[1]Yogesh Chandrakant Khairnar,

[2]Nagesh Salimath

Integrating Blockchain with IoT: Developing a Secure and Distributed Access Control Framework Using Advanced Algorithms

Journal of Electrical Systems

Abstract - As the Internet of Things (IoT) continues to expand, traditional access control mechanisms, such as Attribute-Based Access Control (ABAC), face challenges of scalability, security, and centralization. These models rely on centralized authorities, leading to potential single-point failures and limited adaptability in dynamic IoT environments. Blockchain technology, with its decentralized, tamper-resistant architecture, offers a promising solution to address these limitations. This research proposes a novel access control protocol for IoT environments that leverages a consortium blockchain to enhance security, scalability, and transparency. By integrating blockchain's distributed consensus mechanisms, cryptographic integrity, and smart contract capabilities, the protocol enables secure, automated decision-making without reliance on a central authority. The study explores the full computational potential of blockchain, utilizing smart contracts to implement access control judgments and manage network behavior. In doing so, it addresses key research gaps, including secure time synchronization, effective channel selection, network congestion, and the vulnerabilities of cryptographic hash functions. Additionally, this research aims to develop advanced algorithms for IoT systems, optimizing blockchain-based transactions and enhancing overall security. Through experimental analysis, the proposed framework demonstrates how blockchain technology can significantly improve access control in IoT, fostering a secure, decentralized, and efficient ecosystem for future IoT applications.

Keywords - Blockchain-based access control, Internet of Things (IoT) security, Decentralized systems, Smart contracts, Consortium blockchain.

I. INTRODUCTION

The Internet of Things (IoT) has revolutionized various sectors by enabling interconnected devices to communicate and share data, greatly enhancing efficiency, data collection, and automation across multiple industries, including engineering, agriculture, and healthcare. However, IoT's widespread connectivity also presents significant security challenges, particularly regarding data access and communication. The open communication stacks used by IoT devices make them susceptible to security breaches, as the large number of connected devices increases the attack surface for malicious actors to exploit.

To address these concerns, security models are applied across different layers of IoT architecture, such as the physical, network, and application layers. Each layer requires specific security approaches. Traditional cryptographic methods, such as encryption for data protection and authentication, are commonly used to secure IoT services. However, classical cryptography faces challenges when applied to IoT devices, especially due to the computational overhead and energy constraints on these devices. Key generation and management processes are also prone to interception, leading to vulnerabilities that can compromise data integrity and confidentiality.

In light of these limitations, blockchain technology has emerged as a promising solution for enhancing IoT security. Blockchain's decentralized and tamper-resistant ledger provides a secure platform for managing cryptographic keys and transactions. By leveraging blockchain, IoT systems can achieve greater transparency, trust, and immutability, reducing the risk of data tampering and security breaches. Smart contracts, which are self-executing contracts written into code, can automate and enforce security policies, minimizing vulnerabilities associated with traditional key management processes.

[1]Department of Computer Science and Engineering, Research Scholar, Madhyanchal Professional University, Bhopal, MP, India. kyogesh444@gmail.com

[2]Professor, Department of Computer Science and Engineering, Madhyanchal Professional University, Bhopal, MP, India. drnageshsalimath84@gmail.com

Blockchain's decentralized architecture also facilitates secure and efficient data sharing among IoT devices, mitigating the risks associated with centralized systems, which are more vulnerable to single points of failure. By distributing data across multiple nodes, blockchain enhances the resilience of IoT networks, ensuring that even if one node is compromised, the overall system remains secure. This decentralized approach is particularly beneficial in large-scale IoT deployments, where collaboration across multiple organizations and agents is required.

Blockchain as a Service (BaaS) further supports IoT by offering blockchain technology on cloud-based platforms, enabling users to develop and host their applications without managing the complex infrastructure. BaaS handles the technical challenges of maintaining and deploying blockchain cores, allowing clients to focus on their core business functions while benefiting from the enhanced security and efficiency of blockchain. Despite technical challenges in integrating blockchain with IoT, particularly in cloud-edge service environments, BaaS plays a crucial role in overcoming these barriers and accelerating the adoption of blockchain in IoT applications.

IoT applications are evolving from isolated systems to large-scale deployments, but several challenges remain, including device security, data privacy, scalability, and vendor compatibility. The lack of standardization in the IoT industry hinders communication between devices from different manufacturers, complicating interoperability. Furthermore, centralized IoT systems raise concerns about data privacy and single points of failure.

Blockchain offers solutions to many of these challenges by providing a secure, decentralized framework for managing IoT services. Numerous studies have demonstrated the effectiveness of integrating blockchain with IoT, particularly in enhancing security for real-world applications such as Fog and Cloud computing. Blockchain can be applied to IoT through several layer-wise mechanisms, including end-to-end blockchains, storage-level blockchains, gateway-level blockchains, and device-level blockchains, each addressing specific security concerns at various stages of IoT data transmission and processing.

In addition to improving security, blockchain facilitates more efficient trust management in IoT environments. Traditional centralized trust management systems suffer from single points of failure and bottleneck issues. A decentralized approach to trust management, enabled by blockchain, allows each node in an IoT network to compute and store local trust scores based on previous interactions. This decentralized model enhances accuracy and reduces vulnerabilities, offering a more reliable solution for trust management in resource-constrained IoT environments.

Overall, the integration of blockchain with IoT has the potential to revolutionize IoT security, addressing the limitations of classical cryptography while offering a decentralized, secure, and scalable framework. As IoT continues to expand into critical areas, the combination of blockchain and IoT offers a powerful solution to the security challenges that have long hindered the field, paving the way for more reliable and trustworthy IoT-enabled services.

A. Research Gap

Traditional access control models, like the Attribute-Based Access Control (ABAC), rely on centralized decision centers to enforce predefined policies. However, this centralization creates a risk of single-point failures and limits scalability, especially in dynamic environments such as the Internet of Things (IoT). The key challenge is to develop a dynamic, trustworthy, and distributed access control system for IoT. Blockchain technology offers a solution due to its decentralized, tamper-resistant nature. With cryptographic algorithms ensuring data integrity, blockchain’s distributed storage and consensus mechanisms guarantee transparency and consistency. Smart contracts, which automate and execute rules on the blockchain, can be leveraged to create decentralized access control systems without relying on a central authority.

Existing research has explored blockchain for IoT access control. Some studies have used blockchain to store and manage access policies, while others, like the Fair Access mechanism, have issued authorization tokens to control access. However, these models primarily focus on blockchain’s storage capability, missing the opportunity to fully utilize its computational potential. Smart contracts have been employed in some research, such as implementing access control judgments and managing misbehavior, harnessing blockchain's computing power.

The research gaps identified include challenges like secured time synchronization for IoT devices, effective channel selection in distributed systems, network congestion, traffic overhead, access control privilege design,

and vulnerabilities in hash functions. Addressing these gaps will enhance the efficiency, scalability, and security of blockchain-based access control systems in IoT environments.

B. Objectives

The proposed research aims to enhance IoT security by leveraging blockchain technology. It focuses on investigating the compatibility of various algorithms with blockchain to ensure stronger security for IoT environments. The study will involve implementing advanced algorithms to improve the transaction parameters within blockchain systems and evaluating their performance using specific tools. Through experimental analysis, the research will demonstrate the effectiveness of different techniques for amplifying IoT security using blockchain. Additionally, the work seeks to develop a reliable time synchronization protocol for IoT devices, ensuring consistent and secure communication across the network. Ultimately, the research strives to address IoT security challenges by integrating blockchain's decentralized and tamper-resistant features with advanced algorithms.

II. LITERATURE REVIEW

The literature review explores the integration of Internet of Things (IoT) and blockchain technology to enhance secure data communication. Blockchain's immutable and decentralized nature provides a robust framework for secure data sharing, crucial for IoT networks that are vulnerable to attacks such as replay, man-in-the-middle, impersonation, and ephemeral secret leakage. Blockchain mitigates these risks through cryptographic hash functions and decentralized consensus mechanisms, ensuring tamper-resistant and verifiable data communication. Several studies have examined the application of blockchain in IoT security. Blockchain not only secures data storage but also facilitates trust and integrity in communications among IoT devices. By leveraging blockchain's cryptographic properties, data shared within IoT networks becomes tamper-resistant and verifiable, addressing risks associated with breaches and unauthorized access.

A key focus is the combination of blockchain with Attribute-Based Access Control (ABAC) and machine learning techniques. Research has explored how these technologies can manage access rights and permissions dynamically based on attributes like user roles and contextual information. Integrating ABAC with machine learning enhances the adaptability and intelligence of access control mechanisms in IoT networks, strengthening security ([1]).

A comprehensive study reviewed from 2008 to 2019 identifies security and privacy risks in IoT and assesses the effectiveness of various countermeasures using machine learning and blockchain approaches. The study emphasizes the importance of addressing both security and privacy comprehensively and advocates for end-to-end solutions ([2]).

In the healthcare sector, blockchain's role in securing medical data and enhancing transparency is highlighted. The integration of AI with blockchain can improve data processing and patient monitoring, addressing privacy concerns and boosting data management efficiency ([3]).

The Secure Incident and Evidence Management Framework (SIEMF) combines Attribute-Based Encryption (CP-ABE) for access control with deep learning-based predictive modeling to improve incident management and forensic investigations. This approach demonstrates the potential of combining blockchain with advanced algorithms to enhance incident response and evidence integrity ([4]).

Research on supply chain management reveals blockchain's potential in improving transparency and sustainability. Blockchain, coupled with IoT, supports ethical production and consumption by providing traceability and reducing ethical concerns ([5]). Advances in hybrid models combining recurrent neural networks (RNN) with genetic algorithms show improved performance in managing supply chain data, highlighting the effectiveness of integrating machine learning with blockchain technology ([6]).

In sewage treatment management, a deep learning-based hybrid model combining classical neural network models shows effective performance in forecasting business volumes. This practical application demonstrates the benefits of advanced algorithms in operational management ([7]).

The integration of blockchain technology with Internet of Things (IoT) systems addresses several security and efficiency challenges associated with IoT networks. The Hyperledger Fabric framework is employed to enhance

security in IoT environments by utilizing cryptography, access controls, and encryption protocols. A study demonstrated that Hyperledger Fabric, when adapted for ARM64-based devices like the Raspberry Pi 4 Model B, effectively supports attribute-based access control (ABAC) mechanisms and efficient chaincode execution ([8]). This showcases Hyperledger Fabric's potential for managing IoT devices through secure and automated processes.

Centralized access control systems often fall short in IoT contexts, facing issues such as data tampering and single points of failure. A proposed attribute-based access control approach enhances efficiency and data security by avoiding the need for access control lists on every device. Blockchain technology is used to manage access and prevent privacy leaks by encrypting data and implementing smart contracts for data access and system automation ([9]).

In the healthcare sector, blockchain technology is combined with hybrid computing to create a decentralized electronic health record system. This system addresses challenges such as latency and high storage costs by incorporating a blockchain-based Distributed Data Storage System (DDSS) and selective access control mechanisms. This architecture ensures privacy and security while automating services via smart contracts, improving data traceability and stakeholder interactions in healthcare systems ([10]).

A study focused on the integration of Hyperledger Fabric for IoT systems highlights its ability to handle edge computing device limitations and scalability issues. The study measured performance metrics such as transaction throughput and latency, demonstrating that Hyperledger Fabric's implementation can efficiently manage resource usage and throughput in various IoT scenarios ([11]).

The use of blockchain technology in managing heterogeneous IoT systems is explored, emphasizing its potential to overcome issues related to decentralization and coordination. The proposed architecture supports diverse IoT devices by allowing them to select appropriate connectivity protocols, thereby reducing computational and communication overheads while enhancing system stability ([12]).

Blockchain-based solutions for IoT medical device security include data encryption and the use of off-chain databases like IPFS for scalability. This approach improves security and privacy for remote patient monitoring by encrypting data and limiting blockchain storage to essential hashes. The proposed solution shows notable improvements in security and scalability compared to existing methods ([13]).

Fog computing, which processes data at network nodes rather than centralized cloud servers, introduces new security requirements. A blockchain-based key management scheme for fog nodes addresses these needs by enabling secure group channels and resource authentication, thus improving data protection and resource management ([14]).

A comprehensive review of IoT and blockchain integration across various sectors—including supply chain, healthcare, and finance—highlights the importance of smart contracts and advanced research in addressing current challenges. This research underscores blockchain's role in enhancing IoT systems' data management and security capabilities ([15]).

Addressing issues of authentication and trust in IoT networks, a proposed system uses multiple smart contracts for managing access control and user behavior. This approach facilitates efficient access management and accountability by monitoring and penalizing misbehavior, offering a streamlined solution for IoT access control ([16]).

Overall, the literature underscores the promising potential of combining blockchain technology with advanced algorithms to address security, privacy, and efficiency challenges in IoT applications. This integration offers a powerful framework for securing data communication and enhancing IoT system functionality.

III. PROPOSED METHODOLOGY

The proposed methodology introduces an advanced framework for secure access control in Internet of Things (IoT) environments by leveraging blockchain technology, specifically Ethereum, and integrating it with machine learning algorithms. This approach addresses the limitations of traditional access control systems through enhanced security, transparency, and reliability facilitated by blockchain's decentralized and immutable nature. By integrating Ethereum's smart contract functionality, the methodology provides a robust attribute-based key

generation system for managing and enforcing data access permissions. This model improves upon existing solutions by offering a more secure and adaptable mechanism for access control in dynamic IoT settings.

Ethereum, a decentralized, open-source blockchain platform, forms the cornerstone of this methodology. Unlike Bitcoin, which functions primarily as a digital currency, Ethereum extends blockchain capabilities by enabling programmable smart contracts that execute automatically upon meeting predefined conditions. Key features of Ethereum include its smart contracts, which enforce agreements without intermediaries, and its decentralized nature, which provides security and transparency through a global network of nodes. Ethereum's native cryptocurrency, Ether (ETH), is used for transaction fees and computational services, while the Ethereum Virtual Machine (EVM) ensures code consistency across the network. Ethereum 2.0, the platform's major upgrade, introduces a Proof-of-Stake (PoS) consensus mechanism, enhancing scalability, security, and energy efficiency.

In the context of IoT, access control involves mechanisms to manage who or what can access and manipulate resources within a network. Given the proliferation of connected devices across various domains, securing these devices and the data they generate is crucial. Traditional access control systems often rely on centralized decision-making, which can create bottlenecks and vulnerabilities. The proposed methodology uses Ethereum's blockchain to decentralize control, providing immutable records of access decisions and distributing trust among network participants. This decentralized approach addresses common issues such as single points of failure and ensures a more resilient system.

Attribute-Based Access Control (ABAC) is central to the methodology, offering a dynamic and granular approach to access management. ABAC evaluates user, resource, environment, and action attributes to make context-aware authorization decisions. This method contrasts with Role-Based Access Control (RBAC), which assigns permissions based on roles. ABAC's flexibility allows for more precise control by considering multiple attributes, making it well-suited for the complex and diverse nature of IoT environments. Policies in ABAC are expressed as "if-then" rules and enforced by Policy Enforcement Points (PEP) and Policy Decision Points (PDP), which manage and evaluate access requests based on defined policies.

The integration of machine learning enhances the proposed system by improving authentication processes and real-time decision-making. Machine learning algorithms can detect anomalies and patterns within blockchain transactions, optimizing security and scalability. For example, anomaly detection algorithms can identify suspicious activities, such as Sybil attacks, by analyzing behavior patterns on the blockchain. Additionally, machine learning can optimize blockchain operations, including transaction processing and consensus mechanisms, improving overall network efficiency. Smart contracts, while beneficial, are vulnerable to bugs and security flaws. Machine learning can aid in verifying and optimizing smart contracts, ensuring they are secure and function as intended.

The training of machine learning models involves feeding them with relevant data to recognize patterns and make accurate predictions. This process includes model initialization, forward passes, loss calculation, and iterative adjustments to minimize errors. The quality and diversity of the training data are critical, as they directly impact the model's performance and ability to generalize to new data. After training, models are evaluated using validation techniques to ensure they perform well on unseen data, avoiding overfitting and ensuring robustness.

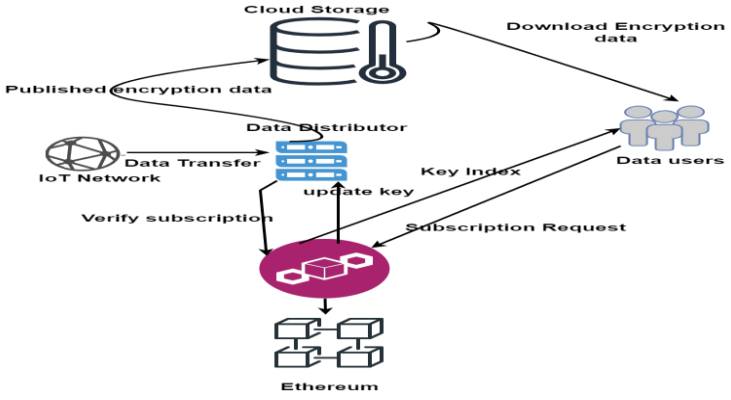

Figure 1 Proposed Model of Access Control Key Approach Based on Blockchain Technology

IV. PROPOSED ALGORITHM

The proposed algorithm outlines an innovative approach to strengthening access control mechanisms for Internet of Things (IoT) environments by integrating blockchain technology and encryption. This framework aims to create a secure and robust information service platform for managing sensitive data, such as medical information, through a combination of identity-based broadcast encryption, blockchain consensus mechanisms, and dynamic key management strategies.

The proposed model incorporates five key components: the IoT network, data distributor, data users, cloud storage, and blockchain technology. These elements work together to establish a comprehensive key management system that enhances both security and transparency.

1. IoT Network: The foundation of this access control mechanism is the IoT network, which connects various IoT devices and sensors. This network serves as the primary interface for data collection and transmission.

2. Data Distributor: The data distributor acts as an intermediary that securely and efficiently handles the transfer of data from the IoT network to subsequent stages. It plays a crucial role in managing data flow and ensuring that information is properly routed.

3. Data Users: This component represents entities, applications, or devices that require access to the data. Users must be authorized to retrieve and interact with the information stored in the system.

4. Cloud Storage: Encrypted data is stored in distributed cloud storage, which provides both scalability and accessibility. The cloud storage serves as a secure repository for sensitive information, ensuring that it is protected from unauthorized access.

5. Blockchain Technology: The backbone of the proposed key management system is blockchain technology. It offers a decentralized and tamper-resistant ledger for recording key transactions and access permissions, enhancing the system's security and transparency.

A. Algorithmic Processing

1. Node Registration and Key Generation:

- Each IoT device registers on the network and generates a public-private key pair. The public key serves as the device's unique identifier within the system.

2. Blockchain Initialization:

- Smart Contracts: Deploy smart contracts on the blockchain to manage access permissions. These contracts define functions for adding, modifying, and revoking access rights, automating the enforcement of access control policies.

3. Access Control List (ACL) Creation:

- Access Rules: Define access control rules that specify which devices or entities can interact with specific IoT devices. Store these rules in the form of ACLs on the blockchain, ensuring that access permissions are clearly defined and managed.

4. Access Request

- Permission Query: When an entity requests access to a device, it submits a request to the blockchain. This request is processed by smart contracts to verify if the requesting entity's public key matches those allowed in the ACL.

-Access Verification: Smart contracts evaluate the access request based on the defined ACL rules. Additional conditions, such as time restrictions or transaction history, may also be considered.

5. Consensus Validation:

- The blockchain network uses the chosen consensus mechanism to validate the transaction and achieve agreement on the access decision. This ensures that all network participants agree on the validity of the access request.

6. Immutable Record:

- Successful access requests and modifications to ACLs are recorded as transactions on the blockchain. This creates an immutable and transparent history of access-related activities, enhancing accountability and traceability.

7. Key Updates:

- Implement mechanisms for dynamic key exchange if access permissions need to be updated regularly. Smart contracts facilitate the secure exchange of updated keys, ensuring that the system remains current with evolving access requirements.

8. Transaction History:

- Maintain an audit trail of access-related transactions for accountability and forensic purposes. This trail helps in investigating security incidents or disputes and provides a record of all access control activities.

9. Self-Sovereign Identity:

- Explore decentralized identity solutions to give entities greater control over their identities and enhance privacy within the system.

10. Key Revocation:

- Include a mechanism for revoking access by removing a device's public key from the ACL if it becomes compromised or if there is a change in authorization.

Proposed algorithm leverages blockchain technology to enhance IoT access control by integrating decentralized ledger capabilities, smart contracts, and dynamic key management. This approach aims to create a secure, transparent, and scalable system for managing access to sensitive data in IoT environments.

Algorithm

Initialization:

- Start with a counter iii and prepare to compute patterns for each data point.

Pattern Extraction:

- For every data point, compute its pattern, extract relevant parameters, and compute vector margins.

Update Process:

- If the counter iii is greater than 0, update support vectors and weights based on previously computed results.

Set Updates:

- Update the support vector set and weights with the newly computed values.

Increment:

- Increase the counter and repeat the process for the next iteration.

Return Results:

- Once all data points have been processed, return the set of AUF values.

V. SIMULATION AND IMPLEMENTATION

The simulation is executed within a Linux-based Ubuntu environment, leveraging its robust support for a variety of development tools and frameworks critical for IoT and blockchain applications. By utilizing Ubuntu, the chapter ensures a versatile and reliable testing ground for validating the security measures of IoT systems. To incorporate blockchain technology, the simulation employs the Ethereum platform's free services. Ethereum's blockchain infrastructure provides a decentralized and secure environment for managing and validating transactions, which is essential for safeguarding user data and authenticating servers in distributed networks. The use of Ethereum facilitates the creation and deployment of smart contracts and decentralized applications (dApps),

thereby enhancing the security and efficiency of the simulated IoT systems. This approach illustrates the practical application of blockchain technology and offers a cost-effective solution for secure data management and authentication.

A. Simulation Tools

The chapter details the use of COOJA, a network simulator designed to emulate real hardware platforms specifically within the Contiki OS environment. COOJA enables the simulation of wireless sensor networks without the need for physical mote hardware. It supports various standards such as TR 1100, TI CC2420, Contiki-RPL, IEEE 802.15.4, and both uIPv6 and uIPv4 stacks. COOJA offers four propagation models to choose from:

1. **Constant Loss Unit Disk Graph Medium (UDGM):** Assumes an ideal transmission range where motes within the disk receive data packets, while those outside do not.

2. **Distance Loss UDGM:** Incorporates radio interference, with packet transmission and reception probabilities based on success ratios.

3. **Directed Graph Radio Medium (DGRM):** Accounts for propagation delays in radio links.

4. **Multipath Ray-tracer Medium (MRM):** Uses ray tracing methods like the Friis formula to calculate received power and accounts for diffraction, reflection, and refraction along radio links.

For implementing the system, Ethereum's blockchain technology is utilized, particularly its support for smart contracts. The smart contract for executing the data access control mechanism is developed using the Remix Integrated Development Environment (IDE) and deployed on the Ethereum public test network Goerli via Metamask software. Written in Solidity, the primary programming language for Ethereum smart contracts, this contract manages access control by interacting with off-chain published content and modifying the smart contract storage to reflect changes in access privileges. A comparative analysis of Ethereum gas consumption is conducted, focusing on the distribution of keys in the proposed model. Encrypted keys are stored in the smart contract as the `bytes32` data type. This analysis is crucial for evaluating the efficiency and cost-effectiveness of key management in the smart contract.

Simulation Case Study

The simulation evaluates the performance and scalability of IoT systems under various scenarios involving different numbers of users and hardware configurations. These scenarios are designed to assess how the system manages varying levels of user access and the impact of different hardware setups on IoT deployments. By simulating diverse conditions, the study aims to understand the system's efficiency, reliability, and capacity to handle multiple users and devices.

Key hardware components in the IoT simulation include Random Access Memory (RAM), Central Processing Unit (CPU), processor cores, and sensor nodes. RAM and CPU are crucial for managing the computational demands of the simulation, while processor cores aid in parallel processing and performance optimization. The number of sensor nodes is vital for simulating network scalability and handling large volumes of data from multiple sources. This comprehensive approach ensures that the simulation provides a realistic view of how IoT systems function under various operational conditions, highlighting potential challenges and performance metrics for effective deployment and management.

Table 1 Test-Bed Parameters for Simulation Scenario-1

Parameters	**Value**
NOSs	10
Data sources	2
Data rate	10 and 20packets/second
Policy changes rate	0.8 requests/second
Block generation time	1 and 2 block/minute

Block dimension	564 byte
Observation time	24 hours

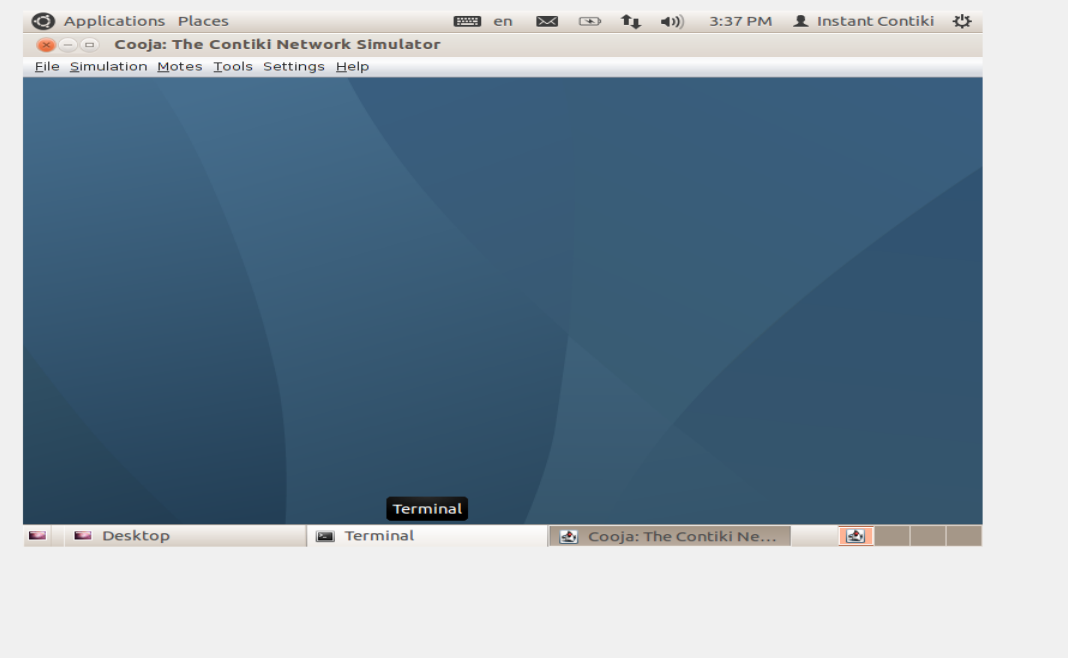

Figure 2 windows show that the Cooja is a simulator within the Contiki-NG operating system

Figure 2 windows show that the Cooja is a simulator within the Contiki-NG operating system, designed for testing and developing IoT and sensor networks. It allows for multi-level simulation, from high-level network protocols to low-level hardware interactions. Cooja can emulate real devices, enabling users to run the same firmware that will be deployed in the field.

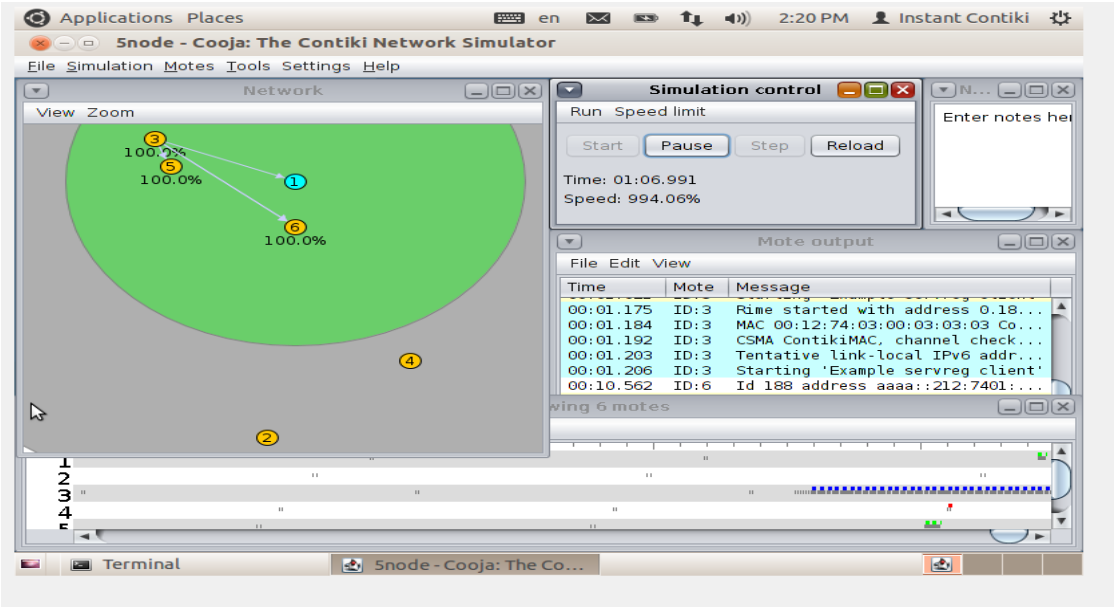

Figure 3 windows show that the Cooja, integrated into the Contiki-NG operating system

Figure 3 windows show that the Cooja, integrated into the Contiki-NG operating system, is a simulator tailored for testing and developing IoT and sensor networks. It offers multi-level simulation, covering both high-level network protocols and detailed hardware interactions. Cooja can emulate real devices, allowing users to test the same firmware intended for deployment in real-world scenarios.

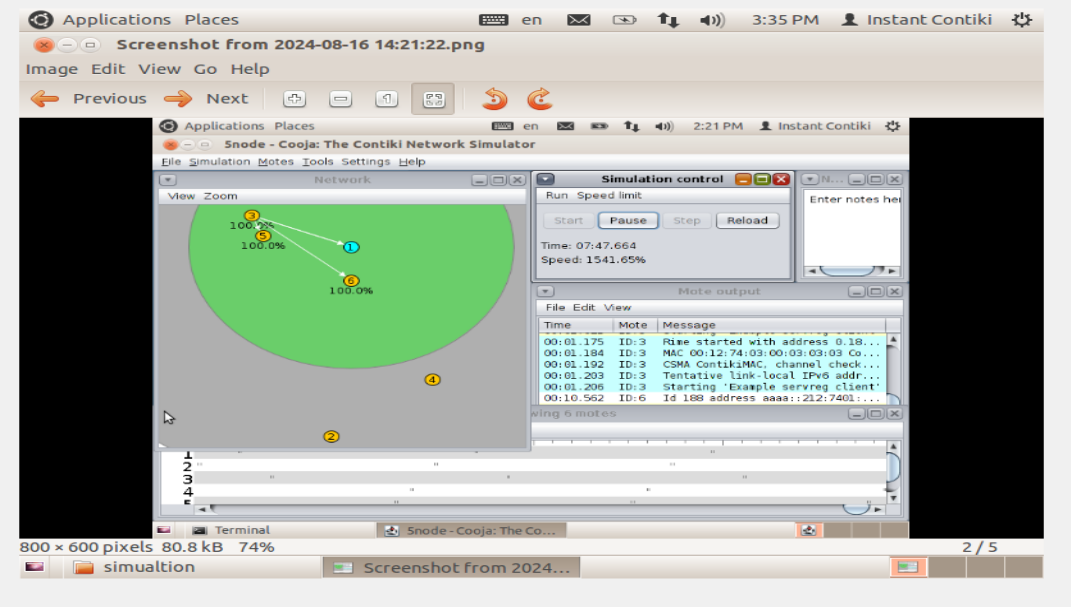

Figure 4 windows show that the Cooja, part of the Contiki-NG operating system

Figure 4 windows show that the Cooja, part of the Contiki-NG operating system, is a simulator designed for testing and developing IoT and sensor networks. It supports multi-level simulation, from high-level network protocols to detailed hardware interactions. Cooja can emulate actual devices, allowing users to test the same firmware that will be deployed in real-world environments.

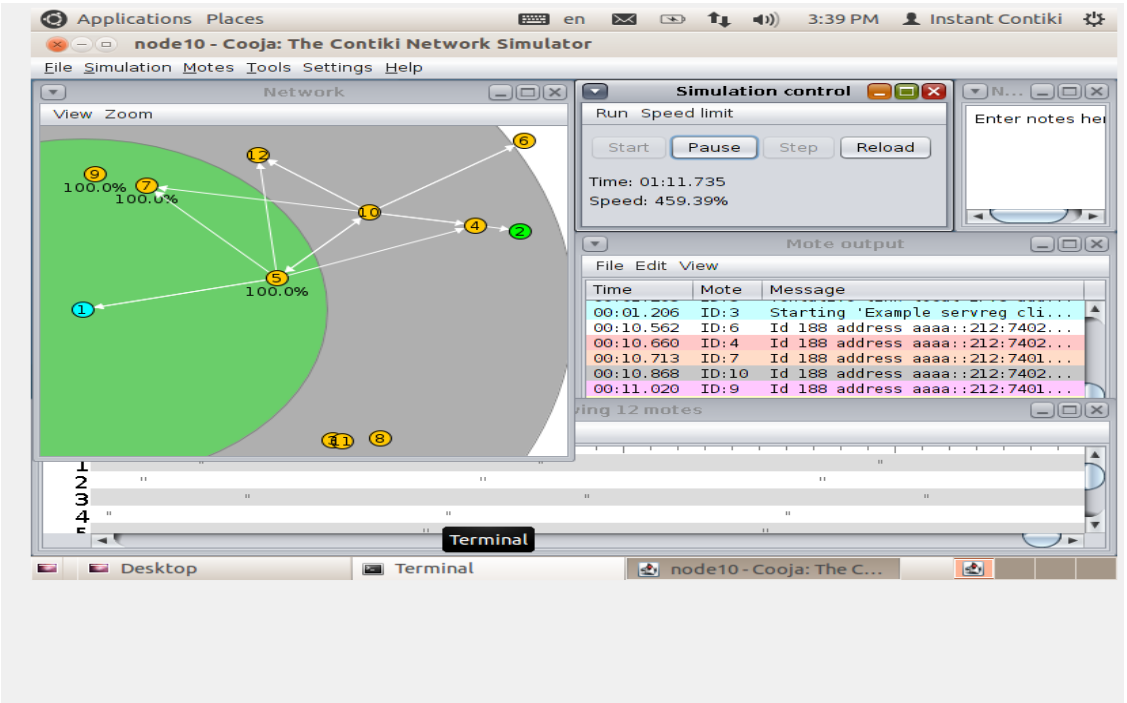

Figure 5 windows show that the Cooja is a simulator integrated into the Contiki-NG operating system

Figure 5 windows show that the Cooja is a simulator integrated into the Contiki-NG operating system, created for testing and developing IoT and sensor networks. It enables multi-level simulation, ranging from high-level network protocols to detailed hardware interactions. Cooja can emulate real devices, allowing users to run the exact firmware intended for deployment in the field.

VI. EXPERIMENT RESULT ANALYSIS

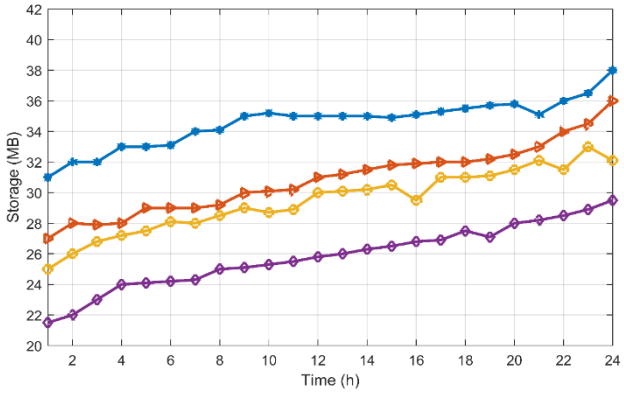

Figure: 6 Comparative performance analysis of storage (MB) and time (h) Line graph.

We saw that the value of time (h) on Storage (MB), which is better than the other three Storage (MB), is as follows: the value of time (h) 24 is 38, whereas the value of the remaining three is less, which is something like this.

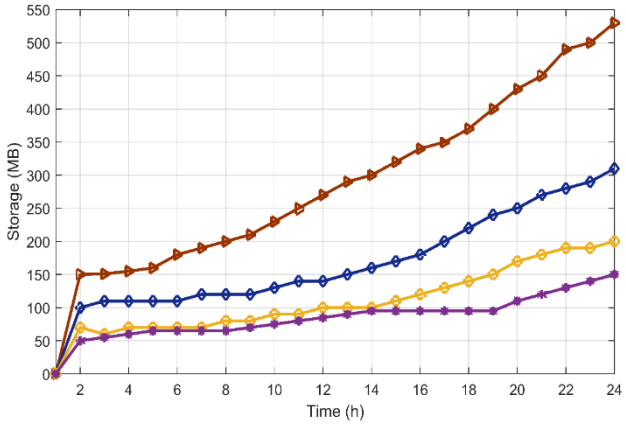

Figure: 7 Comparative performance analysis of storage (MB) and time (h) Line graph.

We saw that the value of time (h) on Storage (MB), which is better than the other three Storage (MB), is as follows: the value of time (h) 24 is 540, whereas the value of the remaining three is less, which is something like this.

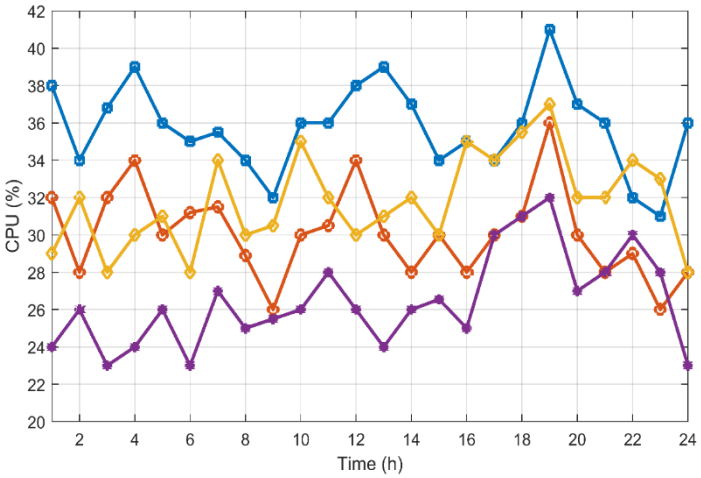

Figure: 8 Comparative performance analysis of CPU (%) and time (h) Line graph.

We saw that the value of time (h) on CPU (%), which is better than the other three CPU (%), is as follows: the value of time (h) is 41, whereas the value of the remaining three is less, which is something like this.

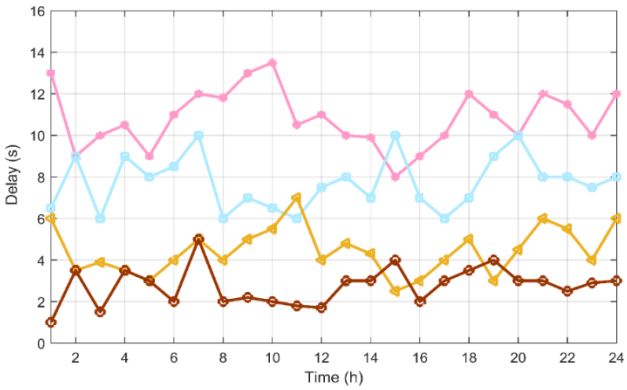

Figure:9 Comparative performance analysis of Delay (s) and time (h) Line graph.

We saw that the value of time (h) on delay (s), which is better than the other three delay (s), is as follows: the value of time (h) 10 is 13, whereas the value of the remaining three is less, which is something like this.

Scenario-2

Table 2 Test-Bed Parameters for Simulation Process

Parameters	Value
NOSs	20
Data sources	3
Data rate	20 and 30 packets/second
Policy change rate	0.10 requests/second
Block generation time	1 and 3 block/minute
Block dimension	500 byte
Observation time	24 hours

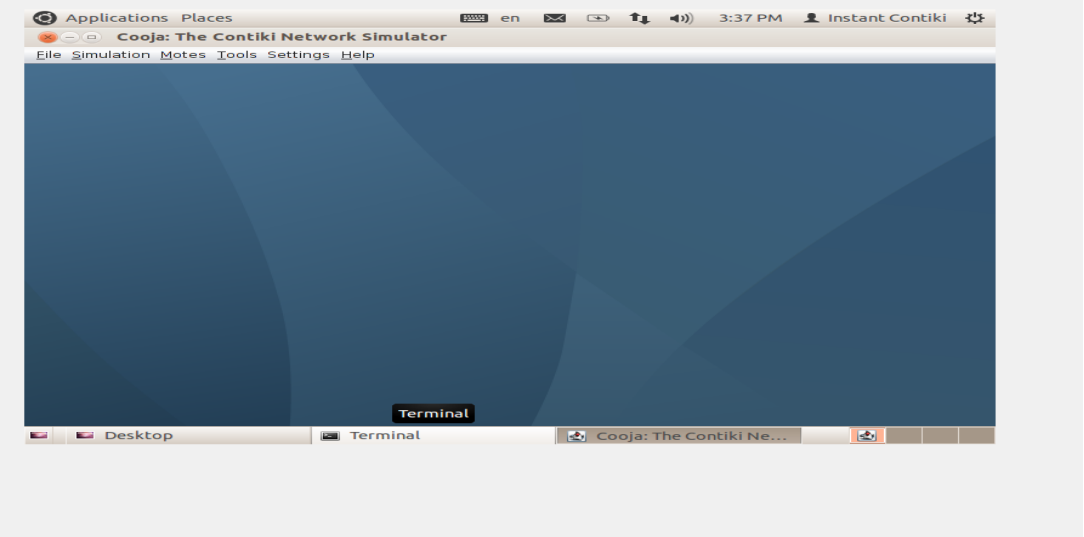

Figure 10 windows show that the Cooja, a simulator within the Contiki-NG operating system

Figure 10 windows show that the Cooja, a simulator within the Contiki-NG operating system, is designed for testing and developing IoT and sensor networks. It supports multi-level simulations, from high-level network protocols to low-level hardware interactions. Cooja can emulate real devices, allowing users to run the exact firmware that will be deployed in the field.

Figure 11 windows show that the Cooja, a simulator within the Contiki-NG operating system

Figure 11 windows show that the Cooja, a simulator within the Contiki-NG operating system, is designed for testing and developing IoT and sensor networks. It supports multi-level simulations, from high-level network protocols to low-level hardware interactions. Cooja can emulate real devices, allowing users to run the exact firmware that will be deployed in the field.

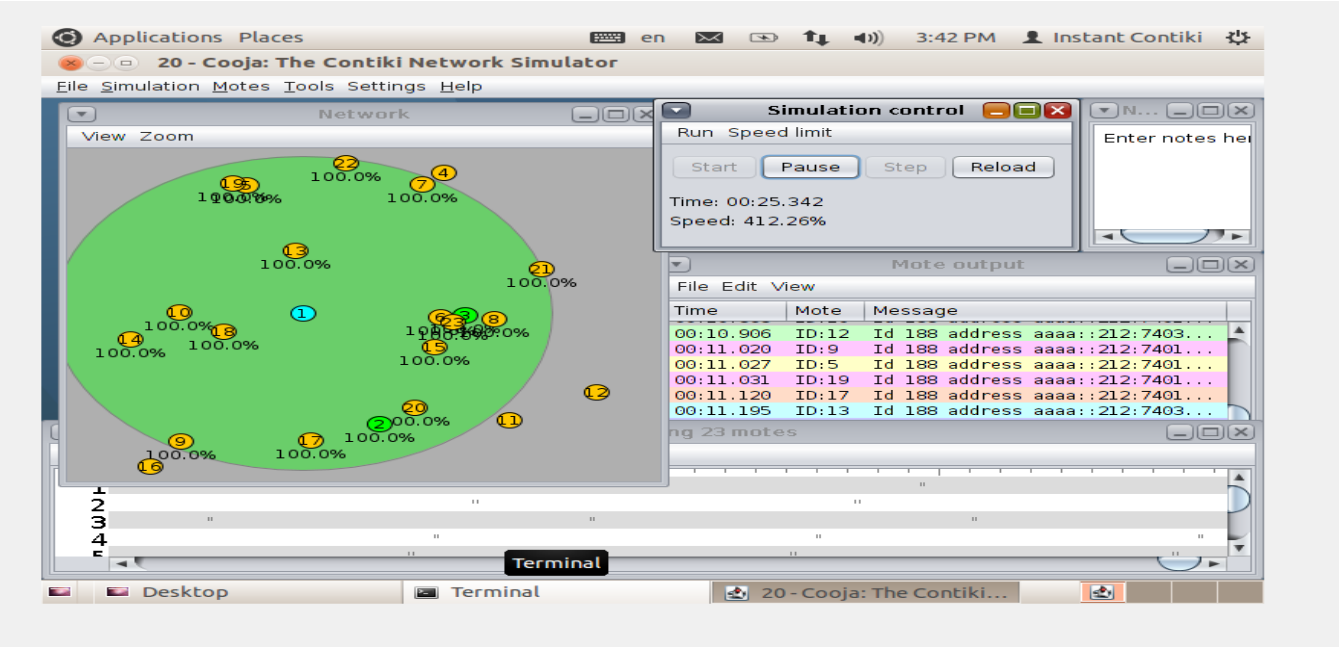

Figure 12 windows show that the Cooja, a simulator included in the Contiki-NG operating system

Figure 12 windows show that the Cooja, a simulator included in the Contiki-NG operating system, is tailored for testing and developing IoT and sensor networks. It enables multi-level simulations, spanning from high-level network protocols to low-level hardware interactions. Cooja also emulates real devices, allowing users to test the exact firmware intended for deployment in real-world environments.

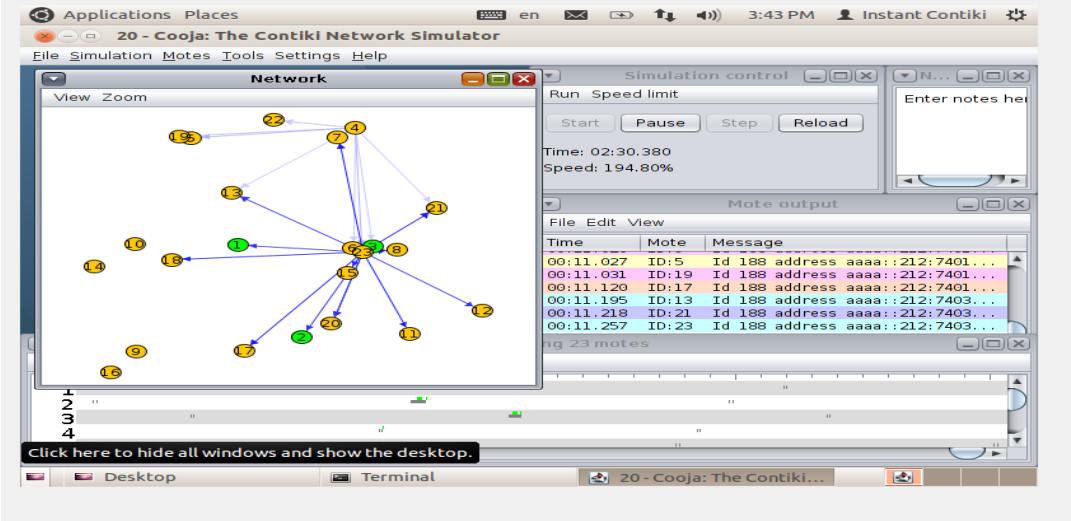

Figure 13 windows show that the Cooja, a simulator included in the Contiki-NG operating system

Figure 13 windows show that the Cooja, a simulator included in the Contiki-NG operating system, is tailored for testing and developing IoT and sensor networks. It enables multi-level simulations, spanning from high-level network protocols to low-level hardware interactions. Cooja also emulates real devices, allowing users to test the exact firmware intended for deployment in real-world environments.

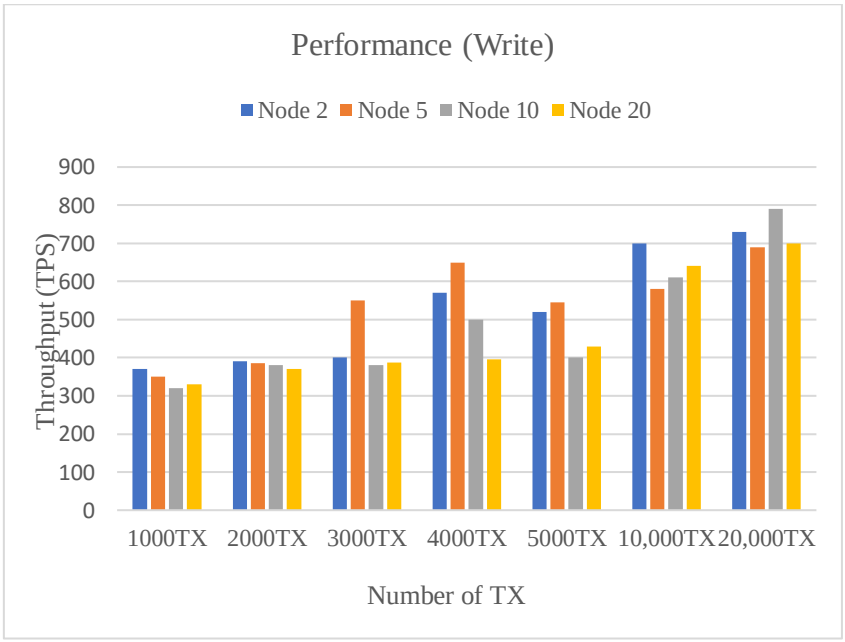

Figure 14 performance of write operation in number of transactions on different nodes of IoT devices.

We obvers that the value of node 2 is better than the other three nodes, which is as follows: the value of node 2 is 750 at the number of TX 10,000, which is better than the rest of the nodes, while the value of node 5 is 650 at the number of TX 4000, and that of node 10 is The value number of TX at 20,000 is better than the rest of the nodes, whose value is 790, and the value number of TX at 20,000 is 700.

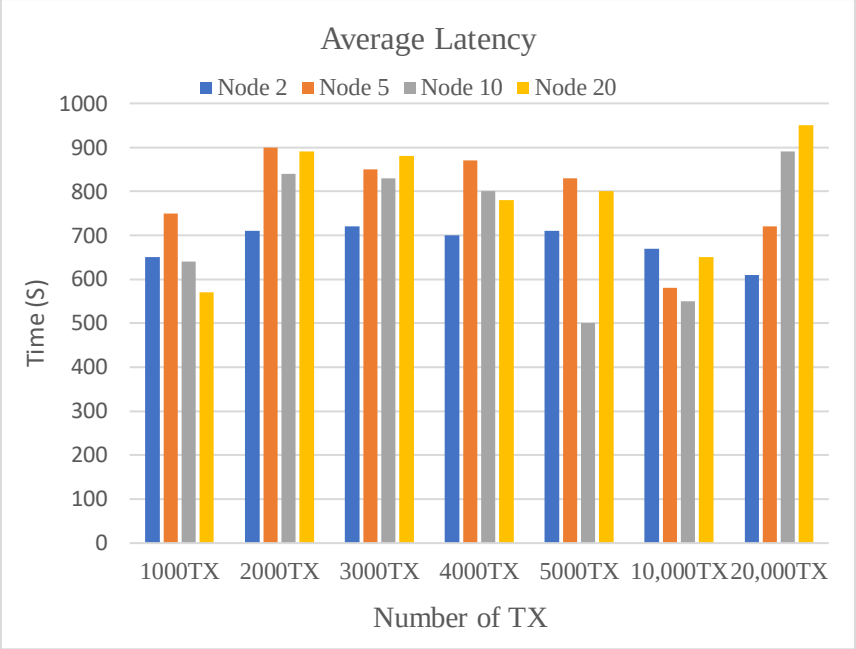

Figure 15 Performance of average latency of IoTs nodes of different transaction

We obvers that the value of node 5 is better than the other three nodes, which is as follows: the value of node 5 is 900 at the number of TX 2000, which is better than the rest of the nodes, while the value of node 20 is 950 at the number of TX 20,000, and that of node 10 is The value number of TX at 20,000 is better than the rest of the nodes 2, whose value is 890, and the value number of TX at 20,000 is 720.

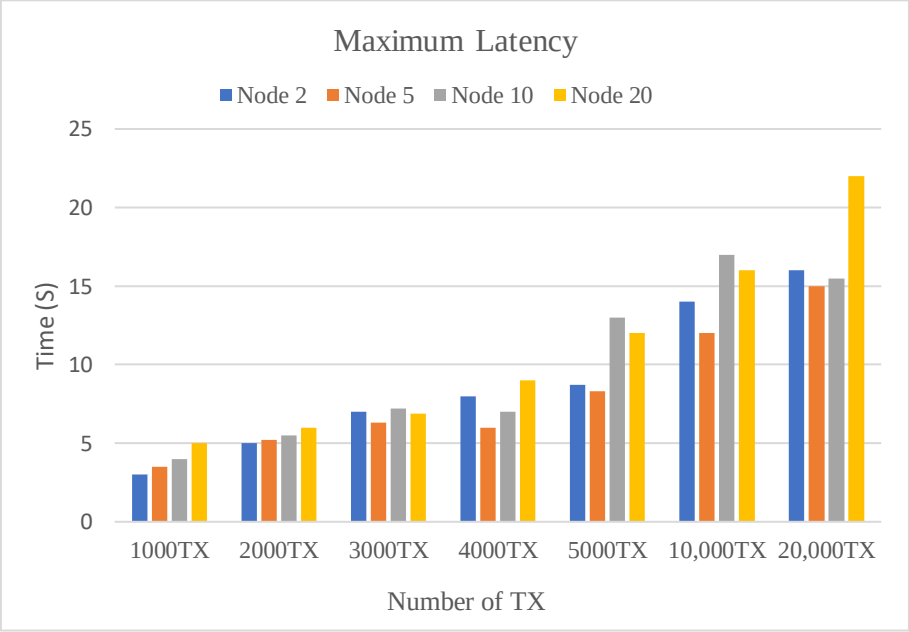

Figure 16 Performance of maximum latency of blockchain for different nodes of IoT devices

We obvers that the value of node 20 is better than the other three nodes, which is as follows: the value of node 20 is 22 at the number of TX 2000, which is better than the rest of the nodes, while the value of node 2 is 16 at the number of TX 20,000, and that of node 17 is The value number of TX at 10,000 is better than the rest of the nodes 10, whose value is 5, and the value number of TX at 20,000 is 15.

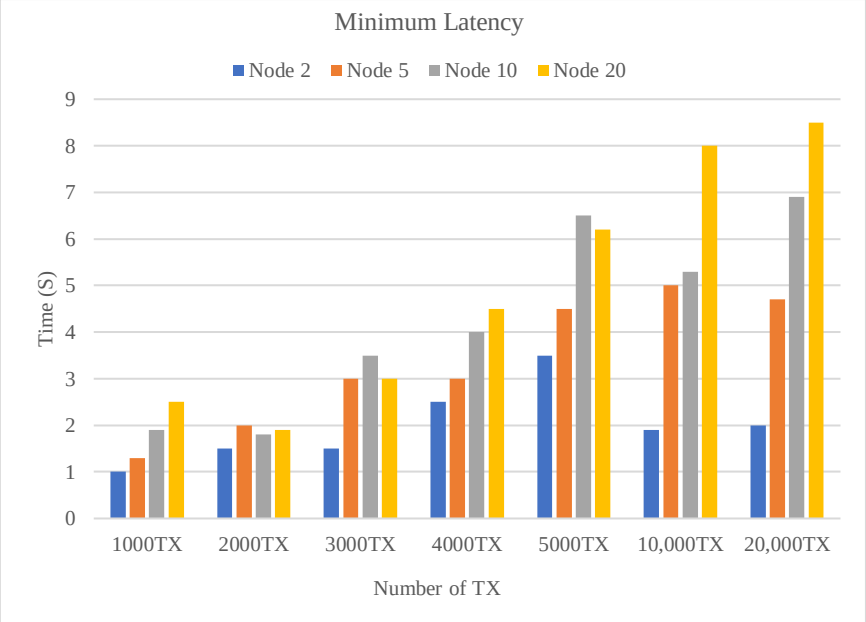

Figure 17 Performance of minimum latency of different transaction of different nodes

We obvers that the value of node 20 is better than the other three nodes, which is as follows: the value of node 20 is 8.5 at the number of TX 20,000, which is better than the rest of the nodes, while the value of node 2 is 3.5 at the number of TX 5000, and that of node 10 is The value number of TX at 10,000 is better than the rest of the nodes 6.9, whose value is 5, and the value number of TX at 10,000 is 5.

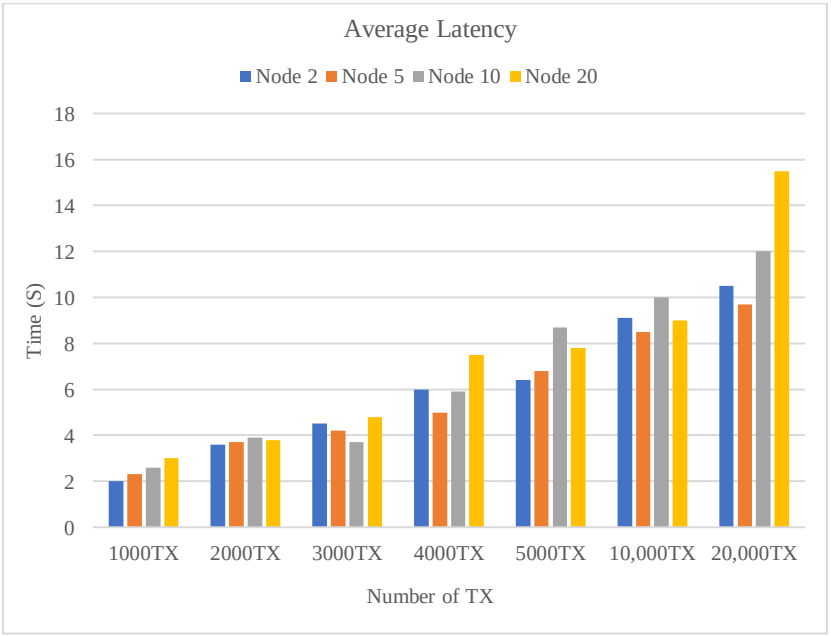

Figure 18 Performance analysis of average latency of different nodes of IoT devices

We obvers that the value of node 20 is better than the other three nodes, which is as follows: the value of node 20 is 15.5 at the number of TX 20,000, which is better than the rest of the nodes, while the value of node 2 is 10.5 at the number of TX 5000, and that of node 10 is The value number of TX at 10,000 is better than the rest of the nodes 12, whose value is 9.7, and the value number of TX at 10,000 is 5.

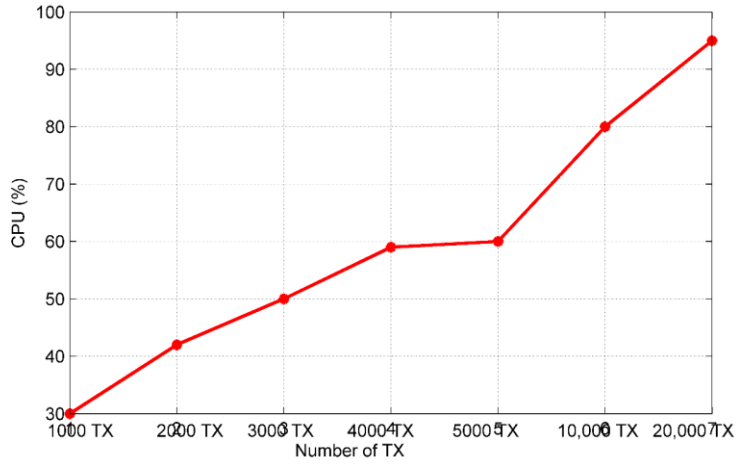

Figure 19 Performance analysis of CPU utilization of different transaction of IoT nodes

We obvers that the value of the CPU% is better, which is shown like this at the number of TX 20,000, which is better, and whose value is 95, which is something like this.

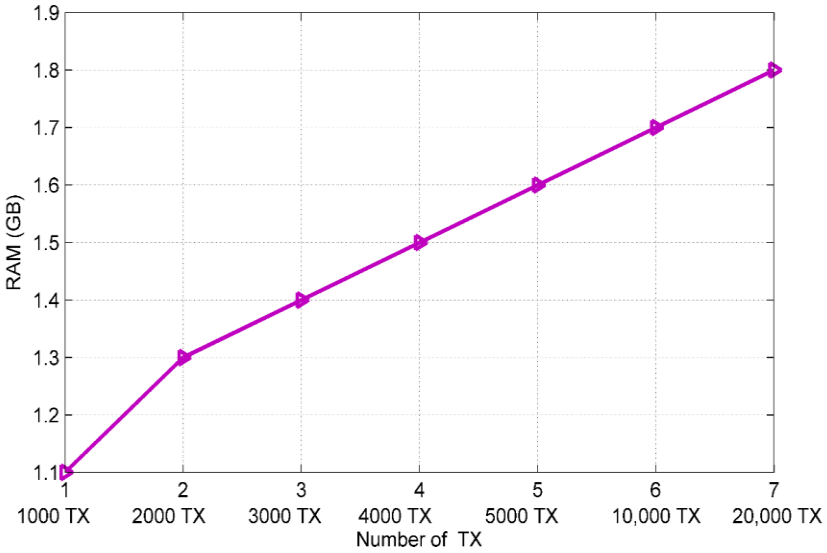

Figure 20 Performance analysis of memory utilization (RAM) in different transaction of different IoT nodes

We obvers that the value of the RAM (GB) is better, which is shown like this at the number of TX 20,000, which is better, and whose value is 1.8, which is something like this.

VII. CONCLUSION

A blockchain-based anonymous data-sharing paradigm designed to enhance security, anonymity, data privacy, and authenticity in distributed computing environments. The approach leverages Ethereum's blockchain for secure transaction management and smart contract deployment, while COOJA is used for simulating IoT networks. The integration of blockchain with cloud computing is explored to address scalability issues inherent in real-time IoT monitoring. The proposed system utilizes Ciphertext-Policy Attribute-Based Encryption (CP-ABE) to manage fine-grained access control, overcoming key escrow issues by employing a two-authority key generation scheme. Immediate attribute-level user revocation enhances scalability and efficiency. Future work will focus on improving system security through integrity-checking mechanisms, public verifiable deletion, and distributed payment systems. The integration of blockchain with a distributed IoT platform, addressing confidentiality and access control without central authority reliance. A novel machine learning-based blockchain

using Hyperledger Fabric is proposed, demonstrating improved scalability and security. Future research will address computational overhead, attribute-based access control issues, and vulnerabilities to man-in-the-middle attacks, aiming to optimize performance and enhance the system's adaptability and efficiency in dynamic IoT environments.

VIII. REFERENCES

[1] Waheed, Nazar, Xiangjian He, Muhammad Ikram, Muhammad Usman, Saad Sajid Hashmi, and Muhammad Usman. "Security and privacy in IoT using machine learning and blockchain: Threats and countermeasures." ACM Computing Surveys (CSUR) 53, no. 6 (2020): 1-37.

[2] Farouk, Ahmed, Amal Alahmadi, Shohini Ghose, and Atefeh Mashatan. "Blockchain platform for industrial healthcare: Vision and future opportunities." Computer Communications 154 (2020): 223-235.

[3] Philip, A. Oommen, and RA K. Saravanaguru. "Secure incident & evidence management framework (SIEMF) for internet of vehicles using deep learning and blockchain." Open Computer Science 10, no. 1 (2020): 408-421.

[4] Hirata, Enna, Maria Lambrou, and Daisuke Watanabe. "Blockchain technology in supply chain management: insights from machine learning algorithms." Maritime Business Review 6, no. 2 (2020): 114-128.

[5] Vergne, Jean-Philippe. "Decentralized vs. distributed organization: Blockchain, machine learning and the future of the digital platform." Organization Theory 1, no. 4 (2020): 2631787720977052.

[6] Khan, Prince Waqas, Yung-Cheol Byun, and Namje Park. "IoT-blockchain enabled optimized provenance system for food industry 4.0 using advanced deep learning." Sensors 20, no. 10 (2020): 2990.

[7] Wan, Keyi, Zhiwei Guo, Jianhui Wang, Wenru Zeng, Xu Gao, Yu Shen, and Keping Yu. "Deep learning-based management for wastewater treatment plants under blockchain environment." In 2020 IEEE/CIC International Conference on Communications in China (ICCC Workshops), pp. 106-110. IEEE, 2020.

[8] Iftekhar, Adnan, Xiaohui Cui, Qi Tao, and Chengliang Zheng. "Hyperledger fabric access control system for internet of things layer in blockchain-based applications." Entropy 23, no. 8 (2021): 1054.

[9] Zaidi, Syed Yawar Abbas, Munam Ali Shah, Hasan Ali Khattak, Carsten Maple, Hafiz Tayyab Rauf, Ahmed M. El-Sherbeeny, and Mohammed A. El-Meligy. "An attribute-based access control for IoT using blockchain and smart contracts." Sustainability 13, no. 19 (2021): 10556.

[10] Egala, Bhaskara S., Ashok K. Pradhan, Venkataramana Badarla, and Saraju P. Mohanty. "Fortified-chain: a blockchain-based framework for security and privacy-assured internet of medical things with effective access control." IEEE Internet of Things Journal 8, no. 14 (2021): 11717-11731.

[11] Honar Pajooh, Houshyar, Mohammad Rashid, Fakhrul Alam, and Serge Demidenko. "Hyperledger fabric blockchain for securing the edge internet of things." Sensors 21, no. 2 (2021): 359.

[12] Tseng, Lewis, Liwen Wong, Safa Otoum, Moayad Aloqaily, and Jalel Ben Othman. "Blockchain for managing heterogeneous internet of things: A perspective architecture." IEEE network 34, no. 1 (2020): 16-23.

[13] Azbeg, Kebira, Ouail Ouchetto, and Said Jai Andaloussi. "Access control and privacy-preserving blockchain-based system for diseases management." IEEE Transactions on Computational Social Systems (2022).

[14] Chen, Tong, Lei Zhang, Kim-Kwang Raymond Choo, Rui Zhang, and Xinyu Meng. "Blockchain-based key management scheme in fog-enabled IoT systems." IEEE Internet of Things Journal 8, no. 13 (2021): 10766-10778.

[15] Dwivedi, Sanjeev Kumar, Priyadarshini Roy, Chinky Karda, Shalini Agrawal, and Ruhul Amin. "Blockchain-based internet of things and industrial IoT: A comprehensive survey." Security and Communication Networks 2021 (2021): 1-21.

[16] Sultana, Tanzeela, Ahmad Almogren, Mariam Akbar, Mansour Zuair, Ibrar Ullah, and Nadeem Javaid. "Data sharing system integrating access control mechanism using blockchain-based smart contracts for IoT devices." Applied Sciences 10, no. 2 (2020): 488.

[17] Yang, Xu, Xuechao Yang, Xun Yi, Ibrahim Khalil, Xiaotong Zhou, Debiao He, Xinyi Huang, and Surya Nepal. "Blockchain-based secure and lightweight authentication for Internet of Things." IEEE Internet of Things Journal 9, no. 5 (2021): 3321-3332.

[18] Ratta, Pranav, Amanpreet Kaur, Sparsh Sharma, Mohammad Shabaz, and Gaurav Dhiman. "Application of blockchain and internet of things in healthcare and medical sector: applications, challenges, and future perspectives." Journal of Food Quality 2021 (2021): 1-20.

[19] Torky, Mohamed, and Aboul Ella Hassanein. "Integrating blockchain and the internet of things in precision agriculture: Analysis, opportunities, and challenges." Computers and Electronics in Agriculture 178 (2020): 105476.

[20] Koshy, Prescilla, Sarath Babu, and B. S. Manoj. "Sliding window blockchain architecture for internet of things." IEEE Internet of Things Journal 7, no. 4 (2020): 3338-3348.

[21] Bhor HN, Kalla M. TRUST-based features for detecting the intruders in the Internet of Things network using deep learning. Computational Intelligence. 2022; 38(2): 438–462.

[22] Pinjarkar, V. U. ., Pinjarkar, U. S. ., Bhor, H. N. ., Mahajan, Y. V. ., Patil, V. R. ., Rajput, S. D. ., Kothari, P. ., Ghori, D. ., & Bhabad, H. P. . (2023). Student Engagement Monitoring in Online Learning Environment. International Journal of Intelligent Systems and Applications in Engineering, 12(1), 292–298.

[23] Bhole, V. ., Bhor, H. N. ., Terdale, J. V. ., Pinjarkar, V. ., Malvankar, R. ., & Zade, N. . (2023). Machine Learning Approach for Intelligent and Sustainable Smart Healthcare in Cloud-Centric IoT. International Journal of Intelligent Systems and Applications in Engineering, 11(10s), 36–48.

[24] Terdale, J. V. ., Bhole, V. ., Bhor, H. N. ., Parati, N. ., Zade, N. ., & Pande, S. P. . (2023). Machine Learning Algorithm for Early Detection and Analysis of Brain Tumors Using MRI Images. International Journal on Recent and Innovation Trends in Computing and Communication, 11(5s), 403–415.

[25] H. N. Bhor and M. Kalla, "An Intrusion Detection in Internet of Things: A Systematic Study," 2020 International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India, 2020, pp. 939-944, doi: 10.1109/ICOSEC49089.2020.9215365.

[26] Picone, Marco, Simone Cirani, and Luca Veltri. "Blockchain security and privacy for the Internet of Things." Sensors 21, no. 3 (2021): 892.

[27] Sawant, S., Soni, P., Somavanshi, A., Bhor, H.N. (2024). Enhancing Medical Education Through Augmented Reality. Lecture Notes in Networks and Systems, vol 878. Springer. https://doi.org/10.1007/978-981-99-9489-2_16.

[28] S. Jogi, S. Warang, H. N. Bhor, D. Solanki and H. Patanwadia, "NLP Unleashed: Transforming Employment Landscapes with Dynamic Recruitment Platforms," 2024 Sixth International Conference on Computational Intelligence and Communication Technologies (CCICT), Sonepat, India, 2024, pp. 455-459, doi: 10.1109/CCICT62777.2024.00104.

[29] Pinjarkar, V.U., Pinjarkar, U.S., Bhor, H.N., Rathod, S.Crowdfunding Campaigns Web Application using Metamask, 6th IEEE International Conference on Advances in Science and Technology, 2023, pp. 217–222.

[30] Pinjarkar, V., Pinjarkar, U., Bhor, H., Jain, A. (2024). Power Ballot: Exploiting Blockchain Technology. Lecture Notes in Networks and Systems, vol 1136. Springer, Cham. https://doi.org/10.1007/978-3-031-70789-6_26