Al-Ahgaff University Journal of Computer Science and Mathematics
مجلة جامعة الأحقاف لعلوم الحاسوب والرياضيات

Vol. 3, December 2025, pp. 27~33
ISSN(Print):3005-9860, ISSN(Online):3005-9879

Performance Evaluation of Authentication Method in Public and Private Blockchains

Asma Abdulrahman Bin Al Sheikh Abubaker
Department of Information Technology, Faculty of Computer Science and Engineering, Al Ahgaff University, Hadhramaut, Al-Mukalla, Yemen
asma.shekh@ahgaff.edu
Makarem Mohammed Bamatraf
Department of Computer Engineering, Faculty of Engineering, Hadhramaut University, Hadhramaut, Al-Mukalla, Yemen
m.bamatraf@hu.edu.ye
Khaled Ahmed Baqais
[3]Department of Computer Science and Engineering, Faculty of Engineering, University of Aden, Aden, Yemen
k_abood@hotmail.com

Article Info

Article history:

Received March 27, 2025
Accepted April 03, 2025

Keywords:

Internet of Things
Authentication
Private and Public Blockchains

ABSTRACT

The Internet of Things (IoT) is a network of connected devices designed to perform specific tasks. Many IoT devices are lightweight, meaning they have limited storage and processing power. Because of these limitations, centralized authentication systems are often used to manage security and access control. Unfortunately, such systems suffer from limitations like single points of failure, scalability issues, cost constraints, and bottlenecks. To overcome these limitations, decentralized systems involving public and private blockchains have emerged. This research evaluates the performance of an authentication system on private (Ganache) and public (Rinkeby and Ropsten) blockchains. Ganache, is an Ethereum emulation tool that facilitates testing in private blockchains, while Rinkeby and Ropsten represent public blockchains. The evaluation metrics employed in this research are execution time, CPU usage, and memory utilization, which play a significant role in group membership association requests and data exchanges. The findings indicate that private blockchains exhibit lower time and CPU usage due to their relatively smaller number of users, whereas public blockchains demonstrate lower memory consumption in comparison.

الخلاصة

إنترنت الأشياء هي مجموعة من الأجهزة المترابطة التي تهدف إلى تحقيق مهام محددة. تمتلك أجهزة إنترنت الأشياء الخفيفة قدرة تخزين ومعالجة محدودة، مما يؤدي إلى اعتماد أنظمة التوثيق المركزية. ومع ذلك، فإن هذه الأنظمة تعاني من بعض القيود مثل نقاط الفشل الواحدة، ومشاكل في التوسع، والقيود المالية، والاختناقات. للتغلب على هذه القيود، ظهرت الأنظمة اللامركزية التي تشمل البلوكتشين العام والخاص. تقوم هذه الدراسة بتقييم أداء نظام التوثيق على شبكات البلوكتشين الخاصة جاناش (Ganache) والعامة رينكبي وروبستن (Rinkeby and Ropsten). جاناش هي أداة محاكاة إيثريوم (Ethereum) تسهل الاختبار في شبكات البلوكتشين الخاصة، بينما تمثل رينكبي وروبستن شبكات البلوكتشين العامة. تتضمن مقاييس التقييم المستخدمة في هذه الدراسة وقت التنفيذ، واستخدام وحدة المعالجة المركزية، واستهلاك الذاكرة، والتي تلعب دورًا كبيرًا في طلبات ارتباط العضوية الجماعية وتبادل البيانات. تشير النتائج إلى أن شبكات البلوكتشين الخاصة تبين وقتًا واستخدامًا أقل لوحدة المعالجة المركزية بسبب عدد المستخدمين الأصغر نسبيًا، في حين تظهر شبكات البلوكتشين العامة استهلاكًا أقل للذاكرة.

1. INTRODUCTION

Internet of Things (IoT) is a network sensors and devices that are able to share and capture data with each other and connect together over a network [1]. One of the significant challenges preventing the widespread adoption of IoT technologies is the concerns relating to privacy and security. The evolution of IoT devices creates a new model of facilities, but at the same time it makes some security weaknesses [2]. In the time before the invention of blockchain technology, a majority of online activities were carried out through centralized servers to insure data integrity and confidentiality.

Blockchain is a decentralized database of transactions. Every user on the blockchain network maintains an authentic copy of the database. So, it is hard to add a malicious transaction because it must be

verified by all network users. A consensus mechanism ensures that all participants in a blockchain network agree on its contents. The most commonly used methods include Proof of Work (PoW), Proof of Stake (PoS), and Proof of Authority (PoA). They differ in their work style [3]. Proof of work is used by most cryptocurrency networks like Bitcoin and Litecoin. Users must prove the work to add new blocks to the blockchain. Although the mining process needs high energy consumption and processing time, proof of stake is another common one with a lower cost and lower energy consumption compared to the proof of work [4], where it depends on financial stake. Proof of work and proof of stake allow for open participation, allowing anyone to join and participate in their respective networks. However, this open participation does not exist in the proof of authority where it restricts the role of validator to trusted entities based on their trustworthiness [5].

There are three types of blockchains public, private, and federated. The public blockchains is open for all types of users to share in the network. It can be secured using crypto-economics, which is a combination of cryptographic verification and economic incentives using consensus mechanisms such as proof of work or proof of stake. Ethereum and Bitcoin, are examples of this type [6]. In private blockchains only a specific set of users has the authority to join the blockchain network. Users of this type get their permission from the organization before joining to the blockchain network. Ripple and Everledger are examples of this type [7]. The private blockchain is easier than public blockchain because the number of users is less compared to the public blockchain. Also, it offers better privacy as only users identified within the blockchain network can read the transactions [8]. The federated blockchain is a partially private blockchain. It runs under the authority of a set of organizations. So, it is a private blockchain for a specific set of organizations and it is faster and offer better scalability and privacy than a public blockchain [9].

Securing network communications is essential requirement, and one of the key measures to achieve this requirement is by properly identify devices through authentication and authorization. However, with the rapid expansion of IoT devices worldwide, traditional centralized authentication methods are becoming less effective. These methods create a single point of failure and bottlenecks, which slow down the authentication process. Studies [7, 11-13] have shown that using a single centralized server for authentication can lead to system vulnerabilities due to this single point of failure. On the other hand, there exists a decentralized authentication approach in the form of blockchain, which can be classified into two types: public blockchain and private blockchain. In public blockchain each transaction takes 14 seconds to be validated. Therefore, public blockchain is not adapted to real-time applications where the long validation time is not appropriate [14]. The private blockchain uses less power and time and is more secure than the public blockchain due to the network's authority where users being chosen [15, 16].

This research aims to evaluate the efficacy of an authentication method in public and private blockchains, specifically Rinkeby, Ropsten, and Ganache. The study investigates and compare the performance differences among these blockchains in terms of time, CPU usage, and memory consumption. This study is an extension of our previous work [24], where we primarily investigated the performance of the authentication method in public blockchains using the mentioned metrics. To the best of our knowledge, no prior studies have evaluated the performance of the public and private blockchains in context of authentication process of IoTs

2. RELATED WORK

Explaining research chronological, including research design, research procedure (in the form of Authentication is the process of verifying the identity of an individual by comparing his/her credentials against stored data in a database in an authentication server [17]. This process can be conducted without utilizing blockchain technology or can leverage the capabilities of a blockchain for authentication purposes. This section presents a literature review of previous studies conducted on the topic of authentication methods. The review is organized into two parts: authentication methods that do not utilize blockchain technology, and authentication methods that leverage blockchains.

2.1. AUTHENTICATION METHODS WITHOUT BLOCKCHAIN

Satapathy et al. [17] proposed an Internet of Things authentication method that runs on a standard Wi-Fi network and uses elliptic curve cryptography (ECC) to authenticate Internet of Things devices. The method assigns the Wi-Fi gateway to initialize system configuration and to authenticate Internet of Things devices. User's access in the method is controlled by mobile device using an Android application. However, the proposed method has the issue of using a public key, which is not effective in storage and computation for Internet of Things constrained devices. Zhang et al. [7] proposed a proximity-based authentication method between the smart phone and the Internet of Things devices. The RSS signal variation and RSS-trace are used to match the variations with the real ones. The issue with the proximity-based authentication is that the authentication data is stored on a centralized local server, resulting in a single point of failure attack. Moreover, the system requires the devices to be close enough if they want to authenticate each other.

2.2. AUTHENTICATION METHODS UTILIZING BLOCKCHAIN

Dorri et al. [18] proposed a lightweight, private, secure blockchain. The method uses three interrelated blockchains: private blockchain for each use case, shared private blockchain and public blockchain. It resolves the identification issue, but it has several drawbacks. Firstly, each operation produces at least eight messages, which reduces the speed of the entire system. Secondly, private blockchains are centralized, which conflicts to their principle because it limits their availability. Griggs et al. [19] proposed utilizing private blockchain to simplify secure analysis and manage a medical sensor. The system resolves many security weaknesses related to distant patient monitoring and mechanizes the transfer of announcements to all involved parties in health insurance portability and accountability. The proposed system has some drawbacks when more smart devices broadcast their transactions to several nodes waiting to confirm the next block. This is not appropriate with the healthcare system because it deals with real-time data. Fayad et al. in [20]. Proposed a new authentication and authorization method for IoT gateways, using both private and public blockchains. This method aims to overcome the bottleneck problem of centralized methods caused by the rapid increase in IoT devices while maitains scalable security. Private blockchain saves money over public blockchain because it does not require transaction fees. Focusing on the scalability issues in blockchain-based IoT, authors in [25] introduced a lightweight, trust-aware authentication mechanism designed to minimize storage overhead. By combining data storage optimization with homomorphic encryption for secure cloud uploading, the framework effectively balances high-performance requirements with robust security for resource-constrained devices. To eliminate the expense of digital certificates in massive IoT networks, authors in [26] introduced a blockchain-based security scheme that functions as a decentralized alternative to Certificate Authorities. This approach prioritizes confidentiality and authorization through a low-cost, methodological framework capable of managing the registration and authentication of widely distributed smart devices. Recognizing the limitations of Proof of Work in resource-constrained environments, authors in [27] proposed a lightweight blockchain system utilizing a simplified Proof of Stake (PoS) consensus and hierarchical topology. By employing efficient cryptography (ECDSA and AES-128), the framework achieved a 54% reduction in energy consumption and maintained sub-30ms latency, offering a viable alternative to traditional centralized or heavy-duty blockchain solutions. Hammi et al. [14] proposed bubbles of trust authentication method. It was executed using a public blockchain and creates secured bubbles (groups) where devices can communicate only inside each group and can't communicate outside. The method has some issues. Firstly, it is not suitable for real-time applications because it is time consuming method due to the use of public blockchain and the transaction in Ethereum is confirmed every 14 seconds (consensus needed time). Thus, transactions (messages) sent by devices will be authenticated only after this time. Secondly, there are various situations on the Internet of Things where this time is not accepted. However, the problem will be solved if a private blockchain is used.

3. RESEARCH METHODOLOGY

This section outlines the research methodology used in this study. The main objective is to evaluate the performance of an authentication method in secure groups within an IoT environment, where each group represents a specific application. The concept of the authentication method and secure groups is inspired by the work in [14], where an IoT group is referred to as a "bubble." In this approach, each IoT device communicates only with members of its own group and treats all other devices as potentially malicious. This ensures that the group remains secure and inaccessible to unauthorized devices.

The authentication method consists of two phases: the association phase and the data exchange phase. The association phase begins when a device attempts to join a specific group, while the data exchange phase starts when two members within the same group want to communicate. In this method, there are two types of entities: the master and the follower. The master is responsible for creating a group. When a follower wants to join, the master first verifies its credentials before granting permission. These credentials include three key values: GroupID, which identifies the group; ObjectID, which identifies the follower; and PublicAddress, which represents the follower’s public address.

To join a group, the follower sends its credential values to the master using a Python socket. The master then signs the combined credential values using Node.js to generate a follower ticket on the blockchain. This ticket is verified using the Elliptic curve digital signature algorithm. If the ticket is valid, the follower becomes a member of the group. However, if the follower tries to join a group that does not exist the transaction will be canceled.

Figure 1 illustrates a dual-environment authentication framework where a Node.js backend issues signed tickets to followers for on-chain verification. The process utilizes ECDSA (ecrecover) within a blockchain environment to validate the "Association" and "Exchange" transactions against a Master public key. As shown in the figure, the architecture is implemented across both public blockchain infrastructures (using MetaMask and Rinkeby/Ropsten) and private blockchain (using Ganache and Injected Web3), with a Python Socket facilitating the communication layer between the components.

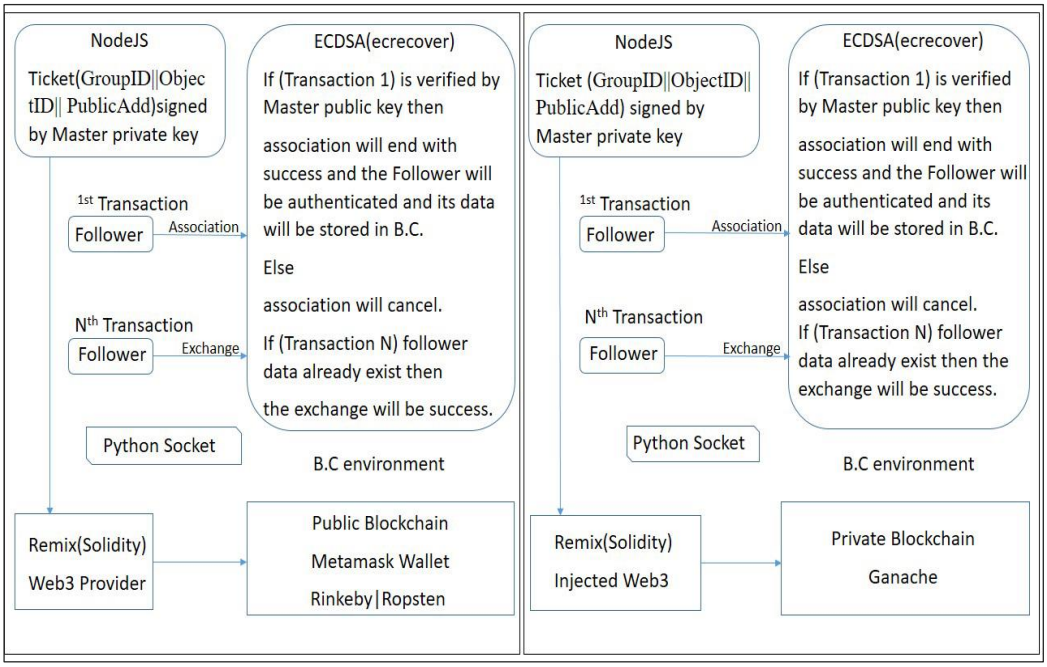

Figure1: Authentication Method Framework

3.1. EVALUATION OF THE AUTHENTICATION METHOD

To evaluate the authentication method in public blockchain, two simulators were used, Rinkeby and Ropsten. The Rinkeby is a test network that uses a Proof of Authority consensus method to validate transactions. The Ropsten is a test network that uses a Proof of Work consensus method to validate transactions. The authentication method was tested using the Remix online editor with a Web3 provider environment to connect to a MetaMask wallet. The Rinkeby test network was selected, and the smart contract was deployed to it. On the Ropsten test network, the same MetaMask account was used, but test ethers were obtained by simply pressing the request button within the MetaMask account. After getting the ethers, the test network is changed to Ropsten. Finally, the same smart contract is deployed to Ropsten test network [21].

To evaluate the authentication method within private blockchain. The execution of the authentication method, along with the testing of distributed applications and smart contracts, are carried out using Ganache simulation. The authentication method is tested in Remix online editor with Injected Web3 environment to start a Ganache process. Ganache minimizes] cost associated with deploying smart contracts. When you want to deploy a smart contract on the Ethereum chain, you need to pay a gas fee for testing purposes. However, Ganache provides a solution by eliminating this cost and allowing testing smart contracts for free [22].

The construction of any group in the blockchain is made by the master of that group. The master triggers a transaction with its identifier and group identifier. The blockchain checks the uniqueness of both the group identifier and master identifier. There are two types of transactions that are performed by followers: association request transaction and data exchange transaction. In the association request transaction, if a follower wants to be a member of a specific group it sends a transaction, then the blockchain validates the uniqueness of the follower's identifier, and checks the legitimacy of the follower's ticket using the public key of the group master. If one of the conditions is not satisfied, the object cannot be a member of the group. The data exchange transaction is done by the members of any group, so a follower's ticket will not be verified because the members have already authenticated in the association request transaction.

3.2. EXPERIMENTAL SETUP

To evaluate the authentication method for time, CPU usage, and memory consumption, two physical devices are used. Since the authentication method has two types of entities (master and follower), the setup includes two laptops. The first laptop runs a virtual machine that acts as the master, while the second laptop has two virtual machines acting as followers. One follower runs Raspberry Pi OS (Buster version), and the other runs Ubuntu 21.04. The follower applications are developed using Python to send their credentials (GroupID, ObjectID, and PublicAddress) to the master, which then signs a ticket for authentication, Table 1 shows the specifications of the used virtual machines.

Table 1: Virtual Machine Specifications.

Virtual Machine	CPU Operation Mode	CPU Max Speed	RAM	Operating system
Master	64-bits	1.80 GHz	8.00 GB	Ubuntu 21.04
Follower 1	64-bits	1.80 GHz	4.00 GB	Ubuntu 21.04
Follower 2	32-bits	1.80 GHz	4.00 GB	Raspberry Pi OS (buster)

Rinkeby and Ropsten were used as a public blockchains and Ganache was used as a private blockchain. The smart contract that satisfies the authentication is deployed using Solidity language [23]. This study focuses on 20 investigations [24] that are conducted to evaluate the performance. The performance of the authentication method in the public and private blockchains is evaluated against the following performance metrics:

1. Time required to send an association request or data exchange and receive a response, which is a critical metric, especially for Internet of Things devices with limited storage and processing capacity. Minimizing the time consumption is crucial to optimize the performance of these devices.
2. CPU usage involved in sending an association request or data exchange and receiving a response. Minimizing CPU usage is ideal for Internet of Things devices with limited storage and processing capacity as it enhances device efficiency.
3. Memory consumption during the transmission of an association request or data exchange and receiving a response. Minimizing memory consumption is crucial for Internet of Things devices with limited storage and processing capacity, as it ensures efficient resource utilization.

4. RESULTS AND DISCUSSIONS

This paper evaluates the performance of an authentication method using two public blockchains and one private blockchain. This section presents the findings from the experimental results related to time, CPU usage, and memory consumption for the both types the evaluated blockchains.

4.1. TIME CONSUMPTION

Table 2, displays the average time in seconds and the corresponding standard deviation for association requests and data exchange. This metric is calculated based on 20 conducted experiments, providing a comprehensive overview of the performance metrics associated with these experiments. The analysis of Table 2 reveals that Ganache exhibits lower average time values and standard deviations compared to Rinkeby and Ropsten for both association requests and data exchange. This happens because Ganache has fewer participants in the network, resulting in faster consensus reaching. Furthermore, Ganache does not employ Proof of Work as its consensus algorithm, which eliminates the computational overhead associated with the Proof of Work method. In contrast, Rinkeby and Ropsten utilize Proof of Work, which involves extensive computation, hence leading to longer processing time. Additionally, Rinkeby and Ropsten operates as a public blockchains, accessible to a wide range of participants, which can further contribute to increased delays.

.

Table 2: Time Consumption.

Device Type	Association request time in seconds						Message exchange time in seconds					
	Ganache		Rinkeby		Ropsten		Ganache		Rinkeby		Ropsten	
	Avg	SD	Avg	SD	Avg	SD	Avg	SD	Avg	SD	Avg	SD
Raspberry PI	1.30	0.00	19.55	3.47	29.00	19.97	1.30	0.00	13.25	3.71	28.00	19.21
Laptop	1.30	0.00	19.07	4.06	29.00	19.97	1.30	0.00	13.55	3.71	28.00	19.21

4.2. CPU USAGE

Table 3, presents the average CPU usage in seconds and the corresponding standard deviation for association requests and data exchange. This metric is calculated based on 20 conducted experiments, providing insights into the CPU usage. The results of Table 3 indicates that Ganache exhibits lower average CPU usage values and standard deviations compared to Rinkeby and Ropsten for both association requests and data exchange. This lower average is because the distinct nature of the private and public blockchains in terms of resource consumption. Rinkeby and Ropsten, being public blockchains, require substantial resources to operate and achieve network consensus. This increased resource demand contributes to higher CPU usage. Additionally, these public blockchains employ Proof of Work as their consensus algorithm, which involves solving complex mathematical puzzles. Additionally, the computational requirements of Proof of Work further contribute to the higher CPU consumption observed in Rinkeby and Ropsten. On the other hand, Ganache operates as a private blockchain limited to users within a specific organization. This user limitation base and the absence of Proof of Work as the consensus algorithm result in lower CPU usage.

Table 3: CPU Usage.

Device Type	Association request CPU usage in seconds						Message exchange CPU usage in seconds					
	Ganache		Rinkeby		Ropsten		Ganache		Rinkeby		Ropsten	
	Avg	SD	Avg	SD	Avg	SD	Avg	SD	Avg	SD	Avg	SD
Raspberry PI	8.70	2.31	9.20	4.81	15.75	10.03	7.90	2.31	8.35	4.32	11.05	5.71
Laptop	8.50	2.67	8.85	4.66	9.70	5.65	7.30	2.11	8.45	4.97	8.80	5.70

4.3. MEMORY CONSUMPTION

Table 4, presents the average memory usage in kilobytes and the standard deviation for association requests and data exchange. This metric is calculated based on 20 conducted experiments. From Table 4 it is clear that Rinkeby and Ropsten has a lower memory value in average and standard deviation compared with Ganache in association requests and data exchange. This result is because Ganache is an Ethereum application, so during its running, it consumes more memory storage, but the interaction with Rinkeby and Ropsten is done using a web page that redirects to https://etherscan.io/.

Table 4: Memory Consumption.

Device Type	Association request memory in Kbytes						Message exchange memory in Kbytes					
	Ganache		Rinkeby		Ropsten		Ganache		Rinkeby		Ropsten	
	Avg	SD	Avg	SD	Avg	SD	Avg	SD	Avg	SD	Avg	SD
Raspberry PI	15.00	2.51	11.60	1.31	16.30	1.18	12.70	2.54	9.35	1.31	14.60	2.37
Laptop	15.50	2.87	13.15	1.18	14.05	1.15	13.50	2.80	10.90	1.29	12.05	1.15

5. CONCLUSION

With the rapid spread of IoT devices and their inherent capability to communicate without human intervention, ensuring the safety and security of such communication becomes important. In this research, a performance evaluation was conducted to assess the effectiveness of an authentication method in one private and two public blockchains. The evaluation covered scenarios where IoT devices were associated with their groups and exchanged data with each other.

Based on the obtained results, it is evident that the private blockchain had lower time and CPU usage compared to the public blockchains. This was because the use of a limited number of users in the private blockchain, whereas the public blockchains are open to anyone, leading to increased number of users. However, the public blockchains demonstrated lower memory consumption compared to the private blockchain. This can be caused by the nature of public blockchains, which allow for the acceptance of a larger number of participants while efficiently managing memory resources. In the context of authentication for IoT applications, blockchain proves to be superior to centralized authentication methods by eliminating a single point of failure. However, it is important to consider the specific requirements of the IoT application. For real-time IoT applications where timing is critical, a private blockchain is recommended due to its lower time consumption. Conversely, if timing is less critical for the IoT application, a public blockchain can be chosen, as it offers the advantage of accommodating the growth number of users. The future work will involve executing a testbed to evaluate at least two IoT applications, each representing an IoT group. One of these applications focuses on real-time functionality, while the other has no strict real-time requirements. By conducting this testbed execution, we aim to evaluate the performance of the authentication method in different blockchain environments, specifically in the context of IoT applications.

REFERENCES

[1] P. Guillemin and P. Friess, "Internet of things strategic research roadmap. The Cluster of European Research Projects," in Tech. Report: River Publishers, 2009.
[2] H. F. Atlam, R. J. Walters, and G. B. Wills, "Internet of nano things: security issues and applications," in Proceedings of the 2018 2nd International Conference on Cloud and Big Data Computing, 2018, pp. 71-77.
[3] J. J. Sikorski, J. Haughton, and M. Kraft, "Blockchain technology in the chemical industry: Machine-to-machine electricity market," Applied Energy, vol. 195, pp. 234-246, 2017.
[4] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," Future Generation Computer Systems, vol. 82, pp. 395-411, 2018.
[5] Coinhouse, "What is Proof of Authority?," 23 July 2019. [Online]. Available: https://www.coinhouse.com/learn/what-is-proof-of-authority/.
[6] M. Samaniego and R. Deters, "Blockchain as a Service for IoT," in 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2016: IEEE, pp. 433-436.
[7] J. Zhang, Z. Wang, Z. Yang, and Q. Zhang, "Proximity based IoT device authentication," in IEEE INFOCOM 2017-IEEE Conference on Computer Communications, 2017: IEEE, pp. 1-9.

[8] H. F. Atlam and G. B. Wills, "Technical aspects of blockchain and IoT," in Advances in Computers, vol. 115: Elsevier, 2019, pp. 1-39.
[9] M. Pilkington, "Blockchain technology: principles and applications," in Research handbook on digital transformations: Edward Elgar Publishing, 2016.
[10] R. Fotohi and F. S. Aliee, "Securing communication between things using blockchain technology based on authentication and SHA-256 to improving scalability in large-scale IoT," Computer Networks, vol. 197, p. 108331, 2021.
[11] M. N. Aman, K. C. Chua, and B. Sikdar, "A light-weight mutual authentication protocol for iot systems," in GLOBECOM 2017-2017 IEEE Global Communications Conference, 2017: IEEE, pp. 1-6.
[12] V. Shivraj, M. Rajan, M. Singh, and P. Balamuralidhar, "One time password authentication scheme based on elliptic curves for Internet of Things (IoT)," in 2015 5th National Symposium on Information Technology: Towards New Smart World (NSITNSW), 2015: IEEE, pp. 1-6.
[13] F. Wu, X. Li, L. Xu, S. Kumari, M. Karuppiah, and J. Shen, "A lightweight and privacy-preserving mutual authentication scheme for wearable devices assisted by cloud server," Computers & Electrical Engineering, vol. 63, pp. 168-181, 2017.
[14] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, "Bubbles of Trust: A decentralized blockchain-based authentication system for IoT," Computers & Security, vol. 78, pp. 126-142, 2018.
[15] N. Kshetri, "Blockchain's roles in strengthening cybersecurity and protecting privacy," Telecommunications policy, vol. 41, no. 10, pp. 1027-1038, 2017.
[16] J. Chen, "Hybrid blockchain and pseudonymous authentication for secure and trusted IoT networks," ACM SIGBED Review, vol. 15, no. 5, pp. 22-28, 2018.
[17] F. K. Santoso and N. C. Vun, "Securing IoT for smart home system," in 2015 International Symposium on Consumer Electronics (ISCE), 2015: IEEE, pp. 1-2.
[18] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in internet of things: challenges and solutions," arXiv preprint arXiv:1608.05187, 2016.
[19] K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, and T. Hayajneh, "Healthcare blockchain system using smart contracts for secure automated remote patient monitoring," Journal of medical systems, vol. 42, no. 7, p. 130, 2018.
[20] A. Fayad, B. Hammi, and R. Khatoun, "An adaptive authentication and authorization scheme for iot's gateways: a blockchain based approach," in 2018 Third International Conference on Security of Smart Cities, Industrial Control System and Communications (SSIC), 2018: IEEE, pp. 1-7.
[21] C. Nnamdi, "Top 4 Ethereum testnets for testing smart contracts," December 7, 2021. [Online]. Available: https://blog.logrocket.com/top-4-ethereum-testnets-testing-smart-contracts/.
[22] Moralis, "What is Ganache Blockchain?," JULY 12, 2021. [Online]. Available: ganache-explained-what-is-ganache-blockchain/.
[23] "Welcome to Remix's documentation!," 2019-21. [Online]. Available: https://remix-ide.readthedocs.io/en/latest/.
[24] Abdulrhman, A., Bamatraf, M. M., & Baqais, K. A. (2022). Performance evaluation of authentication public blockchains. 2022 International Conference on Intelligent Technology, System and Service for Internet of Everything (ITSS-IoE).
[25] A. K. Al Hwaitat, M. A. Almaiah, A. Ali, S. Al-Otaibi, R. Shishakly, A. Lutfi, and M. Alrawad, "A New Blockchain-Based Authentication Framework for Secure IoT Networks," *Electronics*, vol. 12, no. 17, 2023, Art. no. 3618.
[26] R. Singh, S. Sturley, B. Sharma, and I. B. Dhaou, "Blockchain-enabled device authentication and authorisation for Internet of Things," in *Proceedings of the 2023 1st International Conference on Advanced Innovations in Smart Cities (ICAISC)*, 2023, pp. 1-6.
[27] W. Villegas-Ch, J. C. Tello-Oquendo, and W. Sanchez-Gomez, "Lightweight Blockchain for Authentication and Authorization in Resource-Constrained IoT Networks," *IEEE Access*, vol. 13, 2025, pp. 48047–48067.