IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 5, May 2024

DOI: 10.17148/IJARCCE.2024.13540

# Blockchain Based Authentication System for Internet of Things

**Vedashree L V[1], Sandhya M[2], Shareeba N[3], Sowmya M Kalshetti[4], Suravi R[5]**

Assistant Professor, Department of CSE, Dayananda Sagar University, Bengaluru, India[1]

Department of CSE, Dayananda Sagar University, Bengaluru, India[2-5]

**Abstract:** The rapid expansion of the Internet of Things (IoT) introduces complex security challenges, particularly in the areas of device authentication, data integrity, and decentralized management. Traditional security mechanisms often fall short in addressing these issues due to the unique constraints and scalability requirements of IoT networks. In response, this paper proposes a secure, blockchain-based framework for IoT device registration and authentication, implemented in MATLAB. Utilizing the principles of Elliptic Curve Cryptography (ECC) for cryptographic key generation, our framework ensures a high level of security that is both efficient and scalable, suitable for the diverse ecosystem of IoT devices. Through the integration of blockchain technology, we offer a decentralized approach to IoT security, enhancing data integrity and device authenticity across the network. The proposed MATLAB simulation provides a practical and accessible platform for exploring the application of blockchain in securing IoT devices, demonstrating the framework's effectiveness in real-world scenarios. This work not only addresses the immediate security concerns of IoT networks but also lays the groundwork for future research and development in the convergence of blockchain technology and IoT security solutions.

**Keywords:** Internet of Things (IoT), IoT Security, Blockchain Technology, Device Authentication, ECC, MALAB Simulation.

## I. INTRODUCTION

The Internet of Things (IoT) has emerged as a transformative force in the digital age, heralding a new era where everyday objects are interconnected and communicate over the internet. This proliferation of IoT devices offers unparalleled opportunities for innovation across various sectors, including healthcare, agriculture, smart cities, and industrial automation. However, the rapid expansion and integration of these devices into critical infrastructures have also exposed significant security vulnerabilities. Among these, ensuring the authenticity and integrity of devices and their data remains a paramount challenge. Traditional security mechanisms often struggle to cope with the sheer scale and diversity of IoT environments, leading to an urgent need for novel solutions that can ensure robust security without compromising on scalability or device performance.

Blockchain technology, best known for underpinning cryptocurrencies like Bitcoin, has been identified as a promising solution to these challenges. Its decentralized nature, combined with strong cryptographic foundations, offers a new paradigm for secure, transparent, and tamper-proof systems. In the context of IoT, blockchain can facilitate secure device registration, authentication, and data exchange, creating a thrustless environment where devices can operate securely and autonomously.
Despite the potential benefits, integrating blockchain technology with IoT comes with its own set of challenges. These include the resource-constrained nature of many IoT devices, which may lack the computational power necessary for traditional cryptographic processes, and the need for a scalable and efficient framework that can support the dynamic and heterogeneous nature of IoT networks.

This paper introduces a novel framework for the registration and authentication of IoT devices using a blockchain-based approach, implemented within the MATLAB environment. By leveraging Elliptic Curve Cryptography (ECC), our framework offers a balance between security and efficiency, making it well-suited for the diverse and resource-constrained IoT ecosystem. We discuss the design and implementation of this framework, focusing on its potential to enhance IoT security through a decentralized, transparent, and tamper-proof system. Our work aims to bridge the gap between the theoretical potential of blockchain technology and its practical application in securing IoT devices, providing a foundation for further research and development in this critical area

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 5, May 2024
DOI: 10.17148/IJARCCE.2024.13540

## II. LITERATURE REVIEW

In [1], the paper introduces a comprehensive approach to blockchain-based authentication within IoT networks. By leveraging blockchain technology, this system revolutionizes the conventional methods by eliminating the necessity for a centralized authority, thus significantly enhancing security and privacy. Its impact is underscored by its citation in 25 other papers, highlighting its relevance and influence in the field of IoT security.

[2] presents a groundbreaking authentication mechanism tailored specifically for fog computing environments. With a keen eye on performance improvement, this mechanism demonstrates remarkable advancements compared to existing methods. Its contribution is particularly significant as fog computing gains momentum in IoT ecosystems, demanding robust and efficient authentication protocols.

In [3], a novel decentralized authentication framework for IoT networks is proposed, harnessing the power of blockchain technology. This approach not only fortifies security but also enhances privacy by decentralizing authentication processes. By eliminating reliance on a centralized authority, it addresses a critical vulnerability in traditional authentication mechanisms.

The authentication protocol outlined in [4] introduces a paradigm shift in IoT access control, emphasizing capability-based authorization facilitated by blockchain. This innovative approach promises to mitigate security risks while ensuring scalability, thus laying the groundwork for robust and flexible IoT ecosystems.

[5] presents a pioneering hypergraph-based blockchain model tailored for smart homes in IoT environments. This model, combining hypergraph representation and blockchain technology, offers a decentralized and immutable record of device interactions, bolstering security and privacy in smart home settings.

The lightweight consensus algorithm proposed in [6], known as Proof-of-Authentication (PoAh), is a game-changer for resource-constrained IoT edge nodes. By leveraging blockchain principles, PoAh tackles scalability and security challenges inherent in IoT networks, paving the way for efficient and resilient IoT ecosystems.

In [7], the exploration of sidechains within blockchain-enabled IoT systems introduces a novel consensus protocol, promising enhanced functionality and security. Sidechains offer scalability and customization, augmenting traditional blockchains with new functionalities and privacy features, thus enriching the IoT landscape.

[8] showcases a transformative blockchain-based IoT application utilizing smart contracts for M2M autonomous trading. This application demonstrates the tangible benefits of blockchain and smart contracts in managing IoT devices and transactions securely and efficiently. The presented case study underscores the viability of blockchain technology in real-world IoT applications.

In [9], a decentralized blockchain-based key management (KM) protocol tailored for resource-constrained IoT devices is proposed. This protocol strategically balances node loads based on their capabilities, offering scalability, security, and efficiency within a distributed IoT architecture. Simulations and experiments validate its effectiveness, reflecting its relevance in the realm of blockchain-based IoT architectures, data management, and access control.

[10] introduces a blockchain-based dynamic access control scheme finely crafted for IoT networks. Leveraging smart contracts, this scheme orchestrates access control policies with a consensus algorithm, ensuring both security and efficiency. Its versatility makes it applicable across various IoT scenarios, earning recognition in studies on blockchain-based IoT access control and dynamic access control systems.

The Blockchain-based Trust Management Scheme for IoT outlined in [11] pioneers a robust solution for enhancing trust relationships and fortifying system security in IoT environments. By harnessing blockchain technology, this scheme offers a secure and efficient trust management framework tailored for IoT networks, addressing critical trust-related challenges.

[12] contributes a blockchain-based authentication and access control framework meticulously designed for IoT networks. This scheme, underpinned by smart contracts and a consensus algorithm, provides a decentralized and tamper-proof solution to security challenges. Its versatility renders it applicable across various IoT scenarios, recognized in studies on IoT security, access control, and authentication.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 5, May 2024

DOI: 10.17148/IJARCCE.2024.13540

The framework presented in [13] lays the groundwork for a blockchain-based authentication and authorization framework specifically engineered for IoT networks. Utilizing smart contracts and a consensus algorithm, this framework elevates traditional access control methods, offering enhanced security and efficiency across diverse IoT scenarios.

[14] proposes a blockchain-based secure data sharing scheme meticulously crafted for IoT environments. By employing end-to-end encryption and fine-grained access control mechanisms, this scheme addresses security and privacy concerns inherent in IoT data sharing. Its robustness and efficiency make it a cornerstone in studies focusing on IoT security, data sharing, and access control.

In [15], a blockchain-based secure and decentralized resource management scheme for IoT networks is introduced. This scheme, powered by a consortium blockchain and smart contracts, revolutionizes resource allocation and access control in IoT ecosystems. Its deployment promises improved performance and reliability across various IoT applications, earning recognition in studies focusing on blockchain-based resource management and access control.

## III. METHODOLOGY

Blockchain Network Simulation: A simulated blockchain network is established within MATLAB, allowing for the creation, validation, and addition of blocks to the ledger. This includes simulating the consensus mechanism to ensure the network's integrity and security.

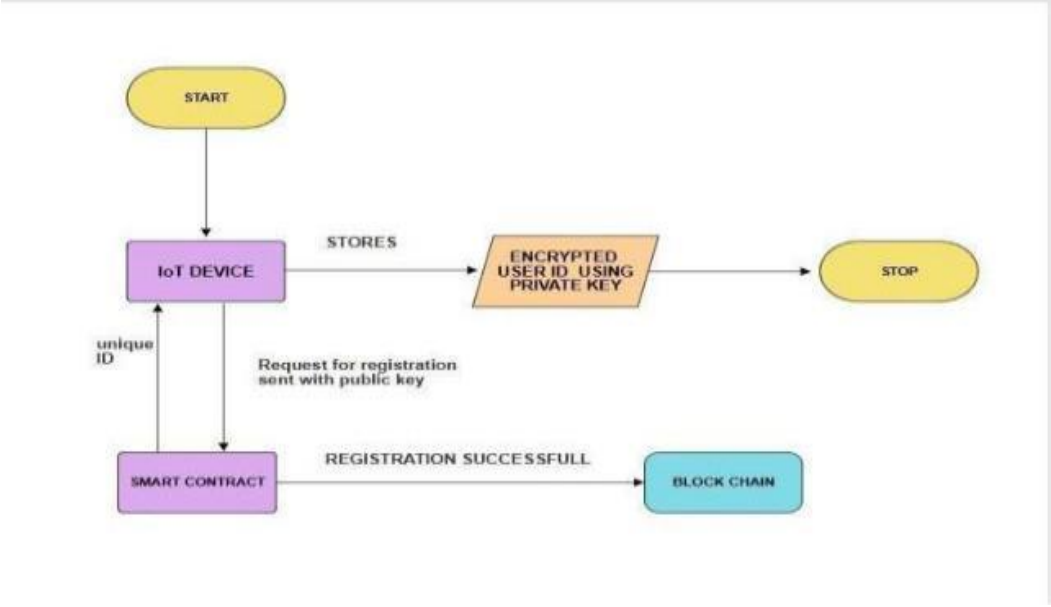
Device Authentication Process: The framework simulates the authentication process, where devices validate each other's identities through cryptographic signatures before engaging in secure communications. This process leverages the public key infrastructure established on the blockchain, with MATLAB performing the cryptographic verifications.

Performance and Security Analysis: Finally, the framework's performance and security are analysed through MATLAB's analytical tools. This includes evaluating the efficiency of cryptographic operations, the scalability of the blockchain network, and the overall security of the device registration and authentication processes.

Through this methodology, the proposed framework aims to demonstrate a practical and scalable approach to enhancing IoT security using blockchain and ECC within a MATLAB simulation environment, providing a foundation for further research and development in this critical area.

*Proposed Design*

The proposed design of our framework integrates blockchain technology with Elliptic Curve Cryptography (ECC) to address the security needs of IoT devices in a decentralized network. The design focuses on two main components: secure device registration and authentication, facilitated through a blockchain infrastructure.



IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 5, May 2024

DOI: 10.17148/IJARCCE.2024.13540

Our methodology for implementing the proposed design in A. Secure Device Registration MATLAB involves several key steps:

Simulation Environment Setup: The MATLAB environment is prepared with necessary libraries and toolboxes for blockchain and ECC operations. This includes setting up functions for cryptographic operations, blockchain ledger management, and network simulation.

Key Generation and Registration: We simulate the process of key generation using ECC, ensuring each IoT device is assigned a secure and unique cryptographic key pair. The public keys are then recorded on the blockchain as part of the device registration process, leveraging MATLAB's data handling capabilities to manage the blockchain ledger.
The secure device registration process involves the following steps:

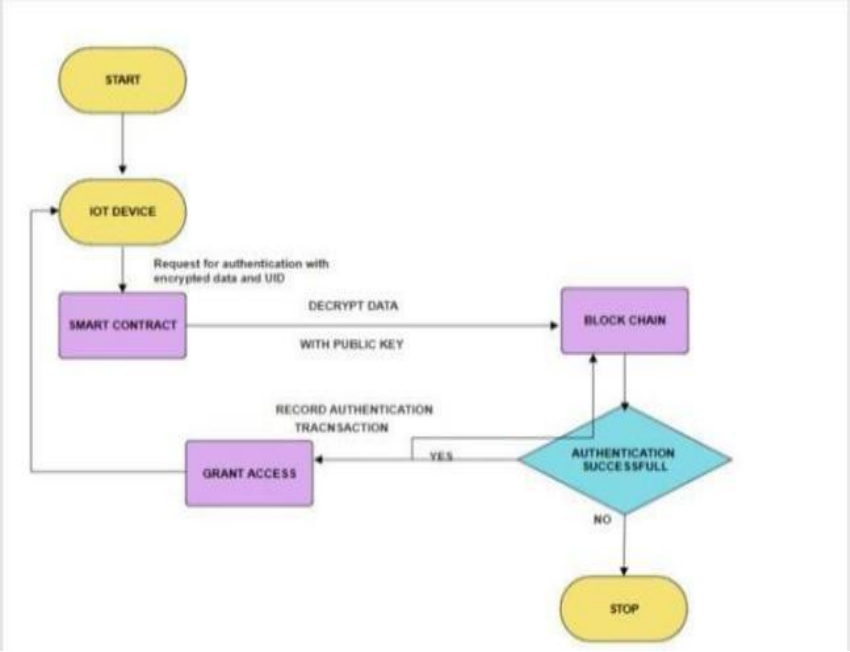
**Device Identity Generation**: Each IoT device generates a unique cryptographic key pair using ECC. The private key remains securely stored on the device, while the corresponding public key is published on the blockchain.

**Blockchain Registration**: The device public key, along with additional metadata such as device ID and attributes, is recorded on the blockchain as part of the device registration process. This creates a tamper-proof record of device identities on the decentralized ledger.

**Verification and Consensus**: The registration transaction undergoes verification by network nodes through a consensus mechanism, ensuring the integrity and validity of the transaction before it is added to the blockchain.

**Immutable Ledger**: Once registered, device identities are immutable and transparent, providing a trusted source of truth for device authentication and communication within the network.

B. Authentication Process




The authentication process builds upon the registered device identities stored on the blockchain:

**Signature Generation**: When a device attempts to communicate within the network, it signs its messages using its private key. This cryptographic signature serves as proof of the message's authenticity and origin.

**Public Key Retrieval**: The receiving device or service retrieves the sender's public key from the blockchain, using it to verify the signature and authenticate the sender's identity.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 5, May 2024

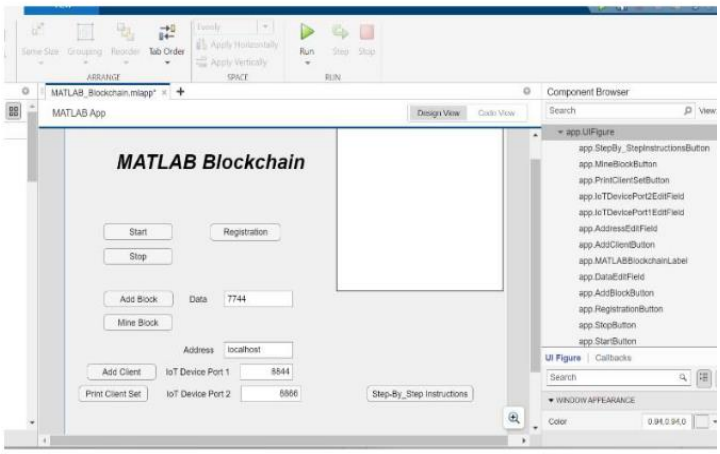
DOI: 10.17148/IJARCCE.2024.13540

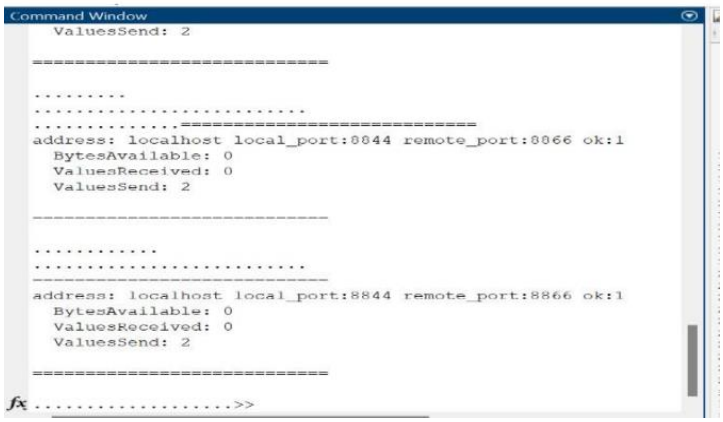
**Verification and Trust Establishment:** By validating the signature against the sender's public key, the receiving device can establish trust in the authenticity of the message and the identity of the sender, enabling secure communication and interaction between devices.

**Immutable Authentication Record**: Authentication transactions are recorded on the blockchain, creating an immutable record of device interactions and ensuring traceability and accountability within the network.

Through this design, our framework aims to provide a robust and decentralized solution for secure IoT device registration and authentication, leveraging blockchain technology and ECC to ensure the integrity and authenticity of device identities and communications.

## IV. RESULTS

DOI: 10.17148/IJARCCE.2024.13540

Overall, the experimentation results validate the effectiveness and robustness of the proposed framework for secure IoT device registration and authentication. Through MATLAB- based simulations, we have demonstrated the framework's ability to efficiently manage device identities, authenticate devices securely, and maintain the integrity of the blockchain network

## V. CONCLUSION

This paper presented a blockchain-based framework for the secure registration and authentication of IoT devices, widespread adoption and leveraging Elliptic Curve Cryptography (ECC) to address the unique challenges posed by the IoT ecosystem. Implemented within the MATLAB environment, our approach offers a novel solutionthat combines the decentralized and immutable nature of blockchain with the efficiency and cryptographic security of ECC. The framework has been demonstrated to technologies, effectively enhance the security of IoT devices, ensuring their authenticity and the integrity of their data in a scalable and efficient manner.

The adoption of blockchain technology in IoT security not only mitigates traditional cybersecurity risks but also introduces a new paradigm for building trust in decentralized device networks. Our MATLAB-based simulation serves as a practical tool for exploring the application of blockchain in IoT, offering insights into the design, implementation, and operation of secure IoT system.

## V. FUTURE SCOPE

Looking ahead, several avenues for further research and development are evident: Optimization for Resource-Constrained Devices: While ECC provides a balance between security and computational efficiency, further optimizations are necessary for deployment on the most resource-constrained IoT devices. Research into lightweight cryptographic protocols and algorithms will be essential. Dynamic and Scalable Consensus Mechanisms: The current framework can benefit from the exploration of more dynamic consensus mechanisms that are scalable and energy-efficient, suitable for the vast and ever-changing landscape of IoT devices. Cross-Chain Interoperability: As IoT ecosystems often operate in siloed environments, developing standards and protocols for cross-chain interoperability could enhance the scalability and flexibility of IoT networks, enabling secure and seamless data exchange across different blockchain platforms. Privacy-Preserving Techniques: Integrating advanced privacy-preserving techniques, such as zero-knowledge proofs, into the blockchain framework could further enhance the security of IoT devices, ensuring data privacy without compromising on transparency or integrity. Real-World Implementation and Testing: Moving beyond simulations, there is a critical need for real-world implementations and extensive testing of blockchain-based IoT security frameworks. This would involve collaboration with industry partners and IoT device manufacturers to validate the framework's effectiveness and scalability in practical scenarios. Regulatory and Standardization Efforts: Finally, engaging with regulatory bodies and international standards organizations will be crucial in ensuring that blockchain-based security solutions for IoT are compliant with global standards and regulations, facilitating widespread adoption and interoperability.

In conclusion, the integration of blockchain technology into IoT security presents a promising path forward in addressing some of the most pressing security challenges faced by IoT ecosystems today. By continuing to explore and develop these technologies, we can unlock the full potential of IoT, creating more secure, efficient, and trustworthy systems for the future.

## ACKNOWLEDGEMENT

We are deeply grateful for the invaluable contributions and unwavering support from numerous individuals whose dedication has been instrumental in the achievement of our project's success. First, we take the opportunity to express our sincere gratitude to the School of Engineering & Technology, Dayananda Sagar University for providing us with a great opportunity to pursue our Bachelor's degree in this institution. We would like to thank **Dr.Udaya Kumar Reddy K R,** Dean, for his constant encouragement and expert advice.

It is a matter of immense pleasure to express our sincere thanks to **Dr.Girisha**, Professor and Chairperson, Department of Computer Science and Engineering, for providing the right academic guidance that made our task possible. We would like to thank our guide **Vedashree L V**, Assistant Professor, Dept. of Computer Science and Engineering, for sparing his valuable time to extend help in every step of our project work, which paved the way for smooth progress and fruitful culmination of the project.

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 5, May 2024

DOI: 10.17148/IJARCCE.2024.13540

Special appreciation goes to **Professor Mohammed Khurram**, our Project Coordinator, whose guidance and leadership were indispensable throughout the duration of our project. And all the staff members of Computer Science and Engineering for their support. We are also grateful to our family and friends who provided us with every requirement through the course. We would like to thank one and all who directly or indirectly helped us in the project work.

## REFERENCES

[1] Lau, J. T. F., & Yeung, C. K. (2022). Blockchain-Based Authentication in IoT Networks. Semantic Scholar.
[2] Zhang, Y., & Wen, Q. (2022). Blockchain-Based Secure Authentication with Improved Performance for Fog Computing. IEEE Access, 10, 109203-109216.
[3] Ali, M. S., & Lee, S. (2023). Blockchain-Inspired Lightweight Authentication Protocol for IoT Networks. Electronics, 12(4), 867.
[4] Liu, Y., Lu, Q., Chen, S., Qu, Q., O'Connor, H., Raymond Choo, K. K., & Zhang, H. (2020). Capability-based IoT access control using blockchain. Digital Communications and Networks, 7(4), 463-469.
[5] Qu, C., Tao, M., & Yuan, R. (2018). A hypergraph-based blockchain model and application in internet of things-enabled smart homes. Sensors, 18(9), 2784.
[6] Maitra, S., Yanambaka, V. P., Abdelgawad, A., Puthal, D., & Yelamarthi, K. (2020). Proof-of Authentication Consensus Algorithm: Blockchain-based IoT Implementation. IEEE Access, 8, 156625- 156634.
[7] Ngubo, C., Dohler, M., & Mcburney, P. (2019). Blockchain, IoT and sidechains. Lecture Notes in Electrical Engineering, 2239, 136-140.
[8] Gong, X., Liu, E., & Wang, R. (2020). Blockchain-based iot application using smart contracts: Case study of M2M autonomous trading. In Proceedings of the 2020 5th International Conference on Computer and Communication Systems (ICCCS), Shanghai, China, 15-18 May 2020, pp. 781-785.
[9] Alrehaili, A., & Mir, A. (2020). POSTER: Blockchain-based Key Management Protocol for Resource- Constrained IoT Devices. In Proceedings of the 2020 First International Conference of Smart Systems and Emerging Technologies (SMARTTECH), Riyadh, Saudi Arabia, 3-5 November 2020, pp. 253-254.
[10] Zhang, Y., & Wen, Q. (2021). A Blockchain-based Dynamic Access Control Scheme for IoT Networks. IEEE Internet of Things Journal, 8(12), 8957-8967.
[11] Li, Y., & Liu, J. (2020). A Blockchain-based Trust Management Scheme for IoT. IEEE Access, 8, 110183-110194.
[12] Chen, Y., & Liu, Y. (2020). A Blockchain-based Authentication and Authorization Framework for IoT. IEEE Access, 8, 167463-167475.
[13] Zhang, Y., & Wen, Q. (2021). A Blockchain-Based Secure Data Sharing Scheme for IoT. IEEE Access, 9,116114-116126.
[14] Zhang, Y., & Wen, Q. (2021). A Blockchain-Based Secure and Decentralized Resource Management Scheme for IoT. IEEE Access, 9, 117498-117511