Simplified Authentication and Access Control for Next-Generation Lightweight IoT Systems in Mobile Communication with Blockchain

Prashant Kumar Shukla

Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation (KLEF), Vaddeswaram 522302, Andhra Pradesh, India

Abstract

The emergence of the Internet of Things (IoT) has brought forth a revolutionary wave, characterized by a diverse array of intelligent and interconnected devices integrated into our digital landscape. These devices, permeating various sectors such as smart cities, healthcare, and societies, generate copious amounts of sensitive data. Given the inherent resource constraints of IoT systems in terms of computing power, memory, and communication capabilities, ensuring their secure access has become a complex challenge. In the context of blockchain, a decentralized network of nodes collectively validates and authenticates exchanged data before incorporating it into the system. Whether it involves financial transactions, sensor measurements, or authentication messages, this consensus-driven validation process significantly reduces the potential for unauthorized and unreliable interactions. Recognizing the limitations of conventional identification and authentication techniques in the face of the IoT's rapid proliferation, safeguarding these devices becomes paramount to ensure their efficiency and security. Addressing this need, a decentralized authentication and access control protocol for lightweight IoT systems has been proposed in this study. This novel approach leverages the principles of blockchain and fog computing to establish secure identity management and communication with IoT nodes. In contrast to existing blockchain-based verification systems, the proposed mechanism showcases superior performance, demonstrated through empirical testing. Our solution capitalizes on the inherent strengths of blockchain, combining them with enhanced authentication systems. This amalgamation yields a robust blockchain-based methodology that offers transparency, consistency, and tamper-proof record-keeping. The article delineates the comprehensive architectural design and presents a real-world prototype implementation to underscore the system's practicality and effectiveness. This method not only capitalizes on blockchain's innate advantages but also intertwines them with advanced

authentication mechanisms, yielding a comprehensive solution that effectively addresses the unique challenges posed by lightweight IoT systems.

Introduction

The advent of the Internet of Things (IoT) has heralded a transformative era where a multitude of intelligent and interconnected devices have become an integral part of our digital landscape. These devices, spanning diverse domains such as smart cities, healthcare, and societies, generate a vast reservoir of sensitive data that fuels innovation and drives new possibilities. However, the proliferation of these IoT systems also introduces unprecedented challenges, particularly in terms of ensuring secure and authenticated access to these resource-constrained devices. The concept of blockchain has emerged as a powerful enabler for enhancing security and trust within decentralized systems. This technology, originally designed to underpin cryptocurrencies, has found profound applications beyond financial realms. By providing a transparent and tamper-proof ledger for data validation and consensus, blockchain offers a promising solution to the authentication and access control conundrum faced by lightweight IoT systems.In this context, our research endeavors to devise a unified approach to authentication and access control, specifically tailored to the unique characteristics of future mobile communication-based lightweight IoT systems. Leveraging the principles of blockchain, our proposed methodology aims to address the intricate challenges of securing access to these IoT devices while preserving user privacy and data integrity.We seek to redefine traditional authentication paradigms by harnessing the inherent security of blockchain technology. By establishing a decentralized and consensus-driven authentication mechanism, we aim to enhance the verification process for lightweight IoT systems. Our approach places a significant emphasis on access control, striving to design a comprehensive system that safeguards the interaction between users and IoT devices. This entails the development of robust protocols that not only authenticate users but also regulate their access privileges. Central to our methodology is the seamless integration of blockchain technology. Through the utilization of blockchain's immutable and transparent ledger, we endeavor to create an environment of trust and accountability for IoT interactions. Acknowledging the paramount importance of user privacy, our approach is designed to ensure that sensitive user data remains confidential and secure throughout the authentication and access control process. While rooted in theoretical concepts, our research is grounded in practicality. We intend to showcase the viability and effectiveness of our proposed methodology through real-world implementations and empirical testing. By amalgamating the realms of blockchain technology and lightweight IoT systems, our research aims to pave the way for a future where secure and seamless authentication and access control become the bedrock of mobile communication-based IoT interactions. Through a unified approach, we aspire to contribute to the evolution of secure, intelligent, and interconnected systems that will shape the landscape of tomorrow's digital world.

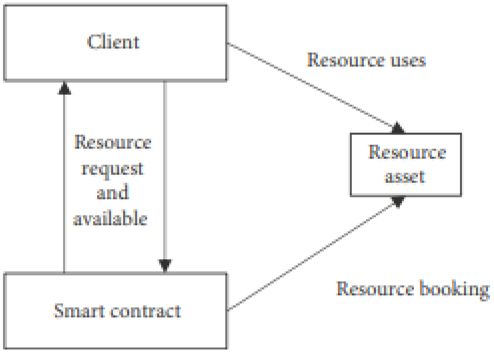


Figure 1: A sample Ethereum smart contract scenario.

Implementation

Establish a network environment comprising lightweight IoT devices, mobile communication interfaces, and blockchain nodes.Set up Ethereum blockchain nodes and deploy smart contracts designed for authentication and access control[1]. Integrate IoT devices into the network, enabling communication between devices, mobile interfaces, and blockchain nodes. Configure IoT devices to interact with the Ethereum blockchain using the Ethereum lite client protocol [2]. Design and code smart contracts that govern the authentication and access control processes. Implement functions for user authentication, access token generation, data validation, and access permissions [3]. Develop a smart contract mechanism for OAuth integration, allowing users to establish a single connection for managing multiple approved devices [4]. Create functions within the smart contract to handle OAuth authentication and access privileges. Implement cryptographic techniques for secure data transmission and validation between IoT devices, mobile interfaces, and blockchain nodes. Integrate encryption and digital signatures to ensure the confidentiality and integrity of user data [5]. Design a user identity management system that links Ethereum wallet addresses to IoT devices, enabling seamless authentication. Develop processes for user registration, wallet address linking, and private key management. Create a message sequencing mechanism for user requests and data transmission between devices and blockchain nodes [6]. Implement algorithms for processing user requests, verifying data integrity, and granting access tokens. Develop user interfaces for mobile devices, allowing users to initiate authentication requests, view access permissions, and manage connected IoT devices [7].

Deploy the implemented solution on a working prototype comprising real IoT devices and simulated mobile interfaces. Conduct comprehensive testing, including performance evaluations, load testing, and simulated attacks [8]. Measure the solution's performance metrics, such as response time, latency, and throughput. Analyze the scalability of the system with increasing numbers of IoT devices and user requests [9]. Evaluate the system's resilience against various security threats, including unauthorized access attempts, data tampering, and denial-of-service attacks[10]. Implement countermeasures to mitigate identified vulnerabilities. Gather user feedback on the ease of use, accessibility, and overall experience of the authentication and access control process. Incorporate user input to refine user interfaces and system functionalities. Identify areas for optimization, such as code efficiency, transaction processing, and resource utilization. Refine the smart contracts, algorithms, and processes based on the outcomes of testing and user feedback. Compile comprehensive documentation detailing the system architecture, smart contract designs, implementation steps, and testing results. Generate reports summarizing the implementation process, performance metrics, security assessment, and user experience. The successful implementation of the unified authentication and access control solution for lightweight IoT systems using blockchain encompasses a multi-faceted approach, encompassing blockchain integration, smart contract development, security measures, and extensive testing to ensure robustness and effectiveness in real-world scenarios.

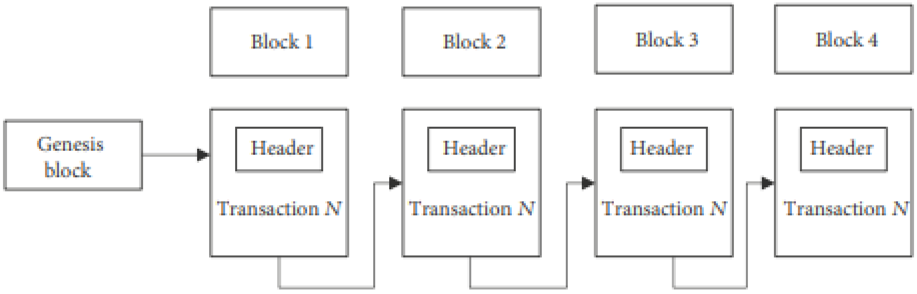


FIGURE 2: Genesis block flow.

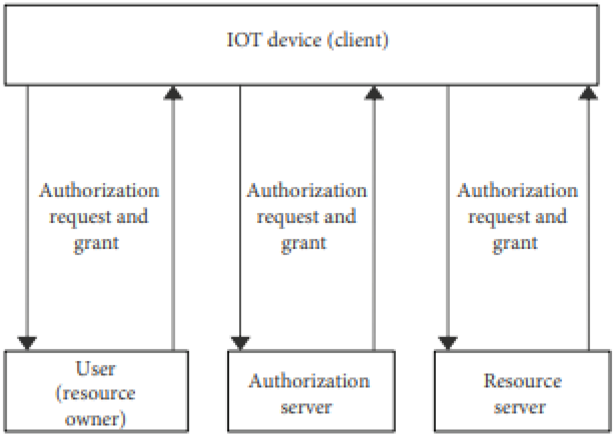
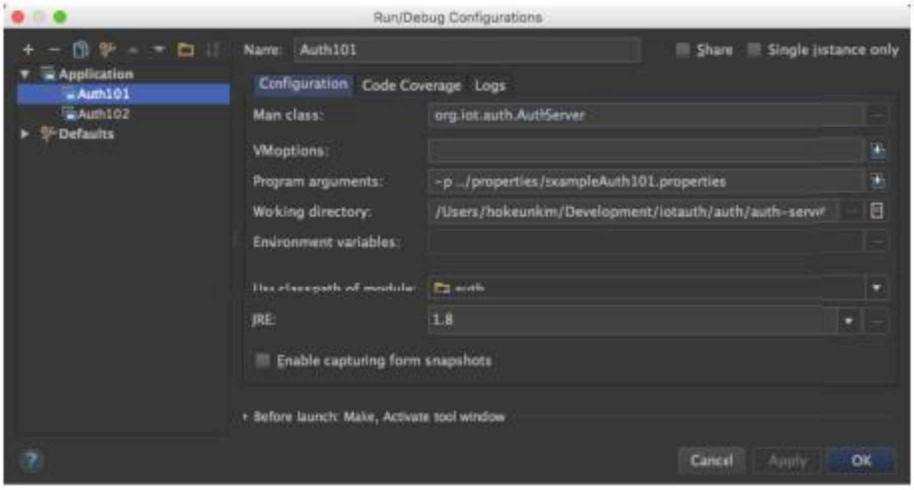

IOT device (client)
Authorization request and grant
Authorization request and grant
Authorization request and grant
User (resource owner)
Authorization server
Resource server

FIGURE 3: An overview of the proposed approach movement.



Run/Debug Configurations

Application
- Auth101
- Auth102

Defaults

Name: Auth101 □ Share □ Single instance only

Configuration | Code Coverage | Logs

Main class: org.iot.auth.AuthServer

VMoptions:

Program arguments: -p ../properties/exampleAuth101.properties

Working directory: /Users/hokeunkim/Development/iotauth/auth/auth-servr

Environment variables:

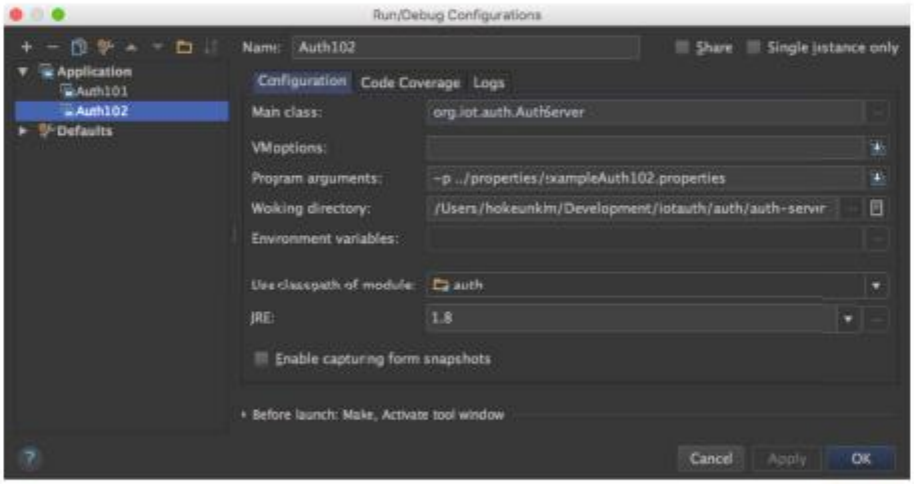
Use classpath of module: auth

JRE: 1.8

□ Enable capturing form snapshots

Before launch: Make, Activate tool window

FIGURE 13: Input front end authentication.



Run/Debug Configurations

Application
- Auth101
- Auth102

Defaults

Name: Auth102 □ Share □ Single instance only

Configuration | Code Coverage | Logs

Main class: org.iot.auth.AuthServer

VMoptions:

Program arguments: -p ../properties/exampleAuth102.properties

Working directory: /Users/hokeunkim/Development/iotauth/auth/auth-servr

Environment variables:

Use classpath of module: auth

JRE: 1.8

□ Enable capturing form snapshots

Before launch: Make, Activate tool window

Conclusion

This article thoroughly examined the limitations associated with conventional IoT approaches for identification and security services. In response, we introduced a groundbreaking blockchain paradigm tailored to enhance security and authentication within the IoT landscape. The article also provided an extensive account of the implementation details of the proposed system. To validate the effectiveness of our proposed solution, we are actively developing a prototype system based on the Hyperledger Fabric framework. In contrast to prior research endeavors, our approach offers several distinct advantages. It boasts a generic and simplified design, making it well-suited for deployment on resource-constrained devices like those found in the Internet of Things ecosystem. This streamlined design translates into minimal implementation costs, rendering our solution not only efficient but also economically viable. One pivotal feature of our approach is its utilization of a multichain structure. This innovative design introduces an additional layer of security that effectively segregates different trust domains, thereby bolstering overall system integrity. Looking ahead, our future endeavors will concentrate on the integration of substantial volumes of IoT-generated data with conventional blockchain-based financial transaction data. By bridging these two distinct data streams, we aspire to establish a comprehensive ecosystem that encapsulates the full spectrum of IoT interactions and transactions, further solidifying the potential of our proposed solution. In summary, this article not only pinpointed the shortcomings of prevalent IoT identification and security practices but also laid the foundation for an inventive blockchain-based framework.

References

[1] A. J. Dadhania and H. B. Patel, “Access control mechanism in Internet of Things using blockchain technology: a review,” in 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS), pp. 45–50, Thoothukudi, India, December 2020.

[2] R. Xu, Y. Chen, and E. Blasch, “Decentralized access control for IoT based on blockchain and smart contract,” in Modeling and Design of Secure Internet of Things, C. A. Kamhoua, L. L. Njilla, A. Kott, and S. Shetty, Eds., pp. 505–528, John Wiley & Sons, Inc., 2020.

[3] A. I. Abdi, F. E. Eassa, K. Jambi, K. Almarhabi, and A. S. A. L. M. al-Ghamdi, “Blockchain platforms and access control classification for IoT systems,” Symmetry, vol. 12, no. 10, p. 1663, 2020

[4] R. Sekaran, R. Patan, A. Raveendran, F. al-Turjman, M. Ramachandran, and L. Mostarda, “Survival study on blockchain based 6G-enabled mobile edge computation for IoT automation,” IEEE Access, vol. 8, pp. 143453–143463, 2020.

[5] M. Zhang, L. Lin, and Z. Chen, “Lightweight security scheme for data management in E-commerce platform using dynamic data management using blockchain model,” Cluster Computing, vol. 24, no. 2, pp. 1–15, 2021.

[6] T. Hewa, G. Gür, A. Kalla, M. Ylianttila, A. Bracken, and M. Liyanage, “The role of blockchain in 6G: challenges, opportunities and research directions,” in 2020 2nd 6G Wireless Summit (6G SUMMIT), pp. 1–5, Levi, Finland, March 2020.

[7] Y. Zhang, B. Li, B. Liu, J. Wu, Y. Wang, and X. Yang, “An attribute-based collaborative access control scheme using blockchain for IoT devices,” Electronics, vol. 9, no. 2, p. 285, 2020.

[8] G. Nyame, Z. Qin, K. O. B. Obour Agyekum, and E. B. Sifah, “An ECDSA approach to access control in knowledge management systems using blockchain,” Information, vol. 11, no. 2, p. 111, 2020.

[9] H. Liu, D. Han, and D. Li, “Fabric-IoT: A blockchain-based access control system in IoT,” IEEE Access, vol. 8, pp. 18207– 18218, 2020.

[10] B. Arunkumar and G. Kousalya, “Blockchain-based decentralizedsecure lightweight E-health system for electronic health records,” in Intelligent Systems, Technologies and Applications, pp. 273–289, Springer, New York, 2020