e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 7, Issue 12, December 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.521

6381 907 438 6381 907 438 ijmrset@gmail.com www.ijmrset.com

© 2024 IJMRSET | Volume 7, Issue 12, December 2024| DOI: 10.15680/IJMRSET.2024.0712254

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Blockchain-Based Secure Authentication Framework for IoT Networks using Artificial Intelligence

Rakesh Jain, Dr.Sathish Ramchandra Tormal

Scholar, Department of Computer Science and Engineering, Sunrise University, Alwar, Rajasthan, India

Research Supervisor, Professor, Department of Computer Science and Engineering, Sunrise University, Alwar, Rajasthan, India

ABSTRACT: The rapid expansion of the Internet of Things (IoT) has transformed modern digital ecosystems by enabling seamless communication among billions of interconnected devices across various domains such as healthcare, smart cities, industrial automation, and transportation. Despite its numerous benefits, IoT networks face significant security challenges due to their distributed architecture, limited computational resources, and large attack surface. Traditional centralized authentication mechanisms are often inadequate for IoT environments because they create single points of failure, are vulnerable to cyberattacks, and struggle to manage the large number of connected devices efficiently. To address these challenges, this research proposes a blockchain-based secure authentication framework integrated with artificial intelligence (AI) to enhance the security, reliability, and scalability of IoT networks.The proposed framework combines the decentralized and tamper-resistant characteristics of blockchain technology with the intelligent threat detection capabilities of AI algorithms.

KEYWORDS: Internet of Things (IoT), Blockchain Technology, Artificial Intelligence (AI), IoT Security.

I. INTRODUCTION

The rapid growth of the Internet of Things (IoT) has transformed the way modern systems communicate, monitor environments, and deliver services across various industries. IoT refers to a network of interconnected devices such as sensors, smart appliances, wearable devices, industrial machines, and autonomous systems that communicate and exchange data through the internet. These devices collect real-time data and enable intelligent decision-making in areas such as healthcare, smart homes, smart cities, agriculture, transportation, and industrial automation. With billions of IoT devices expected to be deployed worldwide in the coming years, the IoT ecosystem is becoming increasingly complex and dynamic. However, the rapid expansion of IoT networks has also introduced significant security challenges, particularly in terms of authentication, privacy, and secure communication.

Authentication is a critical security requirement in IoT networks because it ensures that only legitimate devices and users can access network resources and exchange data. Traditional authentication mechanisms used in conventional networks are often unsuitable for IoT environments due to the limited computational power, storage capacity, and energy resources of IoT devices. Many IoT devices are lightweight and cannot support complex cryptographic algorithms used in traditional security frameworks. As a result, these devices are vulnerable to various security threats such as identity spoofing, unauthorized access, replay attacks, and distributed denial-of-service (DDoS) attacks. Furthermore, centralized authentication systems commonly used in many IoT architectures create a single point of failure, making the entire network vulnerable if the central authority is compromised.

To address these challenges, blockchain technology has emerged as a promising solution for enhancing security in IoT networks. Blockchain is a decentralized and distributed ledger technology that allows data to be securely recorded and shared across multiple nodes without relying on a central authority. Each transaction in a blockchain is verified by network participants and stored in blocks that are cryptographically linked together, ensuring data integrity and immutability. Because of its decentralized nature, blockchain eliminates the need for a centralized authentication server and reduces the risk of single-point failures. It also provides transparency, traceability, and tamper-resistant data storage, which are essential features for securing IoT communications.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

In the context of IoT networks, blockchain can be used to manage device identities, verify authentication requests, and record transactions securely. Each IoT device can be assigned a unique digital identity stored on the blockchain. When a device attempts to join the network or communicate with another device, its identity can be verified through blockchain-based authentication protocols. Smart contracts, which are self-executing programs stored on the blockchain, can be used to automatically enforce authentication rules and access control policies. This approach improves trust among devices in the network while ensuring that unauthorized devices cannot gain access.

While blockchain provides a strong foundation for secure and decentralized authentication, it also has certain limitations when applied directly to IoT environments. Blockchain networks often require significant computational resources and storage capacity, which may not be suitable for resource-constrained IoT devices. In addition, blockchain systems may experience latency due to the time required for consensus mechanisms and block validation. These limitations make it necessary to integrate complementary technologies that can improve the efficiency and intelligence of blockchain-based IoT security frameworks.

Artificial Intelligence (AI) has gained significant attention as a powerful technology capable of enhancing the security and performance of IoT networks. AI techniques such as machine learning and deep learning can analyze large volumes of network data, identify patterns, and detect anomalies in real time. By continuously learning from network behavior, AI systems can detect suspicious activities and potential cyber threats before they cause significant damage. AI-based security systems can also adapt to evolving threats, making them highly effective in dynamic environments such as IoT networks.

II. LITERATURE REVIEW

The rapid growth of the Internet of Things (IoT) has transformed modern digital infrastructure by enabling communication among billions of interconnected devices. IoT devices are widely used in smart homes, healthcare, transportation, agriculture, and industrial automation. However, the large number of connected devices and their heterogeneous nature introduce serious security challenges, including unauthorized access, identity spoofing, data tampering, and distributed denial-of-service attacks. Consequently, researchers have focused on developing advanced security mechanisms such as blockchain technology and artificial intelligence (AI) to enhance authentication and communication security in IoT networks.

Traditional IoT security frameworks rely heavily on centralized architectures for authentication and access control. While these systems simplify management, they create single points of failure, making networks vulnerable to cyberattacks. Blockchain technology provides a decentralized solution that allows devices to authenticate and communicate securely without depending on a central authority. The blockchain operates as a distributed ledger where every transaction is verified through consensus mechanisms and recorded in immutable blocks, ensuring transparency and data integrity. Research shows that blockchain-based security solutions are increasingly applied in IoT networks because they enable secure data sharing, decentralized authentication, and tamper-proof records of device interactions.

Several studies have highlighted the potential of blockchain for enhancing authentication mechanisms in IoT systems. For example, blockchain-based authentication frameworks enable IoT devices to verify each other's identities through cryptographic keys stored on distributed ledgers. This approach eliminates reliance on centralized authentication servers and reduces the risk of data manipulation. According to surveys on blockchain cybersecurity, nearly half of blockchain security research focuses on IoT applications due to the technology’s ability to provide secure device communication and decentralized identity verification.

Despite its advantages, blockchain alone cannot fully address all security challenges in IoT networks. IoT environments generate massive volumes of data and require real-time threat detection. Traditional rule-based security systems often fail to detect new or unknown attacks. This limitation has led researchers to integrate artificial intelligence and machine learning techniques with blockchain to improve IoT security frameworks. AI algorithms can analyze large datasets generated by IoT devices and detect abnormal patterns that indicate cyber threats. Machine learning models, including supervised and unsupervised learning techniques, have been used for anomaly detection, intrusion detection, and predictive security analysis in IoT systems.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

The integration of AI with blockchain creates a powerful hybrid architecture for secure authentication in IoT networks. Blockchain ensures secure storage and verification of authentication data, while AI enhances the system's ability to identify suspicious behavior and unauthorized access attempts. Studies indicate that AI-driven anomaly detection combined with blockchain's immutable ledger significantly improves the reliability and trustworthiness of IoT communication systems. AI can also optimize blockchain operations by improving consensus mechanisms and reducing computational overhead, which is particularly important for resource-constrained IoT devices.

Another important aspect of blockchain-based IoT security is consensus mechanisms, which determine how transactions are validated within the network. Early blockchain systems relied on Proof of Work (PoW), which requires high computational power and energy consumption. This mechanism is not suitable for IoT devices with limited resources. Researchers have therefore proposed alternative consensus algorithms such as Proof of Stake (PoS), Proof of Authority (PoA), and Practical Byzantine Fault Tolerance (PBFT). These mechanisms reduce computational complexity while maintaining security, making them more suitable for IoT environments. Studies have shown that PoA and PBFT are particularly effective in permissioned blockchain networks designed for IoT applications.

III. MATERIAL AND METHODS

System Overview

The proposed framework integrates blockchain technology and artificial intelligence (AI) to create a secure authentication mechanism for Internet of Things (IoT) networks. IoT devices often operate in distributed environments and are vulnerable to attacks such as impersonation, data tampering, and unauthorized access. Traditional centralized authentication systems introduce single points of failure and scalability limitations. To overcome these issues, this research proposes a decentralized authentication architecture where blockchain ensures data integrity and trust, while AI-based models detect malicious behaviors and anomalies in device authentication requests.

The system consists of four major layers: IoT device layer, edge computing layer, blockchain network layer, and AI-based security analysis layer. These layers work together to provide secure authentication, access control, and anomaly detection in IoT communication.

Materials

IoT Devices

Various IoT devices are considered in the experimental environment to simulate real-world scenarios. These devices include sensors, actuators, smart cameras, and environmental monitoring devices. Each device is assigned a unique device identity and cryptographic key pair for authentication within the network.

The devices communicate using lightweight communication protocols such as MQTT or HTTP over wireless networks. Due to limited computing resources, lightweight encryption mechanisms and efficient authentication procedures are implemented to ensure minimal overhead on device performance.

Blockchain Platform

A private blockchain network is implemented to maintain authentication records and device registration information. Blockchain is selected because of its decentralized structure, immutability, and ability to maintain secure distributed ledgers without relying on centralized authorities.

The blockchain network consists of multiple nodes that store authentication logs and validate transactions. Each authentication request from an IoT device is recorded as a transaction in the blockchain ledger. Once verified by network nodes, the transaction becomes part of an immutable block.

Smart contracts are deployed within the blockchain network to automate device registration, authentication verification, and access control decisions. These smart contracts ensure that only registered devices with valid credentials can participate in the IoT network.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

IV. DATA ANALYSIS

The rapid growth of the Internet of Things (IoT) has led to billions of interconnected devices such as sensors, smart home appliances, wearable devices, and industrial machines. These devices continuously exchange data over networks, enabling automation and intelligent decision-making. However, the expansion of IoT has also increased security risks including unauthorized access, data breaches, device spoofing, and denial-of-service attacks. Traditional centralized authentication systems often fail to secure IoT environments due to scalability issues, single points of failure, and limited device resources.

To overcome these challenges, researchers propose Blockchain-based secure authentication frameworks integrated with Artificial Intelligence (AI). Blockchain provides a decentralized, tamper-proof ledger for verifying identities and recording transactions, while AI enables intelligent threat detection and adaptive security mechanisms. Together, these technologies offer a powerful solution for securing IoT networks and improving authentication processes.

IoT Security Challenges and Need for Secure Authentication

IoT devices are typically resource-constrained and often lack strong built-in security features. As a result, they are vulnerable to multiple cyberattacks. One major challenge in IoT networks is **authentication**, which ensures that only authorized devices can communicate within the network. Traditional authentication systems rely on centralized servers to manage credentials and verify devices. However, this architecture introduces a single point of failure, making the system vulnerable to attacks or service outages. Additionally, centralized systems struggle to handle the large number of IoT devices and transactions generated in modern smart environments.

Furthermore, IoT devices collect large amounts of sensitive data, including personal, industrial, and environmental information. If authentication mechanisms are weak, attackers may intercept or manipulate this data. Studies show that centralized IoT architectures can expose sensitive information and increase the risk of data breaches due to storing large volumes of data in a single location. Therefore, there is a need for a secure, scalable, and decentralized authentication framework that can protect IoT networks from malicious activities while maintaining efficiency.

Role of Blockchain in IoT Authentication

Blockchain technology introduces a decentralized approach to authentication and data management. Instead of relying on a central authority, blockchain stores device credentials and authentication records across multiple nodes in a distributed ledger. This ensures transparency, immutability, and trust among devices in the network. One of the main advantages of blockchain is its **tamper-resistant structure**. Once a transaction is recorded on the blockchain, it cannot be altered or deleted, ensuring the integrity of authentication data. Blockchain also eliminates single points of failure by distributing data across multiple nodes, improving the reliability of IoT systems.

In a blockchain-based authentication framework, each IoT device is assigned a unique cryptographic identity. When a device attempts to access the network, its credentials are verified through blockchain transactions and consensus mechanisms. Only verified devices are allowed to communicate with other devices in the network.Different consensus algorithms such as Proof of Stake (PoS), Proof of Authority (PoA), and Practical Byzantine Fault Tolerance (PBFT) can be used to validate transactions in blockchain networks. These algorithms are more energy-efficient than traditional Proof of Work systems and are better suited for IoT environments.

Additionally, blockchain enables smart contracts, which are self-executing programs that automatically enforce authentication rules. For example, a smart contract can verify whether a device is authorized before allowing it to send data to another device.

V. RESULT AND DISCUSSION

The proposed Blockchain-Based Secure Authentication Framework for IoT Networks Using Artificial Intelligence was implemented and evaluated to analyze its effectiveness in improving authentication security, detecting malicious behavior, and maintaining reliable communication within IoT environments. The experimental evaluation focused on several key performance indicators including authentication accuracy, detection rate of malicious nodes, latency,

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

computational overhead, and system scalability. The framework integrates artificial intelligence techniques for anomaly detection with blockchain technology for decentralized authentication and immutable record keeping. The results demonstrate that the hybrid approach significantly improves the overall security and reliability of IoT communication networks when compared to traditional centralized authentication mechanisms.

During the experimental phase, a simulated IoT environment consisting of multiple sensor nodes, gateways, and cloud services was developed. The nodes generated regular communication traffic along with simulated malicious attempts such as spoofing attacks, replay attacks, and unauthorized access attempts. Artificial intelligence algorithms were trained using historical communication patterns to identify abnormal activities and suspicious device behavior. The trained model was then integrated with the blockchain layer, where authentication requests and device identity records were stored in distributed blocks using smart contracts. The evaluation results indicated that the proposed system achieved a high authentication success rate for legitimate devices while successfully preventing unauthorized access attempts. The decentralized structure of blockchain eliminated the need for a central authority, thereby reducing single points of failure and increasing system resilience.

One of the most significant results observed during the experiments was the improvement in authentication accuracy. The AI-based detection module was able to classify legitimate and malicious requests with high precision due to its ability to learn complex communication patterns in IoT traffic. Compared with traditional rule-based authentication systems, the AI-enabled approach demonstrated greater adaptability to dynamic IoT environments where device behaviors frequently change. The blockchain component further strengthened the authentication process by maintaining tamper-proof records of device identities and transaction logs. Once a device was authenticated and registered on the blockchain ledger, its identity could not be altered without consensus from network participants. This ensured integrity and transparency across the authentication system.

Another important performance metric analyzed during the evaluation was the detection of malicious devices. The AI model showed a strong capability to detect various attack scenarios, including spoofing, impersonation, and abnormal communication bursts. The results showed a high detection rate for malicious nodes, which significantly reduced the risk of compromised devices entering the network. In many IoT environments, compromised devices can propagate attacks throughout the system, leading to data breaches or service disruptions. However, the proposed hybrid framework effectively identified suspicious nodes at an early stage and prevented them from being authenticated through the blockchain network. This proactive detection mechanism contributed to a safer communication environment for IoT applications.

VI. CONCLUSION

The integration of blockchain technology and artificial intelligence presents a promising solution for addressing the growing security challenges in Internet of Things (IoT) networks. In this research, a blockchain-based secure authentication framework enhanced with artificial intelligence techniques was proposed to improve the reliability, transparency, and trustworthiness of communication among IoT devices. Traditional authentication mechanisms often struggle to provide adequate security in IoT environments due to the large number of connected devices, limited computational resources, and the presence of various cyber threats. By combining the decentralized nature of blockchain with the intelligent decision-making capability of AI, the proposed framework offers a robust approach to strengthening authentication and protecting sensitive data within IoT networks. The blockchain component of the framework ensures that authentication records are stored in a decentralized and tamper-resistant ledger. This eliminates the need for a centralized authority and reduces the risk of single points of failure or data manipulation. Each authentication transaction is securely recorded and verified through consensus mechanisms, providing transparency and immutability. As a result, unauthorized modifications or malicious access attempts can be easily detected and prevented. Furthermore, the use of smart contracts enables automated verification of device identities and access permissions, improving the efficiency and reliability of authentication processes in the network.

Artificial intelligence plays a critical role in enhancing the overall security of the system by analyzing patterns in network behavior and identifying potential threats. Machine learning algorithms can monitor device communication and detect anomalies that may indicate unauthorized access, compromised devices, or malicious attacks. By continuously learning from new data, the AI model becomes more effective in identifying suspicious activities and

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

preventing security breaches before they cause significant damage. This intelligent monitoring mechanism significantly strengthens the defense capability of IoT systems compared to conventional rule-based security approaches.

The hybrid framework also improves scalability and adaptability in dynamic IoT environments. As the number of devices connected to IoT networks continues to grow rapidly, maintaining secure authentication becomes increasingly complex. The decentralized nature of blockchain allows the system to handle large-scale networks without compromising security or performance.

REFERENCES

1. Waheed, N., He, X., Ikram, M., Usman, M., & Hashmi, S. S. (2020). *Security and privacy in IoT using machine learning and blockchain: Threats and countermeasures*. IEEE Access / arXiv.
2. Dhieb, N., Ghazzai, H., Besbes, H., & Massoud, Y. (2020). *Scalable and secure architecture for distributed IoT systems*. IEEE Internet of Things Journal.
3. Ali, J., Ali, T., Musa, S., & Zahrani, A. (2020). *Towards secure IoT communication with smart contracts in a blockchain infrastructure*. IEEE Access.
4. Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). *On blockchain and its integration with IoT: Challenges and opportunities*. Future Generation Computer Systems.
5. Dorri, A., Kanhere, S. S., & Jurdak, R. (2017). *Blockchain in Internet of Things: Challenges and solutions*. IEEE Internet of Things Journal.
6. Dorri, A., Kanhere, S. S., & Jurdak, R. (2016). *Blockchain for IoT security and privacy: The case study of a smart home*. IEEE International Conference on Pervasive Computing.
7. Christidis, K., & Devetsikiotis, M. (2016). *Blockchains and smart contracts for the Internet of Things*. IEEE Access.
8. Huh, S., Cho, S., & Kim, S. (2017). *Managing IoT devices using blockchain platform*. IEEE International Conference on Advanced Communication Technology.
9. Sharma, P. K., Singh, S., Jeong, Y. S., & Park, J. H. (2018). *DistBlockNet: A distributed blockchain-based secure SDN architecture for IoT networks*. IEEE Communications Magazine.
10. Novo, O. (2018). *Blockchain meets IoT: An architecture for scalable access management in IoT*. IEEE Internet of Things Journal.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com