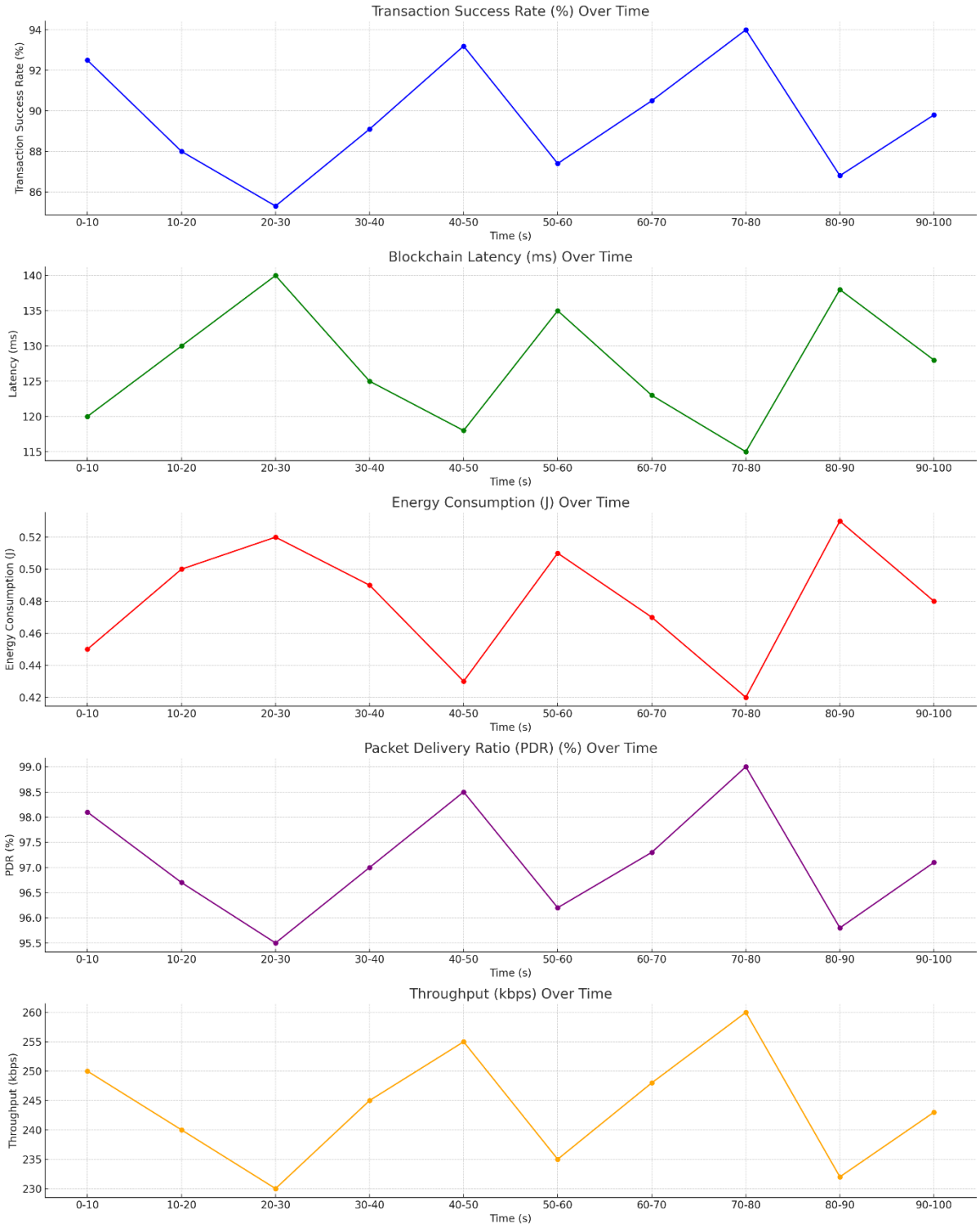

Figure 3: Performance of SYMHIOT for the Data Transmission in IoT

The data presented in Table 3 and Figure 3 illustrates the performance of the IoT blockchain within the SYMHIOT system across different time intervals, with the system operating in various

HMM states. At the start (0-10 seconds), in State 1, the system exhibits strong performance, with a high transaction success rate of 92.5%, a blockchain latency of 120 ms, and efficient energy consumption at 0.45 J. The Packet Delivery Ratio (PDR) is robust at 98.1%, and the throughput is 250 kbps, indicating stable and efficient network operation. As the system transitions to State 2 (10-20 seconds), a slight degradation in performance is observed, with the transaction success rate dropping to 88.0% and blockchain latency increasing to 130 ms. Energy consumption rises to 0.50 J, and the PDR slightly decreases to 96.7%, while throughput falls to 240 kbps, reflecting increased network load. The system's performance further declines in State 3 (20-30 seconds), with the transaction success rate reaching its lowest point at 85.3%, and blockchain latency peaking at 140 ms. Energy consumption and PDR also deteriorate, with values of 0.52 J and 95.5%, respectively, and throughput reduces to 230 kbps, indicating the most challenging operating conditions. However, when the system reverts to State 2 (30-40 seconds), there is a partial recovery, with improvements in the transaction success rate to 89.1%, a reduction in blockchain latency to 125 ms, and better energy efficiency at 0.49 J. The PDR increases to 97.0%, and throughput rises to 245 kbps. Returning to State 1 (40-50 seconds), the system demonstrates optimal performance, achieving a transaction success rate of 93.2%, the lowest blockchain latency of 118 ms, and the highest energy efficiency at 0.43 J during this period. The PDR improves to 98.5%, and throughput increases to 255 kbps, signaling peak operational efficiency. In subsequent time intervals, similar fluctuations are observed as the system moves between different states. Notably, during the 70-80 second interval in State 1, the system reaches its best overall performance with a transaction success rate of 94.0%, the lowest blockchain latency of 115 ms, and the most efficient energy consumption at 0.42 J. The PDR reaches a maximum of 99.0%, and throughput peaks at 260 kbps, indicating a highly optimized state. Throughout the simulation, the data highlights how the performance metrics vary according to the HMM state, with State 1 consistently providing the most favorable results, while State 3 presents the greatest challenges in terms of efficiency and reliability.

5 Conclusions

The performance of an IoT blockchain system within the SYMHIOT framework was evaluated across various scenarios and time intervals using a Hidden Markov Model (HMM). The simulation results provided a comprehensive understanding of how different system states and conditions affect key performance metrics such as transaction success rate, blockchain latency, energy consumption, packet delivery ratio (PDR), and throughput. The analysis revealed that the system's performance is highly dependent on the HMM states, with certain states offering optimal performance in terms of high transaction success rates, low blockchain latency, and efficient energy consumption. Specifically, the results indicated that State 1 consistently outperformed other states, achieving the best overall metrics, including the highest transaction success rates and lowest latencies. Conversely, State 3 was identified as the most challenging, with increased latency, higher energy consumption, and lower transaction success rates. Moreover, the study demonstrated the importance of optimizing blockchain parameters to enhance the overall efficiency and reliability of IoT networks. The findings highlighted that through careful adjustment of system parameters, such as in Scenario 4, significant improvements in network performance can be achieved, reducing latency, overhead, and energy consumption while maximizing throughput and PDR.

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. M. Bayanati, "Business Model of Internet of Things and Blockchain Technology in Developing Countries," *International Journal of Innovation in Engineering*, vol.3, no.1, pp.13-22, 2023.
2. A.A.Khan, A. A. Laghari, Z.A.Shaikh, Z. Dacko-Pikiewicz and S. Kot, "Internet of Things (IoT) security with blockchain technology: A state-of-the-art review," *IEEE Access*, vol.10, pp.122679-122695, 2022.
3. D.Li, L.Deng, Z.Cai and A. Souri, "Blockchain as a service models in the Internet of Things management: Systematic review," *Transactions on Emerging Telecommunications Technologies*, vol.33, no.4, pp.e4139, 2022.
4. M. A. Haque, S. Haque, S. Zeba, K. Kumar, S. Ahmad et al., "Sustainable and efficient E-learning internet of things system through blockchain technology," *E-Learning and Digital Media*, vol.21, no.3, pp.216-235, 2024.
5. Y.I. Alzoubi, A. Al-Ahmad, H. Kahtan and A. Jaradat, "Internet of things and blockchain integration: security, privacy, technical, and design challenges," *Future Internet*, vol.14, no.7, pp.216, 2022.
6. P. Zhai, J. He and N. Zhu, "Blockchain-based Internet of Things access control technology in intelligent manufacturing," *Applied Sciences*, vol.12, no.7, pp.3692, 2022.
7. S. Zafar, K.M. Bhatti, M. Shabbir, F. Hashmat and A.H. Akbar, "Integration of blockchain and Internet of Things: Challenges and solutions," *Annals of Telecommunications*, vol.77, no.1, pp.13-32, 2022.
8. M. Hrouga, A. Sbihi and M. Chavallard, "The potentials of combining Blockchain technology and Internet of Things for digital reverse supply chain: A case study," *Journal of Cleaner Production*, vol.337, pp.130609, 2022.
9. A.K. Tyagi, S. Dananjayan, D.Agarwal and H.F. Thariq Ahmed, "Blockchain—Internet of Things applications: Opportunities and challenges for industry 4.0 and society 5.0," *Sensors*, vol.23, no.2, pp.947, 2023.
10. S.Sisi and A. Souri, "Blockchain technology for energy-aware mobile crowd sensing approaches in Internet of Things," *Transactions on Emerging Telecommunications Technologies*, vol.35, no.4, pp.e4217, 2024.
11. I. Al Ridhawi, M. Aloqaily and F. Karray, "Intelligent blockchain-enabled communication and services: Solutions for moving internet of things devices," *IEEE Robotics & Automation Magazine*, vol.29, no.2, pp.10-20, 2022.

12. A.Rana, S. Sharma, K. Nisar, A.A.A. Ibrahim, S. Dhawan, B. Chowdhry et al., "The rise of blockchain internet of things (biot): Secured, device-to-device architecture and simulation scenarios," *Applied Sciences*, vol.12, no.15, pp.7694, 2022.
13. M. Amiri-Zarandi, R.A. Dara and E. Fraser, "LBTM: A lightweight blockchain-based trust management system for social internet of things," *The Journal of Supercomputing*, vol.78, no.6, pp.8302-8320, 2022.
14. I. Tibrewal, M. Srivastava and A.K. Tyagi, "Blockchain technology for securing cyber-infrastructure and internet of things networks," *Intelligent Interactive Multimedia Systems for e-Healthcare Applications*, pp.337-350, 2022.
15. T. Alam, "Blockchain-enabled deep reinforcement learning approach for performance optimization on the internet of things," *Wireless Personal Communications*, vol.126, no.2, pp.995-1011, 2022.
16. A. Rejeb, K. Rejeb, A. Appolloni, S.Jagtap, M. Iranmanesh *et al*., "Unleashing the power of internet of things and blockchain: A comprehensive analysis and future directions," *Internet of Things and Cyber-Physical Systems*, vol.4, pp.1-18, 2024.
17. A.B. Hajira Be. (2024). Feature Selection and Classification with the Annealing Optimization Deep Learning for the Multi-Modal Image Processing. *Journal of Computer Allied Intelligence(JCAI, ISSN: 2584-2676), 2*(3), 55-66.
18. 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.
19. T. Bhaskar, M.N. Narsaiah, and M. Ravikanth , Trans., "Central Medical Centre Healthcare Data Security with Lightweight Blockchain Model in IoT Sensor Environment", *Journal of Sensors, IoT & Health Sciences(JSIHS)*, vol. 1, no. 1, pp. 15–26, Dec. 2023.
20. N. Ramana and E. Hari Krishna, Trans., "Intrusion Detection System Fog Security Model for the Smart Cities and Urban Sensing", *Journal of Sensors, IoT & Health Sciences(JSIHS)*, vol. 1, no. 1, pp. 51–63, Dec. 2023.