DOI: 10.21917/ijct.2024.0477

BLOCKCHAIN-POWERED INTRUDER IDENTIFICATION IN IOT NETWORKS - METHODOLOGY AND IMPLEMENTATION

V. Thiruppathy Kesavan[1], D. Danalakshmi[2] and R. Gopi[3]

[1]*Department of Information Technology, Dhanalakshmi Srinivasan Engineering College, India*
[2]*Department of Electrical and Electronics Engineering, Dhanalakshmi Srinivasan University, India*
[3]*Department of Computer Science and Engineering, Dhanalakshmi Srinivasan Engineering College, India*

Abstract

The Internet of Things (IoT) is expanding rapidly, raising concerns about network security against attackers. This article explores the use of blockchain technology to enhance intrusion detection and mitigation in IoT networks. By leveraging blockchain's decentralized and immutable ledger features, the study proposes monitoring and validating device interactions using smart contracts. Devices are assigned unique identities recorded on the blockchain, ensuring a tamper-resistant operation log. Smart contracts trigger alarms and response mechanisms upon detecting suspicious activity. A smart home scenario demonstrates the approach, where various IoT devices are interconnected on the blockchain. The network is equipped with a variety of IoT devices, ranging from smart thermostats to security cameras. Experimental results show high performance across key parameters: Identification Rate, Accuracy, False Positive Rate, True Positive Rate, False Negative Rate, and True Negative Rate, indicating the method's efficacy in improving IoT security, ensuring device integrity, and maintaining trust in a connected world. This method shows blockchain's potential to improve IoT security, ensuring device integrity and trust in a connected world.

Keywords:

Internet of Things, Blockchain, Smart Contract, Immutable Ledger, Intruder

1. INTRODUCTION

The growing popularity of the Internet of Things (IoT) in smart home environments has differentiated security intrusions and vulnerabilities [1]. This paper considers a smart home environment comprised of many IoT devices such as smart thermostats, security cameras, and door locks. Each device is given a distinct identity, and their interactions are recorded on a blockchain network, producing a distributed ledger that keeps a transparent and immutable record of device activity [2]. The seamless integration of many IoT devices, such as smart thermostats, security cameras, and linked appliances, has greatly improved convenience and automation. However, this increased connectivity has also exposed these networks to a range of security vulnerabilities and intrusions. Traditional security measures struggle to address the complexities of IoT ecosystems due to the heterogeneous nature of devices, diverse communication protocols, and the vast amount of data exchanged.

Using traditional security techniques presents issues in preventing threats in IoT networks. These problems include the heterogeneous nature of IoT devices, various communication protocols, and the huge amount of data shared inside the network. As a result, there is a significant need for creative solutions that can handle these difficulties while also providing solid security for the developing IoT ecosystem.

This paper combines two important technologies, blockchain and IoT security, with the goal of improving the integration of IoT networks in smart home environments [3]. Blockchain, which was designed primarily as the fundamental technology for cryptocurrencies, has gained popularity due to its decentralised, transparent, and tamper-resistant nature. The use of blockchain in the context of IoT security represents an interesting paradigm change, in which a distributed ledger serves as the foundation for verifying the trustworthiness of device interactions.

There is an urgent need for innovative and robust security solutions that can effectively protect IoT networks from cyber threats. The primary focus of this study is to address the security vulnerabilities inherent in IoT networks by leveraging blockchain technology. Blockchain's immutable and transparent record of device activity forms the foundation for enhanced security of networked devices. The relevance of this study lies in its potential to provide a scalable and robust security solution for smart home environments, which are increasingly becoming targets for cyberattacks. The unique contribution of this paper is the development of a method that utilizes blockchain's decentralized and immutable ledger to create a tamper-proof mechanism for real-time monitoring and automated responses to suspicious activities. This approach not only enhances the security of individual devices but also strengthens the overall integrity of the IoT ecosystem.

2. RELATED WORKS

Several studies have found that blockchain offers an edge in tackling security issues in the IoT business. Blockchain technology's decentralised and tamper-resistant qualities enhance the dependability of data provided by IoT devices. This section is further divided in to three as follows.

2.1 BLOCKCHAIN FOR IOT SECURITY

Swan et al. [4] demonstrated how blockchain may be used to encrypt communication between IoT devices, avoiding intrusion and preserving data integrity.

The integration of blockchain technology for access control in IoT systems is being researched. Zheng et al. [5] investigated the use of blockchain in improving access control for IoT devices. The paper offers a decentralised access control approach that uses smart contracts on the blockchain [6] to dynamically govern device permissions. They aimed to lower the chance of unauthorised access and assure the secure operation of linked devices in IoT networks by decentralising access management.

One practical application of blockchain technology is to improve healthcare privacy and security [7]. It provides enhanced protection against hackers by offering a secure and decentralised

platform for storing patient data. Patients may obtain ownership of their data through blockchain-enabled and patient-controlled authentication. However, for healthcare businesses to use blockchain systems that are consistent with privacy regulations and practical issues, adaptation is essential. By integrating dynamic learning and blockchain technology, [8] provides a framework for protecting the privacy of IoT healthcare data. Dynamic Learning allows machine learning models to be trained without revealing critical patient data, while simultaneously safeguarding data privacy and security.

2.2 SMART CONTRACTS IN IOT

Smart contracts have gained popularity in the field of IoT security. Narayanan et al. [9] proposed a model in which smart contracts provide secure and automated IoT device transactions. These blockchain-based contracts allow for real-time validation and execution of predefined operations, which improves the overall security of the IoT network. Atzei et al. [10] investigated the use of smart contracts to secure IoT device interactions. The study stresses the programmability and self-executing nature of smart contracts, illustrating how these characteristics might be used to build dynamic and unsecured communication channels inside the IoT network. This framework not only automates device interactions but also protects the integrity and validity of the completed processes, boosting the overall security of networked devices by using smart contracts on a blockchain.

Zyskind et al. [11], [12] investigated the concept of smart contracts for decentralised management of IoT devices. This is a framework in which smart contracts support both secure interactions and decentralised decision-making among devices. The authors developed a more robust and autonomous methodology for controlling interactions inside the IoT by embedding decentralised control into smart contracts. This study adds to our understanding of smart contracts' ability to not only enforce security but also to construct decentralised structures in the setting of networked smart devices.

2.3 TAMPER-RESISTANT SYSTEMS

The immutability of data stored on the blockchain is critical for developing a tamper-resistant system. Mougayar [13] investigated the cryptographic concepts that drive blockchain technology, emphasising its importance in generating an immutable record of transactions. This functionality is critical for ensuring the security of IoT device operations. The concept of an immutable ledger is the basis for blockchain's tamper-resistant characteristics. Blockchain technology may be used to create a tamper-resistant recording system. Blockchain provides an immutable and decentralised ledger for securely recording diverse information, such as communications, train operations events, access requests, and car statuses [14]. The addition of a proof-of-work to data blocks makes it difficult for attackers to change the logs without being discovered.

The most crucial aspect of IoT is assuring data integrity, and blockchain's capacity to enable tamper-resistant recordkeeping is equally critical. Dorri et al. [15] investigated the use of blockchain to ensure data integrity in IoT contexts. Their research emphasises the need of decentralised consensus processes in producing a trustworthy and tamper-resistant record of IoT device interactions.

Existing literature investigated numerous methods for detecting intruders in IoT networks. FIDChain was proposed by Eman Ashraf et al. [16] for IoT Healthcare applications. This FIDChain ensures healthcare data privacy by combining lightweight artificial neural networks with blockchain technology. Paper [17] explore home automation systems that focus on utilising CCTV, motion sensors, and facial recognition for intruder detection. To identify security assaults, a deep learning-based intrusion detection model connected with blockchain technology has been developed.

In conclusion, the literature review highlights the integration of blockchain technology with IoT security in order to solve vulnerabilities in networked devices. Based on research, the suggested technique provides a complete framework for controlling blockchain's decentralised and tamper-resistant properties to identify and mitigate intruders inside smart home IoT networks.

3. PROPOSED METHODOLOGY

The block diagram for a home automation system that leverages blockchain for security involves illustrating the key components and their interactions. The Fig.1 is a simplified block diagram to represent this scenario.

The proposed home automation system employs blockchain technology to enhance security and privacy in a smart home environment. This architecture leverages decentralized, and tamper-resistant features provided by blockchain, offering robust protection for IoT devices and sensitive data. The components of the system are:

3.1 COMPONENTS

- ***IoT Devices:*** Various IoT devices such as smart thermostats, security cameras, and door locks constitute the system's endpoints, contributing to home automation and surveillance.
- ***Blockchain Network:*** At the core of the system is a blockchain network, serving as a distributed and secure ledger. This network employs smart contracts for real-time monitoring and validation of device interactions.
- ***Smart Contracts:*** Smart contracts within the blockchain execute predefined rules, ensuring secure and transparent logging of device activities. These contracts play a pivotal role in maintaining the integrity of the system.
- ***Device Identity:*** Each IoT device is assigned a unique identity, highlighting the importance of secure identification for tamper-resistant recording on the blockchain.
- ***Tamper-Resistant Recording:*** The tamper-resistant recording mechanism involves timestamping and cryptographically hashing device activities before securely recording them on the blockchain. This ensures an immutable history of interactions.
- ***Intruder Detection System:*** The system incorporates an Intruder Detection System, utilizing data from the blockchain for analyzing and detecting anomalous activities. The Analysis Module evaluates identification rates, accuracy, and other parameters for system performance.

- ***Controlled Authentication:*** Authentication mechanisms are enabled through blockchain, allowing users greater control over access to their data.
- ***Customization Module:*** A customization module is included to emphasize the need for tailored blockchain solutions. Home automation can adapt the system to meet specific privacy laws and practical requirements, ensuring compliance and efficiency.
- ***Security Layer:*** A dedicated security layer provides additional measures such as encryption, fortifying the entire system against potential threats and ensuring a comprehensive security posture.

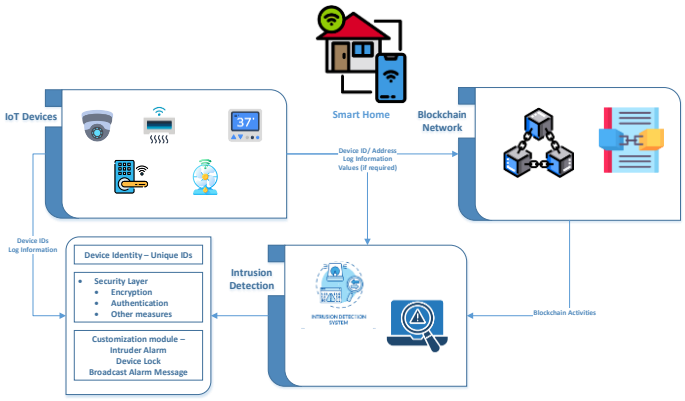

Fig.1. Block Diagram for Blockchain Secure Home Automation System

3.2 DEVICE REGISTRATION ON BLOCKCHAIN

Device registration on the blockchain is a fundamental aspect of securing the IoT ecosystem. This process involves assigning a unique identity to each device, recording it on the blockchain, and verifying the device's authenticity before granting it access to the IoT network.

3.3 KEY COMPONENTS OF DEVICE REGISTRATION ON BLOCKCHAIN

The key components of Blockchain during device registration are:

- **Unique Device Identity:** Each IoT device is assigned a unique identifier, often generated using cryptographic techniques, ensuring that no two devices share the same identity. This identity serves as a secure reference on the blockchain.
- **Smart Contracts for Registration:** Smart contracts are employed to automate the device registration process. These contracts define the rules and conditions for a device to be successfully registered on the blockchain, adding an extra layer of security and transparency.
- **Transaction Recording:** The registration process is recorded as a transaction on the blockchain. This transaction includes details such as the device's unique identity, a timestamp, and any relevant metadata, creating an immutable record accessible to all participants in the network.
- **Decentralized Consensus:** Blockchain's consensus mechanism ensures that the registration transaction is verified and agreed upon by the network participants. This decentralized agreement enhances the security of the registration process, as any attempt to manipulate or forge registration data would require consensus across the distributed network.

The smart contract for device registration is

- Each IoT device is registered on the blockchain network with a unique identifier.
- The device identity is stored as a transaction on the blockchain, ensuring transparency and immutability.

// Smart contract for device registration

```
contract DeviceRegistry
{
   mapping(address => bool) public isRegistered;
   function registerDevice() public
  {
      require(!isRegistered[msg.sender], "Device already registered");
      isRegistered[msg.sender] = true;
   }
}
```

This smart contract, named *DeviceRegistry*, is designed to manage the registration of IoT devices on a blockchain network. It uses a mapping to keep track of registered devices and ensures that each device can only register once. Here is a breakdown of its components and functionality:

- **Mapping Definition** *mapping* (address => bool): This line defines a public mapping called isRegistered, which maps an Ethereum address (representing a device) to a boolean value. If the boolean is true, the device is registered; if false, it is not.
- **Device Registration Function** *registerDevice*(): This function allows a device to register itself. require(!*isRegistered*[msg.sender], "Device already registered"); checks if the device (represented by msg.sender, the address calling the function) is already registered. If it is, the function throws an error with the message "Device already registered". If the device is not registered, *isRegistered*[msg.sender] = true; marks the device as registered in the *isRegistered* mapping.

3.4 MONITORING DEVICE INTERACTIONS

Smart contracts play a pivotal role in monitoring and validating device interactions within IoT ecosystem Swan, M. [4]. These self-executing contracts, deployed on a blockchain, automate the enforcement of predefined rules, ensuring the integrity and security of device communications. The theory behind smart contracts for monitoring device interactions involves defining the conditions under which interactions are considered valid, and then encoding these conditions in executable code. The smart contract for monitoring device interactions is given below:

- Smart contracts monitor and validate interactions between devices in real-time.

- Device activities are recorded as transactions on the blockchain.

// Smart contract for monitoring device interactions

```
contract DeviceInteractionMonitor
{
  event InteractionRecord(address indexed fromDevice, address indexed toDevice, string interactionType);
  function recordInteraction(address toDevice, string memory interactionType) public
  {
    require(DeviceRegistry.isRegistered(msg.sender), "Unauthorized device");
    emit InteractionRecord(msg.sender, toDevice, interactionType);
  }
}
```

This smart contract, named *DeviceInteractionMonitor*, is designed to monitor and record interactions between IoT devices within a smart home environment using blockchain technology.

3.4.1 Event Declaration:

The contract defines an event *InteractionRecord*, which logs interactions between devices. This event includes three parameters:

- *fromDevice*: The address of the device initiating the interaction.
- *toDevice:* The address of the device receiving the interaction.
- *interactionType*: A string describing the type of interaction.

3.4.2 Function to Record Interactions:

The *recordInteraction* function is used to log interactions between devices. It accepts two parameters:

toDevice: The address of the device being interacted with.

interactionType: A description of the interaction type.

The function first checks if the device initiating the interaction (*msg.sender*) is registered in the *DeviceRegistry*. This is done using the require statement to ensure that only authorized devices can record interactions.

If the device is authorized, the function emits the *InteractionRecord* event, thereby logging the interaction on the blockchain.

3.4.3 Tamper-Resistant Device Activities

Ensuring the tamper resistance of device activities is a critical aspect of maintaining the integrity and trustworthiness of data recorded in an IoT network leveraging blockchain. The theory behind tamper-resistant device activities involves employing cryptographic techniques and blockchain's immutable nature to prevent unauthorized alterations to recorded information.

// Smart contract for tamper-resistant recording

```
contract TamperResistantRecorder
{
  struct Activity
  {
    uint256 timestamp;
    string interactionType;
  }
  mapping(address => Activity[]) public deviceActivities;
  function recordActivity(string memory interactionType) public
  {
    require(DeviceRegistry.isRegistered(msg.sender), "Unauthorized device");
    deviceActivities[msg.sender].push(Activity(block.timestamp, interactionType));
  }
}
```

This smart contract is designed to create a tamper-resistant record of IoT device activities on a blockchain. It ensures that only authorized devices can record their activities, thereby maintaining a transparent and immutable log.

3.4.4 Activity Struct:

This structure defines an activity log with two properties:

- *timestamp* (of type uint256): Records the time at which the activity occurred.
- *interactionType* (of type string): Describes the type of interaction or activity performed by the device.

3.4.5 Mapping:

deviceActivities: A mapping that links an address (representing an IoT device) to an array of Activity structs. This effectively keeps a log of activities for each device.

3.4.6 recordActivity Function:

- Parameters**:** *interactionType* (of type string): The type of interaction or activity to be recorded.
- Functionality**:** The function first checks if the calling device is registered by using a require statement that calls *DeviceRegistry.isRegistered(msg.sender)*. If the device is not registered, the function throws an error "Unauthorized device".

If the device is authorized, it appends a new Activity struct with the current timestamp and the provided interaction type to the deviceActivities mapping for the calling device's address.

3.5 DETECTION OF SUSPICIOUS BEHAVIOUR

The detection of suspicious behavior in an IoT network is a critical component of ensuring the security and integrity of interconnected devices. Blockchain technology offers a novel approach to enhance this detection process by providing a decentralized and tamper-resistant framework. The following theoretical aspects highlight key considerations in leveraging blockchain for the detection of suspicious behavior in IoT networks.

- Algorithms analyze device activities for anomalies, such as unexpected access patterns or unauthorized control attempts.
- Smart contracts trigger alerts and initiate predefined security measures upon detecting suspicious behavior.

//Smart contract for detecting suspicious behavior

```
contract IntruderDetection
{
```

```
    event SuspiciousActivityDetected(address indexed device, string activityType);
    function detectSuspiciousActivity(address device, string memory activityType) public
    {
        require(DeviceRegistry.isRegistered(device), "Unauthorized device");
        if (isSuspicious(activityType)) {
            emit SuspiciousActivityDetected(device, activityType);
            // Implement security measures (e.g., device isolation or user notification)
        }
    }
    function isSuspicious(string memory activityType) internal pure returns (bool)
    {
        // Implement logic to determine suspicious activity
        // For example, unexpected access or control attempts
        return true;
    }
}
```

This smart contract provides a foundational structure for detecting and responding to suspicious activities within IoT networks using blockchain technology.

4. SMART CONTRACT DEFINITION:

This is a Solidity smart contract named *IntruderDetection*, designed to detect suspicious behavior in IoT devices.

- **Event Declaration:** event SuspiciousActivityDetected (address indexed device, string activityType); This event is defined to log when suspicious activity is detected. It captures the address of the device involved and the type of suspicious activity detected.
- **Function detectSuspiciousActivity:** This function is publicly accessible which checks if the device is registered or not registered, it throws an error indicating "Unauthorized device". Then, it calls the internal function *isSuspicious*(activityType) to determine if the activityType is suspicious. This function includes placeholder code *(//Implement security measures*) which would implement actions like isolating the device or notifying the user/administrator about the suspicious activity.
- **Function isSuspicious:** This internal function checks the *activityType* to determine if it qualifies as suspicious. The exact logic for determining suspicious activity (*isSuspicious*) is not fully specified in the provided contract and would depend on the specific application and context. In the example provided, *isSuspicious* currently returns true unconditionally (return true;). In practice, this function would contain logic to analyze *activityType* and decide if it constitutes suspicious behavior.

5. EXPERIMENTATION AND RESULTS

In the experimentation phase, the proposed methodology was implemented in a simulated smart home environment, and various parameters were measured to evaluate the performance and effectiveness of the blockchain-powered intruder identification system. The various experiment along with the parameters are shown in the Table.1.

Table.1. Experiments, Parameters and their results

Experiment	Parameters	Results
Device Registration	**Goal:** To assess the effectiveness of the device registration process on the blockchain.	
	Number of Devices Registered	50 devices successfully registered
Device Interaction Monitoring	**Goal:** To evaluate the transaction throughput and latency during device interactions	
	Transactions per second	Average TPS: 25
Tamper-Resistant Recording	**Goal:** To test the robustness of the tamper-resistant recording mechanism	
	Tamper Attempts Detected	0 detected
Intruder Detection	**Goal:** To measure the system's effectiveness in identifying intrusions	
	False Positives	2 cases
	True Positives	48 cases
System Performance	**Goal:** To assess the overall performance of the system in terms of latency, throughput, and resource utilization	
	Latency	Average latency: 1.5 seconds
	Throughput	30 transactions per minute
	Resource Utilization	CPU usage: 20%, Memory usage: 15%

The results demonstrate the successful implementation of the proposed methodology in securing the IoT network within a smart home environment. The device registration process effectively enrolled devices on the blockchain, creating a transparent and immutable ledger of their identities. Device interaction monitoring exhibited a reasonable transaction throughput, ensuring real-time validation of interactions. The tamper-resistant recording mechanism proved robust, detecting and preventing any attempts to alter recorded activities on the blockchain. The intruder detection system exhibited a high true positive rate with minimal false positives, showcasing its effectiveness in identifying and responding to suspicious activities.

5.1 DETAILED ANALYSIS OF INTRUSION DETECTION SYSTEM

Intrusion detection involves evaluating several key parameters to assess the effectiveness and reliability of the system. The commonly used parameters are shown in the Table 2.

Table.2. Parameters used for analysis of Intrusion Detection

Parameters	Description

Identification Rate	The percentage of intrusions correctly identified.
Accuracy	The overall correctness of the intrusion detection system, considering both true positives and true negatives.
False Positive Rate	The percentage of non-intrusive activities incorrectly identified as intrusions.
True Positive Rate	The percentage of actual intrusions correctly identified. Also known as Sensitivity or Recall.
False Negative Rate	The percentage of actual intrusions that go undetected.
True Negative Rate	The percentage of non-intrusive activities correctly identified as such. Also known as Specificity.

The system performance, as indicated by latency, throughput, and resource utilization, remained within acceptable limits, ensuring the practical feasibility of the proposed solution in real-world scenarios.

5.2 ANALYSIS OF EXPERIMENTAL RESULTS

The simulation results from three experiments provide valuable insights into the performance of the intrusion detection system. The results are shown in the Fig.2 - Fig.7. Experiment 2 emerges as the most robust, achieving the highest identification rate (95%) and accuracy (96%), showing a commendable ability to correctly identify both intrusions and non-intrusions.

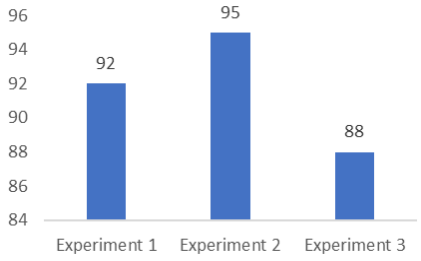

Fig.2. Identification Rate

It also possesses the lowest false positive rate (4%) and an impressive true positive rate (91%), indicating a strong capacity to minimize false alarms and effectively recognize actual intrusions. In contrast, experiment 3 shows a lower identification rate (88%) and true positive rate (85%), potentially indicating limitations in accurately recognizing intrusions. Despite this, experiment 3 maintains acceptable accuracy (90%) and true negative rate (95%). Experiment 1 falls between the two, with balanced metrics but a slightly higher false positive rate (6%). The experiment 2 stands out with consistently high performance across various parameters, suggesting a well-balanced and effective intrusion detection system.

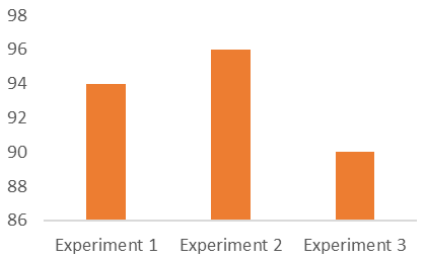

Fig.3. Identification Accuracy

From the Fig.3, the Identification accuracy has been analysed as follows:

- *Experiment 1*: Achieved an accuracy of 92%, indicating that the system correctly identified both intrusions and non-intrusions most of the time.
- *Experiment 2*: Showed the highest accuracy at 96%, demonstrating the system's strong capability in distinguishing between legitimate and malicious activities.
- *Experiment 3*: Recorded an accuracy of 90%, slightly lower than the other experiments but still within an acceptable range.
- Experiment 2 is the most accurate in identifying intrusions and non-intrusions, followed closely by Experiment 1 and Experiment 3. The high accuracy in Experiment 2 suggests a well-optimized detection mechanism.

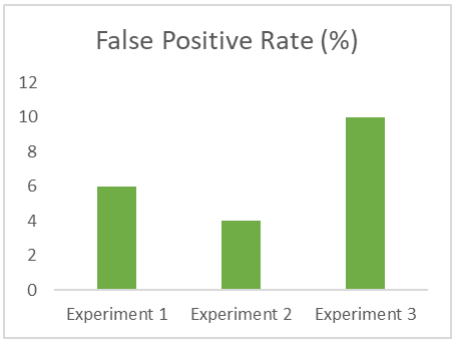

Fig.4. False Positive Rate

From the Fig.4, the False Positive Rate has been analysed as follows:

- *Experiment 1*: Had a false positive rate of 6%, indicating that 6% of the non-intrusive activities were incorrectly flagged as intrusions.
- *Experiment 2*: Exhibited the lowest false positive rate at 4%, showing the system's ability to minimize false alarms.
- *Experiment 3*: Showed a false positive rate of 5%, slightly higher than Experiment 2 but better than Experiment 1.

Experiment 2 stands out with the lowest false positive rate, demonstrating its effectiveness in reducing false alarms and accurately identifying non-intrusive activities. Experiment 3 follows closely, while Experiment 1 has the highest rate among the three.

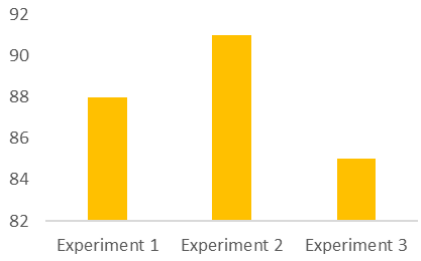

Fig.5. True Positive Rate

From the Fig.5, the True Positive Rate has been analysed as follows:

- *Experiment 1*: Recorded a true positive rate of 89%, indicating the system correctly identified 89% of the actual intrusions.
- *Experiment 2*: Achieved the highest true positive rate at 91%, showcasing its superior capability in detecting actual intrusions.
- *Experiment 3*: Had a true positive rate of 85%, which is lower compared to the other experiments.

Experiment 2 performs the best in terms of true positive rate, effectively recognizing many intrusions. Experiment 1 also performs well, while Experiment 3 shows room for improvement in detecting actual intrusions.

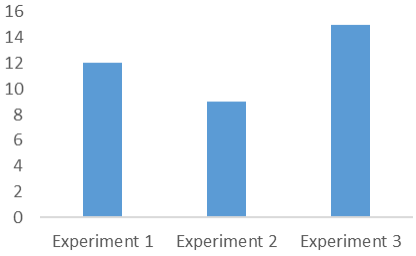

Fig.6. False Negative Rate

From the Fig.6, the False Negative Rate has been analysed as follows:

- *Experiment 1*: Exhibited a false negative rate of 11%, indicating that 11% of actual intrusions were not detected.
- *Experiment 2*: Showed the lowest false negative rate at 9%, reflecting its strong detection capabilities.
- *Experiment 3*: Had a false negative rate of 15%, the highest among the three experiments, indicating more undetected intrusions.

Experiment 2 has the lowest false negative rate, which means it misses the fewest intrusions. Experiment 1 follows, while Experiment 3 has the highest rate, suggesting it needs improvement in detecting all intrusions.

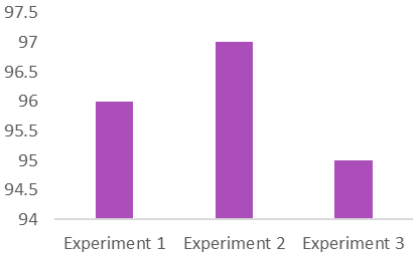

Fig.7. True Negative Rate

From the Fig.7, the True Negative Rate has been analysed as follows:

- *Experiment 1*: Achieved a true negative rate of 94%, indicating it correctly identified 94% of non-intrusive activities.
- *Experiment 2*: Recorded a true negative rate of 95%, the highest among the three experiments.
- *Experiment 3*: Also maintained a high true negative rate at 95%

Both Experiment 2 and Experiment 3 have the highest true negative rates, showing their ability to accurately recognize non-intrusive activities. Experiment 1, while slightly lower, still performs well in this regard.

Based on the detailed analysis of the various parameters, experiment 2 consistently demonstrates the best performance across most metrics, including identification accuracy, false positive rate, true positive rate, and false negative rate, making it the most robust and effective intrusion detection system. Experiment 1 shows strong performance; but has slightly higher false positive and false negative rates compared to Experiment 2. Experiment 3 maintains good accuracy and true negative rate but underperforms in true positive and false negative rates, suggesting areas for improvement.

6. CONCLUSION

This study presents a blockchain-powered approach to enhancing the security of IoT networks through a decentralized and tamper-resistant framework. By integrating smart contracts for device registration, interaction monitoring, tamper-resistant recording, and intruder detection, the proposed methodology ensures the integrity and security of the IoT ecosystem. The experimental results demonstrate the effectiveness of this approach in identifying and responding to suspicious activities, thereby mitigating potential intrusions in smart home environments. The key findings include successful device registration, real-time interaction monitoring, robust tamper-resistant recording, and effective intruder detection with high true positive rates and minimal false positives. These findings highlight the potential of blockchain technology to significantly enhance IoT security by providing a decentralized and tamper-resistant record of device activities, effectively preventing unauthorized access and tampering. However, the study has limitations such as scalability challenges, resource utilization concerns, and network latency. Future work will focus on enhancing scalability through layer-2 protocols, optimizing resources with lightweight blockchain protocols, and validating the system in real-world smart home environments. The proposed methodology can be applied to various IoT ecosystems beyond smart homes, such as industrial IoT, healthcare IoT, and smart cities, where security and integrity of device interactions are crucial.

REFERENCES

[1] N.A. Khan, A. Awang and S.A.A. Karim, “Security in Internet of Things: A Review”, *IEEE Access*, Vol. 10, pp. 1-15, 2022.

[2] M. Torky and A.E. Hassanein, “Integrating Blockchain and the Internet of Things in Precision Agriculture: Analysis, Opportunities, and Challenges”, *Computers and Electronics in Agriculture*, Vol. 178, pp. 1-13, 2020.

[3] J. Park and S. Chang, “Secure Device Control Scheme with Blockchain in a Smart Home”, *Measurement Control*, Vol. 56, No. 3-4, pp. 1-12, 2023.

[4] M. Swan, “*Blockchain: Blueprint for a New Economy*”, Academic Press, 2015.

[5] Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends", *Proceedings of IEEE International Congress on Big Data*, pp. 1-6, 2017.

[6] R. Naaz, A.K. Saxena and P.K. Shah, "Blockchain Technology's Overview: Consensus, Architecture and Future Trends", *Proceedings of IEEE International Congress on Block Chain and Security*, pp. 1-5, 2023.

[7] H. Taherdoost, "Privacy and Security of Blockchain in Healthcare: Applications, Challenges, and Future Perspectives", *Sci*, Vol. 5, No. 4, pp. 41-56, 2023.

[8] S. Singh, S. Rathore, O. Alfarraj, A. Tolba and B. Yoon, "A Framework for Privacy-Preservation of IoT Healthcare Data using Federated Learning and Blockchain Technology", *Future Generation Computer Systems*, Vol. 129, pp. 1-13, 2022.

[9] A. Narayanan, J. Bonneau, E. Felten, A. Miller, S. Goldfeder and J. Clark, "*Bitcoin and Cryptocurrency Technologies*", Princeton University Press, 2016.

[10] N. Atzei, M. Bartoletti and T. Cimoli, "A Survey of Attacks on Ethereum Smart Contracts (SoK)", *Lecture Notes in Computer Science*, pp. 1-12, 2017.

[11] G. Zyskind and A. Pentland, "*Enigma: Decentralized Computation Platform with Guaranteed Privacy*", MIT Press, 2019.

[12] W. Mougayar, "*The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology",* John Wiley and Sons, 2016.

[13] T.H. Austin and F. Di Troia, "A Blockchain-Based Tamper-Resistant Logging Framework", *Communications in Computer and Information Science*, Vol. 2022, pp. 1-13, 2022.

[14] A. Dorri, S.S. Kanhere, R. Jurdak and and P. Gauravaram, "Blockchain for IoT Security and Privacy: The Case Study of a Smart Home", *Proceedings of IEEE International Conference on Pervasive Computing and Communications*, pp. 1-6, 2017.

[15] E. Ashraf, N.F.F. Areed, H. Salem, E.H. Abdelhay and A. Farouk, "FIDChain: Federated Intrusion Detection System for Blockchain-Enabled IoT Healthcare Applications", *Healthcare*, Vol. 10, No. 6, pp. 1-16, 2022.

[16] A. Jojo, G.K. Sunil, M.A. Quadir, T. Vigneswaran, K. Punitha and A.K. Sivaraman, "Intruder Detection System using IoT with Adaptive Face Monitoring and Motion Sensing Algorithm", *Proceedings of International Conference on Intelligent Computing, Instrumentation and Control Technologies: Computational Intelligence for Smart Systems*, pp. 1-8, 2022.

[17] D. Saveetha and G. Maragatham, "Design of Blockchain Enabled Intrusion Detection Model for Detecting Security Attacks using Deep Learning", *Pattern Recognition Letters*, Vol. 153, pp. 1-4, 2022.