OPEN ACCESS

International Journal of Innovations in Science & Technology

50SEA

Check for updates

IJIST
P ISSN : 2618-1630
E ISSN : 2909-6130

(LSM: A Lightweight Security Mechanism for IoT Based Smart City Management Systems using Blockchain)

Original Article

Hafiz Humza Saeed[1], Abdullah Bin Masood[2],Hassaan Khaliq Qureshi[1]
[1]National University of Science and Technology (NUST), Islamabad, Pakistan.
[2]University of Cyprus (UCY), Nicosia, Cyprus.
[2]CYENS - Centre of Excellence, Nicosia, Cyprus.
*Correspondence: (hsaeed.msee18seecs, hassaan.khaliq)@seecs.edu.pk, amasoo01@ucy.ac.cy

Citation | Saeed, H. H., Bin Masood, A., & Khaliq Qureshi, H. (2021). LSM: A Lightweight Security Mechanism for IoT Based Smart City Management Systems using Blockchain. International Journal of Innovations in Science & Technology, 3(4), 1–14. Retrieved from https://journal.50sea.com/index.php/IJIST/article/view/91

DOI | https://doi.org/10.33411/IJIST/2021030501

Received Dec 15, 2021; **Revised** |Dec 19, 2021, **Accepted** | Dec 19, 2021; **Published** | Dec 20,2021.

Smart cities utilize digital technologies for the improvement of its services' quality and performance by reducing resources' cost and consumption, with a commitment of action and efficiency to its citizens. The increased urban migration has led to many problems in cities, such as traffic congestion, waste management, noise pollution, energy consumption, air pollution, etc., as nowadays COVID-19 pandemic has seized the whole world. So, it is necessary to carry out its standard operating procedures (SOPs), including less human interaction. Thus, technology plays a vital role via Internet-of-Things (IoT) based systems. In this paper, a lightweight security mechanism (LSM) is proposed to enrich the IoT based systems. Blockchain technology is integrated, and its completely decentralized peer-to-peer (P2P) technology enables the users' authentication and authorizes legitimate procedures. The IoT based management system is developed to monitor some of the aforementioned problems and solve solid waste, air, and noise monitoring systems. The Ethereum blockchain is used to implement a smart contract based framework for the system's security and access control. The evaluation of performance of the LSM demonstrates that it is an efficient and lightweight tool in terms of cost, resources, and computation and superior over related security studies.

Keywords: Smart City, Internet-of-Things, Lightweight Security Mechanism, Blockchain, Smart Contract.

Acknowledgment:
This manuscript has not been published or submitted to any other journals

Author's Contribution
This work is conceptualized by H. K. Q. Associated application concepts and experimentation design is done by H. H. S. A. B. M. provided technical input to improve the quality and presentation of work. All the authors read and approved the final manuscript.

Informed consent: Informed consent was obtained from all the individuals included in the study.

Conflict of interest
The authors declare no conflict of interest in publishing this manuscript in IJIST.

Project details.
This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 739578 and the Government of the Republic of Cyprus through the Deputy Ministry of Research, Innovation and Digital Policy.

Introduction

According to the 2017 census, Pakistan's urban population was 32% in 1998, which has increased to 40% and is predicted to reach 50% by 2025 [1]. With the rise of population, the burden on city administrations to provide essential services to all citizens has also increased. Moreover, the COVID-19 pandemic has held onto the entire world. Thus, it is vital to complete its standard operating procedures (SOPs), which incorporate less human interaction utilizing technology for several purposes [2], [3]. There has been a significant development in the intelligence of digital devices, such as smart machines, smartphones, and smart sensors, leading to the high-quality pursuits of the Internet-of-Things (IoT) to meet administrative requirements [4]. IoT uses the internet to connect different devices in different areas to collect and analyze information without human-to-human interaction [5].

IoT works on mechanism of transferring the data from sensor to cloud through gateway to store data from where different integrated devices share their information to communicate or to exchange data with each other. This working mechanism reduced the human interaction with computer as sensors automatically exchange their information with each other. Human have just to monitor the data on Graphical-User Interface (GUI) developed for different types of data. IoT includes three layers, the perception layer, the network layer and the application layer [6]. The perception layer includes a group of devices authorized for the Internet which are able to sense the objects, and for exchange of data with other devices by Internet communication systems. Radio Frequency Identification Devices (RFID), cameras, sensors, Global Positioning Systems (GPS) are examples of layer of perception of the devices. Information transmits from perception layer to application layer through the network layer. IoT systems use a combination of short-range systems of communication technologies such as Bluetooth and ZigBee to carry the data of the devices of the perception to a gateway near based on the functionality of the parties' appellants. The technologies of the Internet such as Wi-Fi, 2G, 3G and 4G carry information on long distances based on the implementation [7].

IoT devices have to be built-in with various devices and units, enabling them to interact and engage seamlessly with each other in an impervious way to reduce human resources [8]. Thus, this large volume of data can also pose many problems as it is centralized and monitored from time to time by a single provider. The cloud is a processing and storage technology that cannot guard its consumers' security and privacy [9]. The work was being started, and different techniques were proposed, but the integration of IoT with blockchain technology gained the limelight of researchers and developers [10], [11]. Blockchain made its space in the market due to its decentralized, distributed, and tamperproof ledger properties. Blockchain technology has proven to be sufficient for economic purposes like Bitcoin and can be of incredible value [12], [13]. Integrating it with the IoT based management system enables an extra layer of security and data integrity by authorizing only authentic users. It maintains transaction archives throughout countless nodes that are Peer-to-Peer (P2P) coupled, making it tamperproof [14], [15].

By smart contract, it allows more functionality to play with the IoT and blockchain's integration with each other. A blockchain based scheme by issuing tokens for user access to fog-enabled IoT devices using a smart contract is developed (J. K. Mudhar et al., 2020) [16]. The tokens are issued to the user by the admin in an off-chain procedure by which the question of the token's confidentiality and integrity is raised. However, the feasibility of the system in a real environment is not tested likewise (J. Oh et al., 2021) [17]. In (A. Ouaddah, 2019) [18], a Fair Access and PPDAC is introduced as a lightweight and privacy-preserving access control-based on blockchain, mainly the open access and public type.

On the other hand, (P. Velmurugadass etal., 2021) [19] constructed a blockchain based architecture that is used for data integrity and privacy in the IaaS cloud. However, Proof-of-Work (PoW) is not suitable for IoT systems as they are resource constraints. Apart from blockchain, (M. Masud et al., 2021) [20], a one-way cryptographic hash, bitwise XOR, and nounce (number used only once) are used to provide a lightweight and secure communication. In (G. Sharma et al., 2019) [21], (M. Wazid et al., 2019) [22], proposed a lightweight authentication scheme that proved to be as insecure against privileged insider attacks.

Considering and overcoming the issues raised in the aforementioned studies, LSM, a lightweight security mechanism is proposed. LSM has a strong authentication with accurate verification and reduced the computational overhead. Its performance evaluation makes it a lightweight mechanism for security, resources, optimization, and time. The application chosen to demonstrate the LSM feasibility and potential in a real environment, IoT based smart city management system, is developed to monitor and provide a solution to solid waste, air, and noise monitoring management systems. These smart applications aimed to lead automation to reduce human-to-human or human-to-computer interaction due to the COVID-19 pandemic.

Waste management is a primary expenditure in many modern cities since both the cost for the service and the storage of waste in landfills are relatively high. In current scenario, collection and management of waste is quite difficult without the use of modern technology [23], [24]. To overcome these waste management problems, an IoT based system can be deployed to allow the terminals, namely "Smart Bins," to monitor the available data to manage and call the garbage truck when necessary. IoT based system also offers statistics on air quality in saturated areas, parks, and health tracks. In this way, humans can locate the healthiest route outdoors. This provision requires that the air pollution sensors be deployed in the metropolis and share the statistics freely with all authorized residents [25], [26].

The noise is also a form of pollution as the carbon dioxide (CO_2) in the air. In this case, the metropolis experts have already issued particular legal guidelines to decrease the quantity of noise in the metropolis [27], [28]. However, despite being written on boards (Quiet zone), people keep making noise in the hospital's regions. IoT based framework will observe noise levels for the authorities to take necessary actions. This service can improve the decorum of hospital areas and the silence at night.

Benefiting from IoT characteristics and the distributed nature of blockchain, proposed LSM: a lightweight security mechanism for IoT based smart city management systems. The main contributions of this paper are given below:

- A computationally efficient smart contract based lightweight security mechanism (LSM) for IoT based smart city management system is proposed.
- LSM is secure against various attacks like a spoof, Sybil, and replay.
- LSM only permits the registered and verified users to access the IoT data through the smart contract they authorized for IoT devices.

Section I presents the introduction, literature review, objective and contributions. System architecture and testbed implementation for LSM is provided in section II. Section III evaluates the performance of the LSM in terms of security, time overhead, and benchmark studies. Further, the concluding remarks are offered in section IV.

Material and Methods

LSM's architecture is shown in Figure 1. The flowchart of the IoT based smart city management is shown in Figure 2. The architecture of the developed system is consisting of two components whose functionalities are discussed below:

Hardware Components:

Different sensors and modules are incorporated in this system architecture to represent IoT system. microphone, MQ-6, and ultrasonic sensors are used for noise, air, and garbage monitoring, respectively. Mini-fan is used as a vacuum for demonstration purposes. Wi-Fi, GSM, and GPS modules transmit IoT data, messages, and locations, respectively. All sensors and modules are interfaced with an Arduino-Uno board, which is an 8-bit microcontroller integrated circuit.

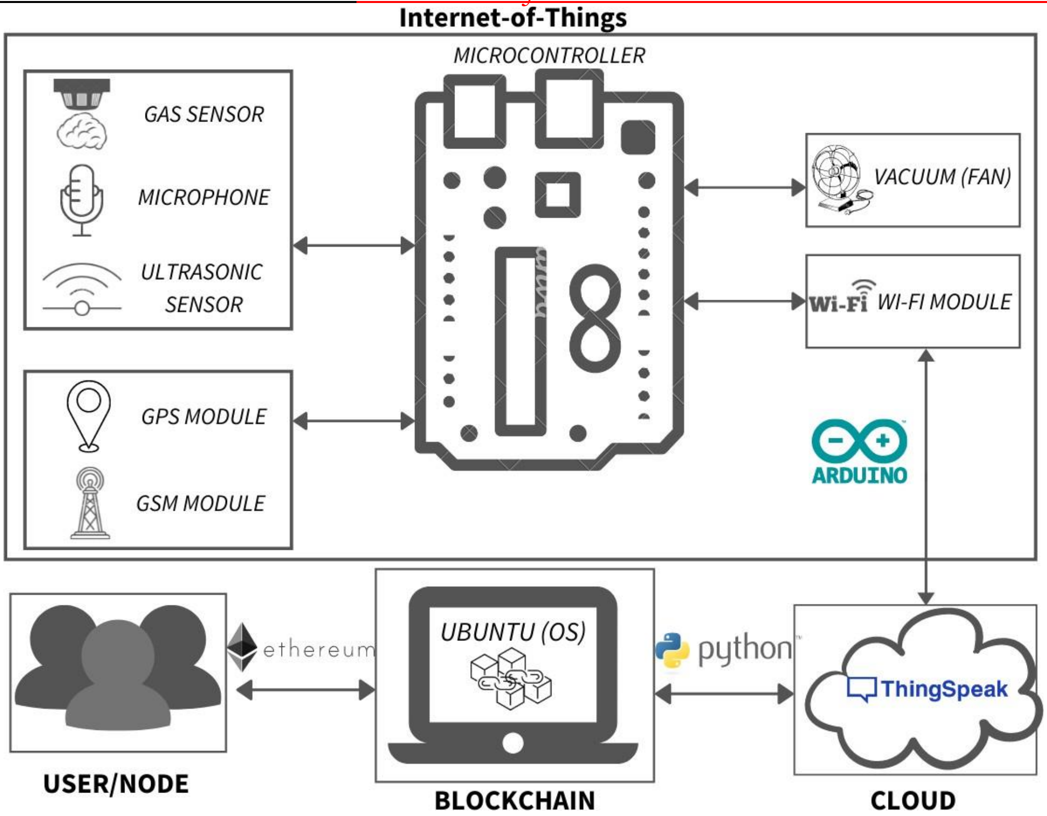


Figure 1 System Architecture of LSM

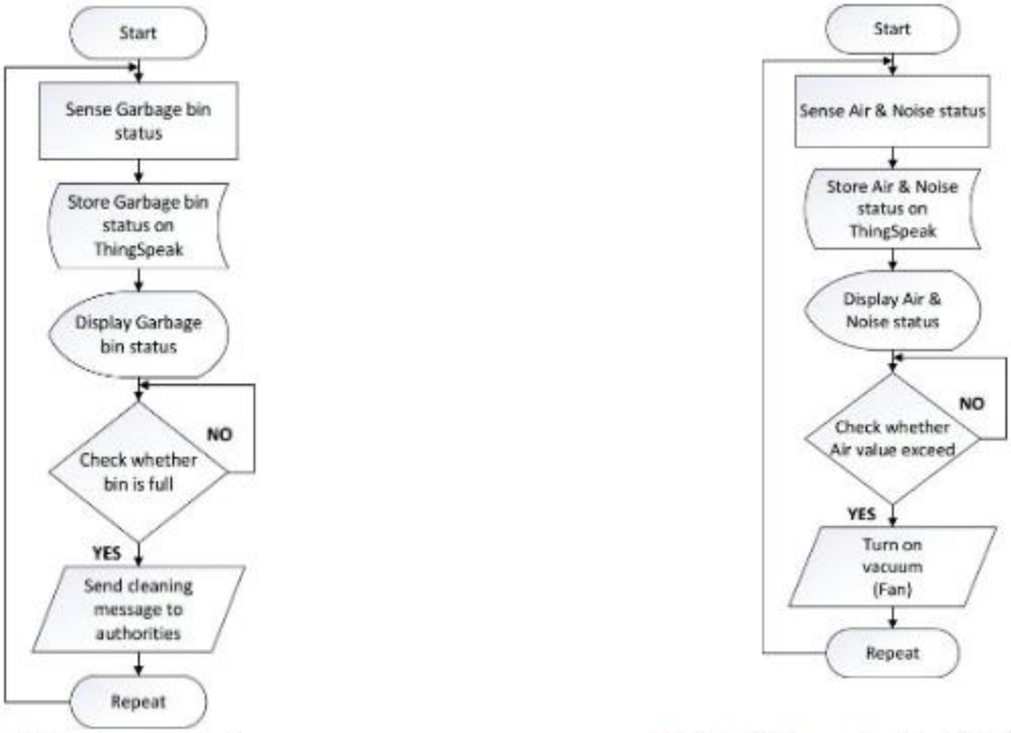
Software Components:

Arduino-Genuino software is used for code compilation and configuration of the modules. To store data on the cloud, the Thing Speak server is used. Ethereum is a popular platform that can process any complex algorithm code through Ethereum Virtual Machine (EVM). So, Ubuntu operating system (OS) is used in this system architecture for Ethereum blockchain development. Communication between Ethereum and cloud is done through a python script that includes the JSON-RPC protocol and the Web3py library1, which are lightweight and efficient for a resource constraint environment. An Ethereum node can call or deploy a smart contract using Go-Ethereum (Geth) client. A smart contract is a bunch of rules or provisions of an agreement that executes on a blockchain to audit and authorize these concurred terms without the association of an outsider. Solidity, a high-level language, is used to write a smart contract. Remix IDE and Truffle suite are used to develop and deploy the smart contract.

The IoT based smart city management system is implemented to demonstrate the potential to carry out the LSM as a Proof-of-Concept (PoC). The garbage monitoring system will update their data after every five minutes. The air monitoring system will update after every fifteen minutes, and the noise monitoring system will continuously update its data. IoT devices are connected with the cloud to upload their data and communicate with each other. Users are connected to the blockchain. The advantage of this method is that users get IoT data only when they request it. Resource optimization is done via this technique. User authentication is done via a smart contract in the blockchain and brings confidentiality, integrity, authenticity, and various security attacks like a spoof, sybil, and replay. This study aims to get a lightweight security mechanism in IoT as they operate in a resource constraint environment. Table 1 shows the notations used in this paper.

IoT based Garbage System

In this system, ultrasonic sensor and GPS module are attached to the garbage bin through which data and location information is fetched. By using the distance formula “s = v × t”, the ultra sonic sensor measures the bin status. Through the Wi-Fi module on it, statistics are uploaded on the cloud, enabling the users to monitor it from anywhere. Whenever the garbage bin is full, the message is sent through the GSM module to authorities to take necessary actions.

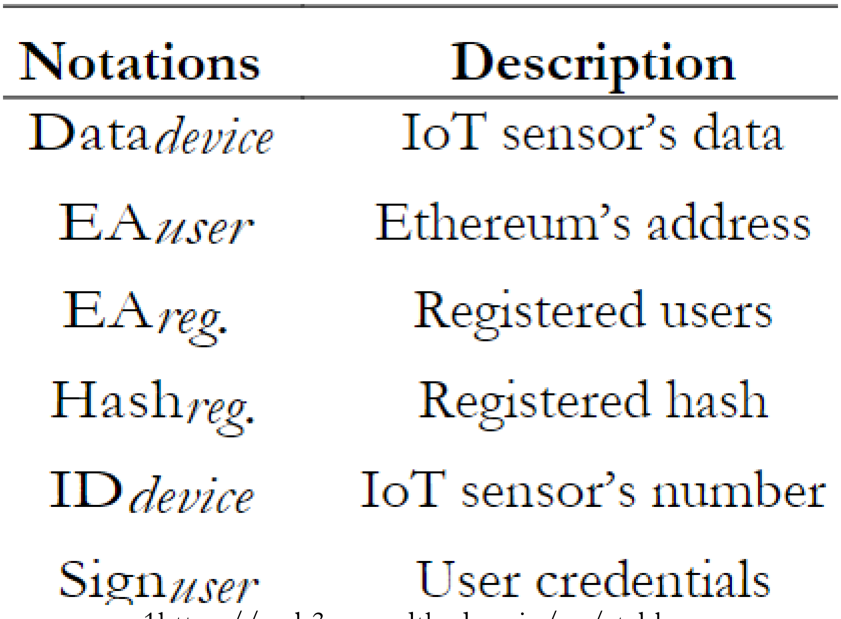

Start
Sense Garbage bin status
Store Garbage bin status on ThingSpeak
Display Garbage bin status
Check whether bin is full
NO
YES
Send cleaning message to authorities
Repeat
Start
Sense Air & Noise status
Store Air & Noise status on ThingSpeak
Display Air & Noise status
Check whether Air value exceed
NO
YES
Turn on vacuum (Fan)
Repeat

(a) IoT based Garbage System

(b) IoT based Air & Noise System

Figure 2 Flowchart of IoT based Smart City Management System

Table 1. Table of Notations



Notations	Description
$Data_{device}$	IoT sensor's data
EA_{user}	Ethereum's address
$EA_{reg.}$	Registered users
$Hash_{reg.}$	Registered hash
ID_{device}	IoT sensor's number
$Sign_{user}$	User credentials

1https://web3py.readthedocs.io/en/stable

IoT based Air & Noise Monitoring System

Different sensors such as MQ-6 and microphones are used to fetch the value of noise and air pollution from the surroundings in this system. In addition, GPS module is used to access the location. Through the Wi-Fi module on it, statistics are uploaded on the cloud, enabling the users to monitor it from anywhere. A relay is used to interface the fan with the air sensor. Whenever a gas value passes a specific value, the signal is given to the relay, and the fan is operated.

Algorithm 1: Smart Contract

```
Input: $Sign_{user}$, $ID_{device}$
Output: $Data_{device}$ Data:
$EA_{reg.}$, $Hash_{reg.}$
                                  // Checking if the user is authorized to the system
if $EA_{user} \neq EA_{reg.}$ then
    return false
                                  // Checking if the user is authorized to the device
    else if $keccak256(Sign_{user}, ID_{device}) == Hash_{reg.}$ then
        return true, $Data_{device}$
        else
            return false
```

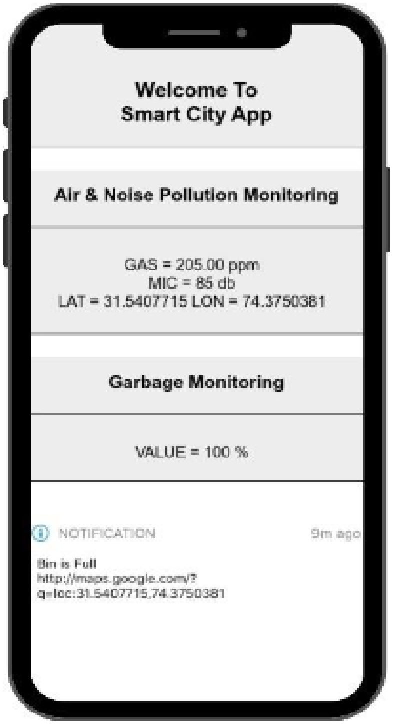
Blockchain Integration

Ethereum blockchain and its nodes are developed using the Geth implementation on Ubuntu OS. The genesis file is created using a puppeth to trigger the Ethereum blockchain. Clique, Proof-of-Authority (PoA), consensus protocol is opted [29]. Keccak256 algorithm is used to create Ethereum addresses [30]. Elliptic Curve Digital Signature Algorithm (ECDSA) generates private and public keys. The smart contract is developed utilizing the Remix IDE platform. The functionality of the smart contract is presented in Algorithm 1. The Truffle suite is utilized for the deployment of the smart contract. Smart contract transactions cannot be changed and are permanently stored in a transparent framework. The deployed code of the smart contract cannot be changed and is only triggered by the sender's transaction message.

Result and Discussion

The developed IoT based smart city management system is illustrated in Figure 3. The specifications of the devices on which the developed system is evaluated are shown in Table 2. The results are system-dependent. They can vary from system to system as their specifications change. The smart city application's results are taken by deploying the IoT system in Lahore city[2]31.5204° N, 74.3587° E.

The incoming sensor's data is transmitted via a python script using JSON-RPC and Web3py library. The python script loads data from the cloud's URL3 and directs it to the blockchain. When the user is required to screen any of the IoT's data, it will enter it self's credentials (Sign user) and the required sensor number (ID device) from its Ethereum address (EA user). Then, the smart contract will first check the authenticity of the user by comparing EA user with the registered users (EA reg.). If the user is authentic, then it will check the combine hash of Sign user and ID device using Keccak256 algorithm with registered hashes (Hashreg.). Different numbers are assigned to various sensors. The number "0" is given to the microphone and "1" to the ultrasonic sensor, and "2" to the gas sensor. If the hash matches and the user is authorized to access the requested IoT's sensor data, then the respective values are then sent to the requested user; otherwise, it will return "false", as illustrated in Figure 4. The complete sequence diagram of LSM is illustrated in Figure 5.



Welcome To
Smart City App

Air & Noise Pollution Monitoring

GAS = 205.00 ppm
MIC = 85 db
LAT = 31.5407715 LON = 74.3750381

Garbage Monitoring

VALUE = 100 %

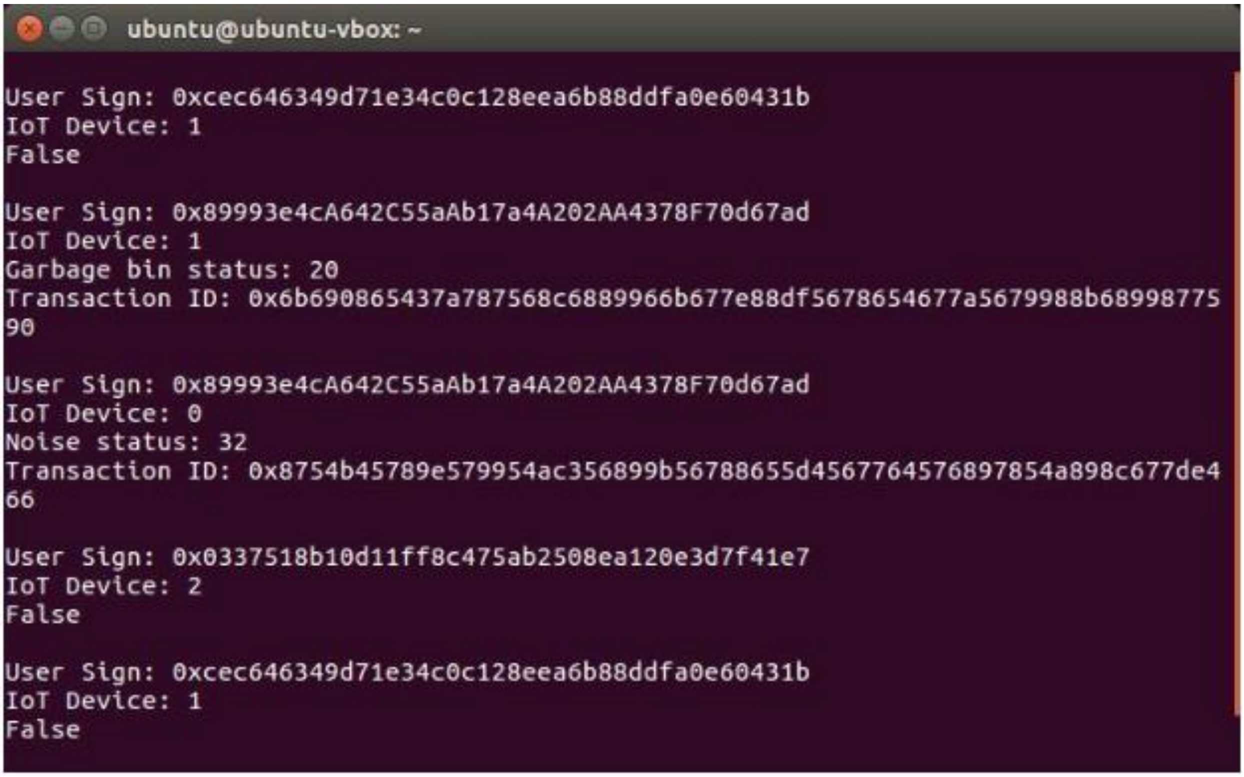
NOTIFICATION 9m ago

Bin is Full
http://maps.google.com/?
q=loc:31.5407715,74.3750381

Figure 3 IoT based Smart City Management System

Table 2 Specification of Devices

Device	Model	Processing Speed
Laptop	HP-450-Notebook	Intel Core i5, 3rd Gen.
Internet Router	PTCL DSL-G2452D	8 Mbps



```
User Sign: 0xcec646349d71e34c0c128eea6b88ddfa0e60431b
IoT Device: 1
False

User Sign: 0x89993e4cA642C55aAb17a4A202AA4378F70d67ad
IoT Device: 1
Garbage bin status: 20
Transaction ID: 0x6b690865437a787568c6889966b677e88df5678654677a5679988b68998775
90

User Sign: 0x89993e4cA642C55aAb17a4A202AA4378F70d67ad
IoT Device: 0
Noise status: 32
Transaction ID: 0x8754b45789e579954ac356899b56788655d4567764576897854a898c677de4
66

User Sign: 0x0337518b10d11ff8c475ab2508ea120e3d7f41e7
IoT Device: 2
False

User Sign: 0xcec646349d71e34c0c128eea6b88ddfa0e60431b
IoT Device: 1
False
```

Figure 4 User Authentication via LSM

Security Analysis

- **Integrity**:

  For the integrity of the data in the system, data is signed before sending data to the recipient, using the ECDSA algorithm supported by Ethereum. The recipient confirms this against the smart contract's address.

- **Identification**:

  Sign user and ID device is required to access the IoT system. Each device and user registered with the system has a separate ID and sign.3https://thingspeak.com/

- **Non-repudiation**:

  All transactions are signed with their respective Sign user. Therefore, the sender cannot repudiate having performed a transaction.

- **Authentication:**

  The user must first be registered with the IoT system. If the user is already registered, the smart contract has the associated credentials. As soon as the smart contract verifies the existence and validity of the details provided by the user, it can interact with the IoT system.

- **Spoof attack**:

  To successfully launch a spoof attack, attacker need a Sign user, ID device and EA user. If the attacker somehow gets the ID device and EA user, still needs the Sign user.

- **Sybil attack**:

  In a Sybil attack, the attacker needs to create a fake identity to enter into the system. In LSM, users and devices are not allowed to have more than one ID. The message is signed with the private key. Therefore, creating a fake identity in the system has been reduced and is almost infeasible.

- **Replay attack:**

  In LSM, all messages generated in the system are assigned to a unique transaction ID and timestamp. Therefore, a replay message with a previously accepted transaction ID will be rejected. So, protection against replay attacks is coped.

Time Overhead

If users directly access the cloud for the IoT data, the delay is less as compared to the blockchain. Because users are interacting with the cloud direct now, but there is no significant security in the cloud. On the other hand, in blockchain, users interact with the cloud via blockchain due to which processing and propagation delay increases. So, this is our trade-off between delay and security. But, as the number of users increases in the cloud, the total delay increases because of the rise in queuing delay. But in blockchain, despite the increase in the number of users, total delay remains almost constant, as illustrated in Figure 6. The total delay is calculated using the total delay equation, illustrated in Figure 7.

Comparison with Relevant Work

Gas is described as a resource that is paid for transaction verification. By increasing the gas limit, the average block size increases, affecting the increase in cost. A large block size means more space to store the Ethereum blockchain. LSM consumed 26664 gas, illustrated in Figure 8. While (J. K. Mudhar et al., 2020)'s request access smart contract consumed 51402 gas. (P. Velmurugadass et al., 2021) used PoW operations which include more CPU power consumption as compared to PoA. So does the energy consumption also increase in PoW which has a negative effect on the system's delay. PoA is a lightweight consensus protocol, and its equipment is also cost effective as compared to PoW.

LSM can scale well regarding the number of devices without affecting the system as the cloud manages it. The computational effort is independent of the number of devices. LSM is tested in a real environment and has a permission access control compared to (J. Oh et al., 2021), and (A. Ouaddah, 2019).

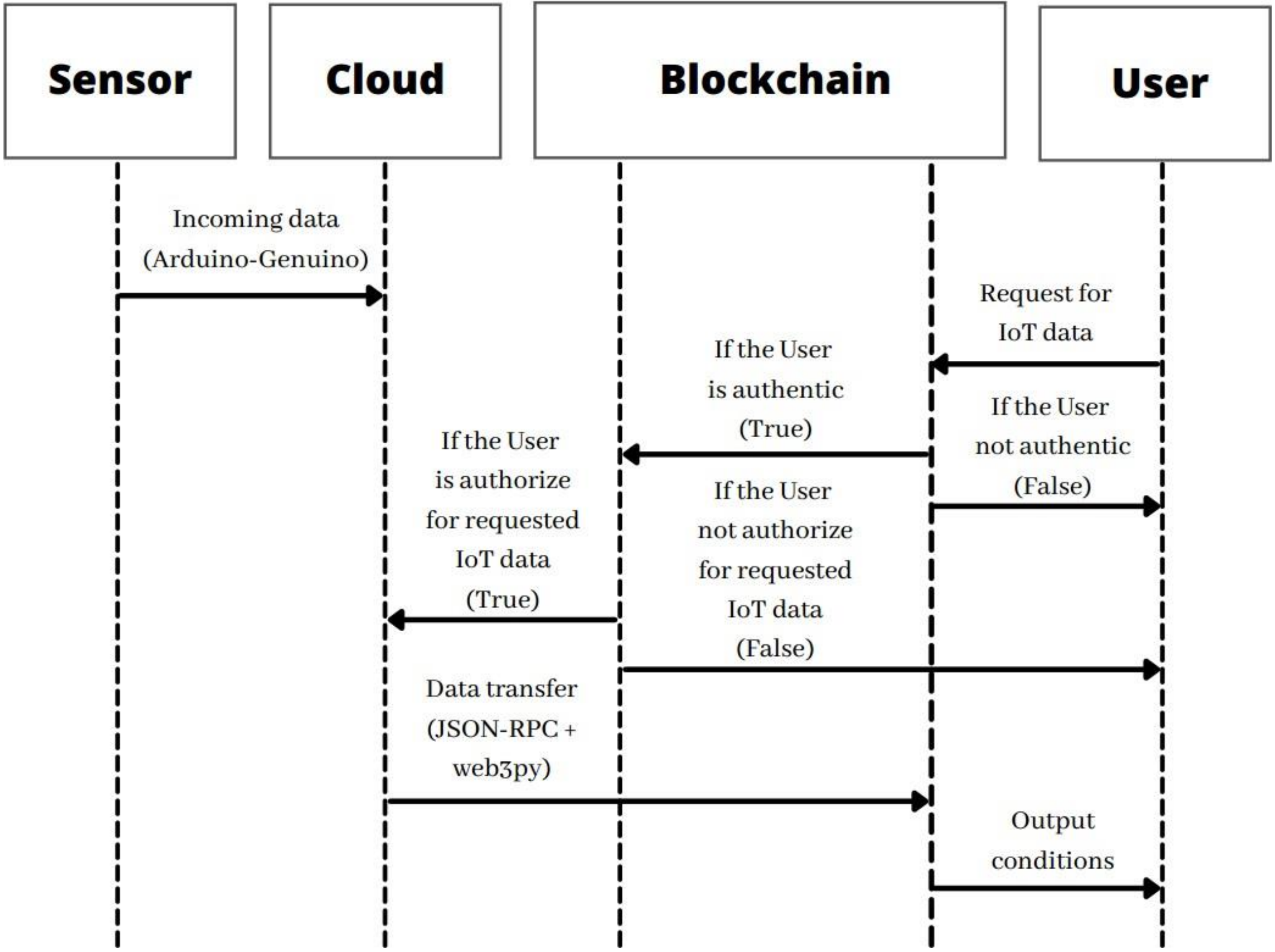

Sensor
Cloud
Blockchain
User
Incoming data (Arduino-Genuino)
Request for IoT data
If the User is authentic (True)
If the User not authentic (False)
If the User is authorize for requested IoT data (True)
If the User not authorize for requested IoT data (False)
Data transfer (JSON-RPC + web3py)
Output conditions

Figure 5 Sequence Diagram of LSM

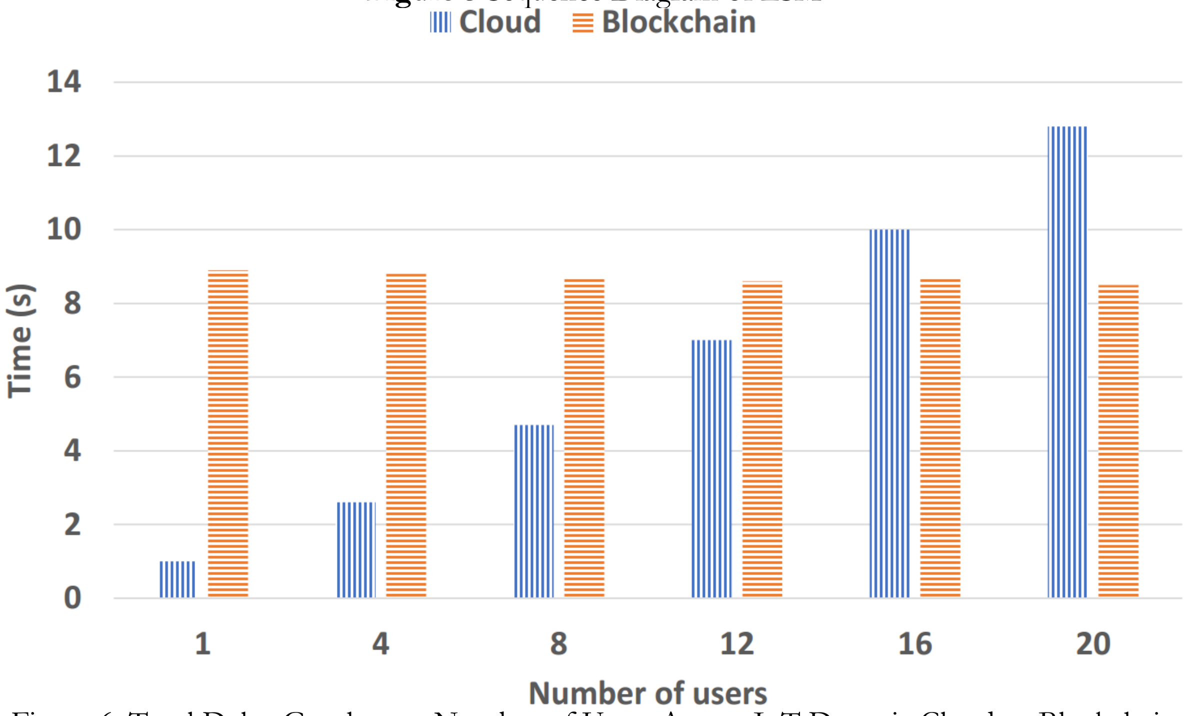


Figure 6. Total Delay Graph over Number of Users Access IoT Data via Cloud vs Blockchain

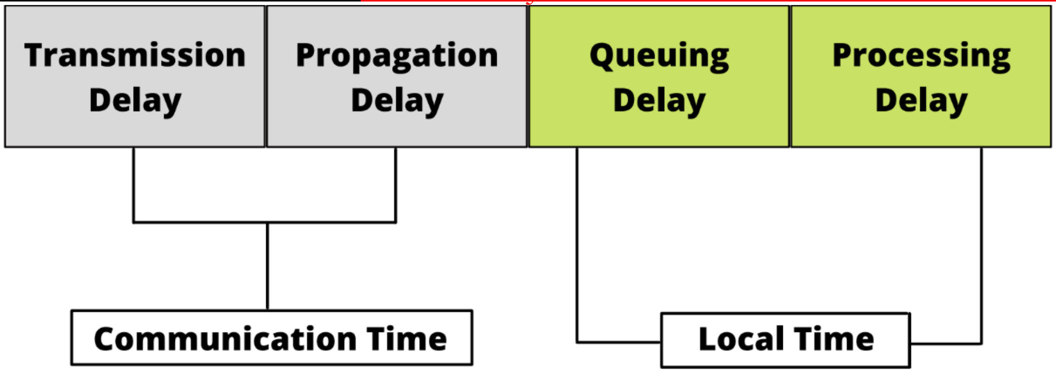


Figure 7. Time Overhead Calculations

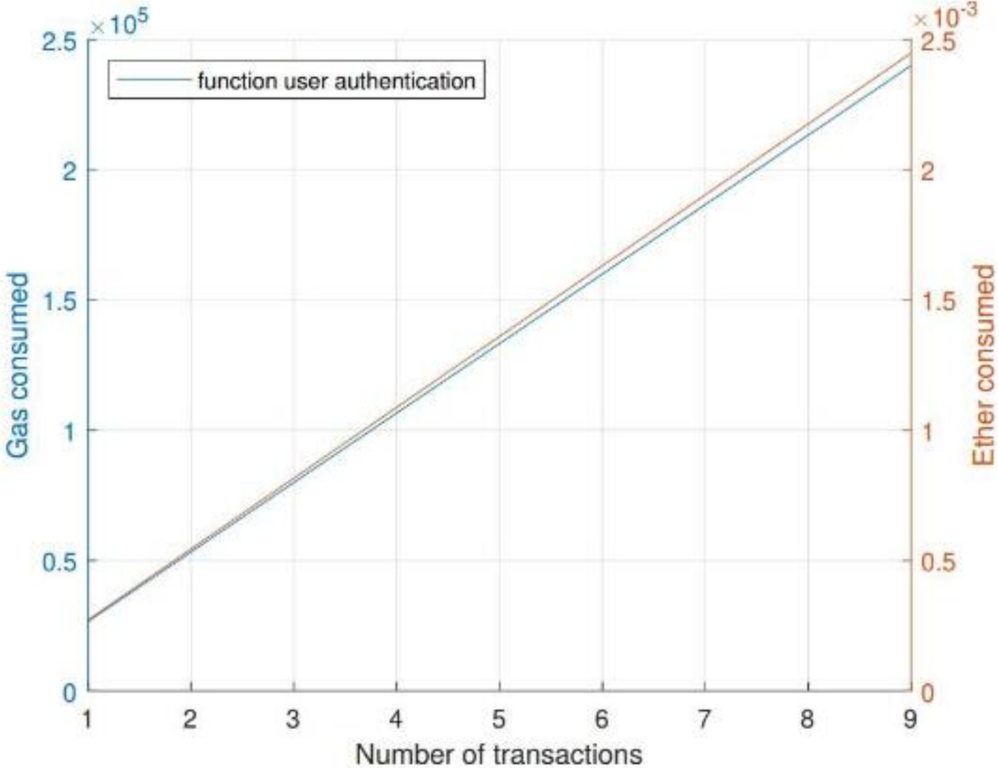


Figure 8. Computational Graph of LMS in terms of Gas and Ether consumed

Conclusion

This paper demonstrated the lightweight security mechanism LSM for an IoT based smart city application management system by integrating blockchain technology within the network, enhancing the user authentication and access control using the smart contract. The performance evaluation illustrates LSM as a lightweight in terms of cost, resources, and computation. While secure in the spoof, sybil, and replay attacks. In the near future, the plan is to extend the system with more applications and add machine learning/deep learning to make smart cities more efficient and autonomous to cope with the recent and zero-day attacks.

References

1. N. V. M. Lopes and S. Farooq, “Smart city governance model for Pakistan,” “Smart Governance for Cities: Perspectives and Experiences” 2020, pp. 17–28.
2. D. Skegg, P. Gluckman, G. Boulton, H. Hackmann, S. S. A. Karim, P. Piot, and C. Woopen, “Future scenarios for the covid-19 pandemic,” “The Lancet” 2021, vol. 397, pp. 777–778.
3. M. Salman, Z. U. Mustafa, N. Asif, N. Shehzadi, T. M. Khan, T. H. Mallhi, Y. H. Khan, F. Saleem et al., “Awareness of covid-19 among illiterate population in Pakistan: A cross-sectional analysis,” “Disaster Medicine and Public Health Preparedness” 2021, pp. 1–17.
4. S. Balne and G. Sindhu, “Network protocol challenges of internet of things (iot) features-review,” “International Journal of Innovative Research in Science, Engineering and Technology” 2021, vol. 10, pp. 2305–2309.
5. M. A. Khan and K. Salah, “Iot security: Review, blockchain solutions, and open challenges,” “Future Generation Computer Systems” 2018, vol. 82, pp. 395–411.
6. Z. Lv, L. Qiao, A. Kumar Singh, and Q. Wang, “Ai-empowered iot security for smart cities,” “ACM Transactions on Internet Technology” 2021, vol. 21, pp. 1–21.
7. .H. Kashani, M. Madanipour, M. Nikravan, P. Asghari, and E. Mahdipour, “A systematic review of iot in healthcare: Applications, techniques, and trends,” “Journal of Network and Computer Applications” 2021, pp. 103164
8. A. Sudha et al., “An analytical review on privacy-preserving and public auditing in cloud storage,” “IEEE Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)” 2021, pp. 74–80.
9. M. M. Khandekar and R. V. Dhumal, “Review paper on cloud computing,” “Case Studies for Research in Computer Science and Engineering” 2021, pp. 17.
10. N. Rifi, E. Rachkidi, N. Agoulmine, and N. C. Taher, “Towards using blockchain technology for iot data access protection,” “IEEE 17th international conference on ubiquitous wireless broadband (ICUWB)” 2017, pp. 1–5.
11. P. Chinnasamy, C. Vinothini, S. Arunkumar, S. A. Sundarraj, and S. Annlin, “Blockchaintechnology in smart-cities,” “Blockchain Technology: Applications and Challenges” 2021, pp. 179.
12. H.-N. Dai, Z. Zheng, and Y. Zhang, “Blockchain for internet of things: A survey,” “IEEE Internet of Things Journal” 2019, vol. 6, pp. 8076–8094.
13. A. F. Aysan, H. B. Demirtas¸ , and M. Sarac¸ , “The ascent of bitcoin: Bibliometric analysis of bitcoin research,” “Journal of Risk and Financial Management” 2021, vol. 14, pp. 427.

14. M. Shurman, A. A.-R. Obeidat, and S. A.-D. Al-Shurman, “Blockchain and smart contract for iot,” “IEEE 11th International Conference on Information and Communication Systems (ICICS)” 2020, pp. 361–366.
15. S. Hakak, W. Z. Khan, G. A. Gilkar, M. Imran, and N. Guizani, “Securing smart cities through blockchain technology: Architecture, requirements, and challenges,” “IEEE Network” 2020, vol. 34, pp. 8–14.
16. J. K. Mudhar, S. Kalra, and J. Malhotra, “An efficient blockchain based authentication scheme to secure fog enabled iot devices,” “IEEE Indo–Taiwan 2nd International Conference on Computing, Analytics and Networks (Indo-Taiwan ICAN)” 2020, pp. 75–80.
17. J. Oh, S. Yu, J. Lee, S. Son, M. Kim, and Y. Park, “A secure and lightweight authentication protocol for iot-based smart homes,” “Sensors” 2021, vol. 21 pp. 1488.
18. A. Ouaddah, “A blockchain based access control framework for the security and privacy of iot with strong anonymity unlinkability and intractability guarantees,” “Advances in Computers” 2019, vol. 115, pp. 211–258.
19. P. Velmurugadass, S. Dhanasekaran, S. S. Anand, and V. Vasudevan, “Enhancing blockchain security in cloud computing with iot environment using ecies and cryptography hash algorithm,” “Materials Today: Proceedings” 2021, vol. 37, pp. 2653–2659.
20. M. Masud, G. S. Gaba, K. Choudhary, M. S. Hossain, M. F. Alhamid, and G. Muhammad, “Lightweight and anonymity- preserving user authentication scheme for iot-based healthcare,” “IEEE Internet of Things Journal” 2021, pp. 1.
21. G. Sharma and S. Kalra, “A lightweight user authentication scheme for cloud-iot based healthcare services,” “Iranian Journal of Science and Technology, Transactions of Electrical Engineering” 2019, vol. 43, pp. 619–636.
22. M. Wazid, A. K. Das, S. Shetty, J. JPC Rodrigues, and Y. Park, “Ldakm-eiot: Lightweight device authentication and key management mechanism for edge-based iot deployment,” “Sensors” 2019, vol. 19, pp. 5539.
23. K. R. Vanapalli, H. B. Sharma, V. P. Ranjan, B. Samal, J. Bhattacharya, B. K. Dubey, and S. Goel, “Challenges and strategies for effective plastic waste management during and post covid-19 pandemic,” “Science of The Total Environment” 2021, vol. 750, pp. 141514.
24. S. Nanda and F. Berruti, “Municipal solid waste management and landfilling technologies: a review,” “Environmental Chemistry Letters” 2021, vol. 19, pp. 1433–1456.

25. S. W. Hunt, D. A. Winner, K. Wesson, and J. T. Kelly, "Furthering a partnership: Air quality modeling and improving public health," "Journal of the Air & Waste Management Association" 2021, vol. 71, pp. 682-688.

26. S. Malleswari and T. K. Mohana, "Air pollution monitoring system using iot devices," "Materials Today: Proceedings" 2021.

27. R. Chandrappa and D. B. Das, "Noise pollution," "Environmental Health-Theory and Practice" 2021, pp. 141–148.

28. D. Dobrilovic´, V. Brtka, G. Jotanovic´, Zˇ. Stojanov, G. Jausˇevac, and M. Malic´, "Architecture of iot system for smart monitoring and management of traffic noise," "5th EAI International Conference on Management of Manufacturing Systems" 2022, pp. 251–266.

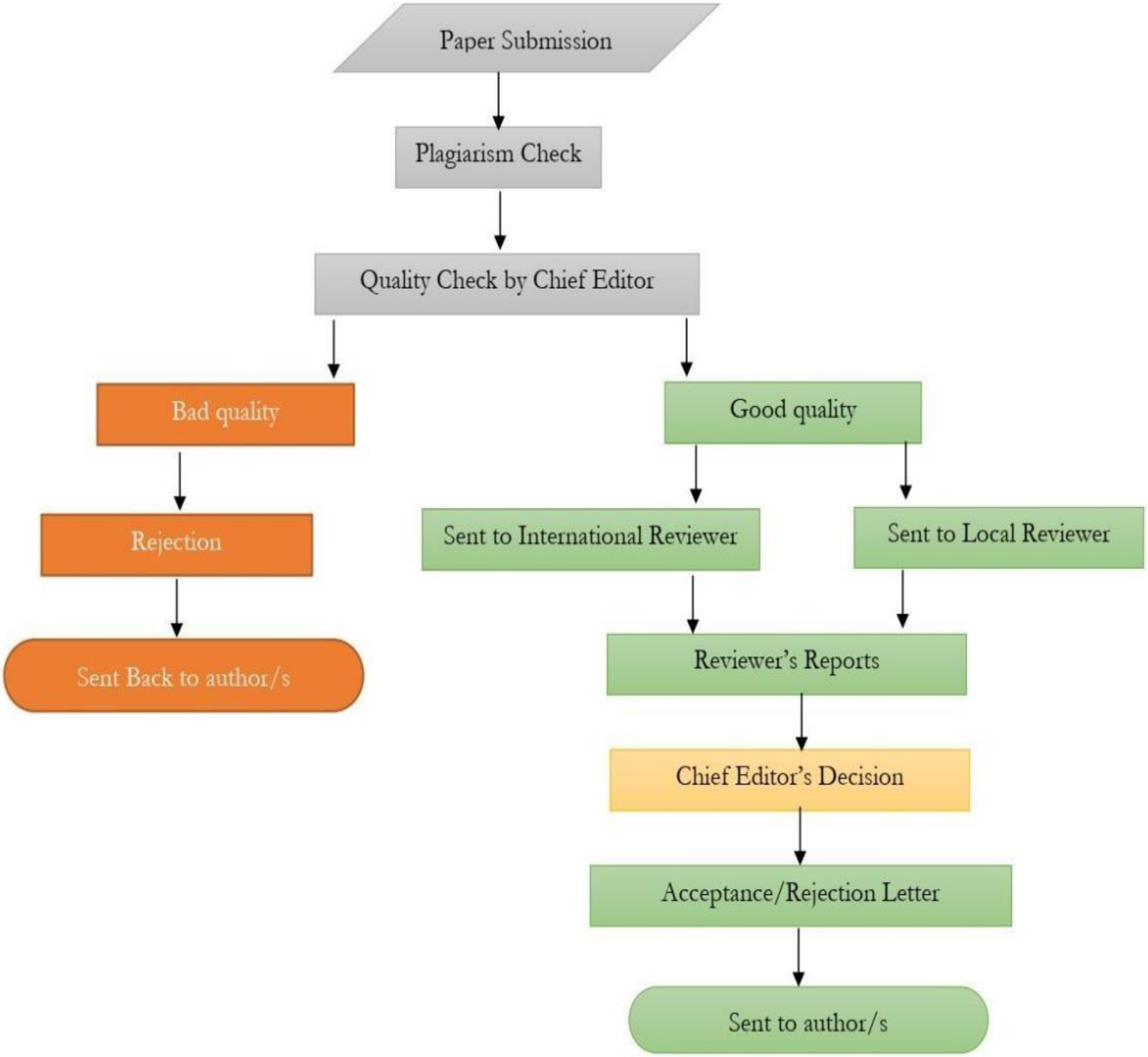
29. S. Joshi, "Feasibility of proof of authority as a consensus protocol model," "arXiv preprint arXiv:2109.02480" 2021.

30. T. A. Alghamdi, I. Ali, N. Javaid, and M. Shafiq, "Secure service provisioning scheme for lightweight iot devices with a fair payment system and an incentive mechanism based on blockchain," "IEEE Access" 2019, vol. 8, pp. 1048–1061.

31. M. Hussain, M. Beg et al., "Fog computing for internet of things (iot)-aided smart grid architectures," "Big Data and cognitive computing" 2019, vol. 3, pp. 8.

32. A. Ahmad, M. Saad, J. Kim, D. Nyang, and D. Mohaisen, "Performance evaluation of consensus protocols in blockchain- based audit systems," "IEEE International Conference on Information Networking (ICOIN)" 2021, pp. 654–656.

Peer Review Process


Paper Submission
Plagiarism Check
Quality Check by Chief Editor
Bad quality
Rejection
Sent Back to author/s
Good quality
Sent to International Reviewer
Sent to Local Reviewer
Reviewer's Reports
Chief Editor's Decision
Acceptance/Rejection Letter
Sent to author/s