INTERNATIONAL JOURNAL OF TECHO-ENGINEERING

ISSN: 2057-5688

A secure privacy preserving storage authentication in IOT using Blockchain

Punna Shiva Krishna[1]

Sayyad Rasheed Uddin[2]

[1]MTech Student, Department of CSE, Malla Reddy College of Engineering, Dulapally Road Maisammaguda, Hyderabad, Telangana 500100, shivakrishnapunna2013@gmail.com

[2]Assistant professor, Malla Reddy College of Engineering, Dulapally Road Maisammaguda, Hyderabad, Telangana 500100, rasheeduddin.mrce@gmail.com

Abstract: There are a variety of sensing devices in the "Internet of Things" (IoTs) that may be used in a variety of ways. Networks in these situations are difficult to safeguard against illicit information access because of their limited storage capacity and data processing capabilities. Many security and data storage options are available to researchers, but only a handful of them are suitable for WSN-enabled IoTs. A decentralised blockchain architecture with authentication and privacy protection techniques is thus being developed for secure communication in Internet of Things (IoT) facilitated by wireless sensor networks (WSNs). In a cloud computing context, communication among sensor nodes and the base station (BS) is enabled via the use of registration, certification, and revocation processes. The BS receives the information from the cluster leaders. Thus, the distributed blockchain stores all of the critical parameters, and massive data is sent to the cloud for storage. All hostile nodes' revoked certificates are removed from the blockchain by BS. When it comes to the suggested scheme's detection accuracy and certification delay as well as the computational overheads, it is examined. Comparative analysis and security testing have shown that the suggested solution is superior to current methods.

Key Terms: Wireless Sensor Network, Internet of Things, Security, Blockchain, Distributed, privacy and authentication.

ISSN: 2057-5688

I. Introduction

Wireless communication and information processing are being transformed by the Internet of Things (IoTs), a widely used, valuable, and increasingly dominating technology [1]. The Internet of Things (IoTs) is a concept that describes 'things' that can be identified, understood, managed, and even found via the internet. Almost anything in the Internet of Things (IoT) can now be linked to the internet because of the internet's communication and processing capabilities, allowing for the development of new and better applications [2]. The Internet of Things (IoT) makes use of a slew of sensor nodes for monitoring, sensing, and automating tasks. IoT [3] would be incomplete without WSNs, a collection of these nodes that can detect and monitor any physical items or actions in a given area. WSNs are an integral aspect of IoT. The aforementioned sensor nodes, also known as ‘motes’, are cheap, tiny and are connected internally and distributed in specific areas [4]. These sensor nodes combine multi-features of sensing, computing and communication through wireless medium and hence in WSNs, physical phenomena are monitored and sensed in real time. Although, WSNs operation is applications specific in terms of the area of interest and way of deployment, but the final aim is monitoring, sensing, broadcasting and the processing of the collected information [5] [6]. However, the amount of information is huge with an extraordinary rate and that need to be addressed in the current technological world. As known, WSNs are used in a variety of applications such as military, industry, smart home, healthcare, surveillance, habitat monitoring and agriculture to name a few. [7] [8]. Sensor nodes, the backbone of WSN, have limited resources such as energy, computational capability, storage, and communication bandwidth. So, when the demands of WSNs are gradually increases in IoT, more challenges are getting unearthed for the efficient use of it. Moreover, security is another most important concern in WSN enabled IoT. If an adversary attacks the network and deliberately compromised the nodes, the network security becomes a threat. Therefore, it is required for WSNs to distinguish and eliminate malicious nodes from the network before becoming an active member in the IoT infrastructure.

II. Related survey

ISSN: 2057-5688

WSNs-based IoT using blockchain technology is discussed briefly before describing the suggested network architecture and the findings gained. It is essential that IoT devices create a big volume of data that can be downloaded on demand for immediate use. Several issues have been raised about cloud storage of IoT-based data [9]. The distribution of data storage in Internet of Things devices has been improved utilising hash values in cloud computing-based data storage [10]. Fog computing has been proposed as an energy-efficient framework for healthcare's IoT big data solution. With reduced latency and delay, the data may be accessed in real time. Data management for IoT devices may now be done in a unique way. Recoverability and survivability were used to assess the scheme's effectiveness in the event that the network in question failed [12]. Fog nodes or mini-clouds in the edge devices have been included into the distributed cloud-IoT system for data optimization.

The proposed scheme offers promising results in terms of latency and energy consumption by proper traffic aggregation and processing [13]. The concept of integration of edge computing with sensor nodes has adopted for processing of data locally by compressing the data quickly. The integrated scheme provides effective results which minimize communication overheads by handling various monitoring, reconfiguration, and data adaption actions [14]. A secure data management and deletion scheme has been introduced using key derivation encryption and data analysis to handle personal information of IoT devices. The sensitive user's information is encrypted using derivation key algorithm which ensures the privacy of data with reducing the page transfer overheads optimally [15]. Various authentication schemes have been recently developed by different researchers can be seen elsewhere [16] [17] [18]. A mutual authentication, agreement and random node join based smart card authentication for WSNs was developed with particular emphasis on the efficiency of authentication [19]. Another, user efficient authentication method has been introduced without using smart card which provided security against insider attack, theft attack and session recovery attack in any WSNs [20]. Further, to improve the functionality, a three-factor based authentication method has been introduced and that accomplish more privacy and authentication in a particular WSNs.

Automated Validation of Internet Security Protocols and Applications (AVISPA) was the next noticeable effort and that utilized formal security verification [11]. Another variation of

ISSN: 2057-5688

mutual authentication-based scheme used biological information and utilized it with hash and XOR computations which offered sufficient password verification. In the category of user efficient authentication, a multi-gateway WSN has been recently developed to accomplish enhanced security. In this exotic approach, the features of most popular schemes, like, password authentication and biometric authenticator are combined to achieve on the desired security. Also, this concept of bio-hashing has been further improved to eradicate the false accept rates without enhancing the false rejection rate efficiently [13].

Authentication mechanisms for IoT systems based on WSNs were many when they were first introduced. The hash and XOR authentication mechanisms were added to the system in the following revision [17] to combat various types of assaults. For WSN-enabled IoTs with fog-assistance, a safe data aggregation mechanism has been created. Peer-to-peer (P2P) communication between sensing nodes is used to transmit sensitive information with an aggregating node, which then broadcasts the information to the fog server securely [18]. Authentication has been made possible via the use of a simple multi-gateway WSN-based IoT system. Sensor 'visit in' and gateway 'out of scope' are the two steps of authentication in this approach [29]. For WSN-based IoT, another authentication method relies on user consent to keep users' identities private. This solution fixes a number of security vulnerabilities while also providing complete anonymity to the user. In this technique, the accuracy of the previous session key is also verified using the user-friendly mutual authentication [20]. For recent WSN-IoT scenarios, an innovative three-factor authentication mechanism has been introduced. This scheme evades different security aspects such as stolen mobile device attack, impersonation attack, poor session key agreement and improbability of revocation phase [21].

However, blockchain, an emerging technology which can improve the security performance by offering various features viz., decentralization, immutability, transparency and distributed consensus. A decentralized blockchain based keyless signature scheme has introduced for secure and efficient key management. Another authentication approach based on blockchain technology has presented for privacy preserving and immutability of vehicles in Vehicular Adhoc Networks (VANETs) [36]. The blockchain in WSN is then an automatic choice to improve the security of WSNIoT with fog or cloud computing or storage. Blockchain based trust model has developed in WSNs for detection of malicious sensor nodes as first step in

ISSN: 2057-5688

this direction. This model identifies malicious nodes in 3D environment using smart contract based blockchain and quadrilateral localization method. The consensus results achieved during this process are stored in a distributed blockchain. Novel trust-based secure localization algorithm has introduced using blockchain technology in WSNs. The beacon nodes have prioritized based on their values of trust for blockchain generation and the consensus construction is subsequently made. Some other blockchain possibilities in IoT are studied. As IoTs are composed of large number of sensing devices with a variety of features applicable for various applications, WSN is indispensable for the growth of IoTs. WSNs consist of a large number of sensing devices with different features deployed in a specific area of interest. But, WSNs faced various challenges in terms of memory, energy, security, computational and communicational cost, etc. The efficient utilization of memory is the most crucial issue of concern and it is also challenging to ensure the privacy of stored information against illegal information access. Therefore, the privacy and authentication of sensor nodes are ensured by BS with registration and certification processes. Further, the information is collected only from authenticated sensor nodes and forwarded towards clouds. The recorded information in clouds is not circulated among third parties.

III. Proposed model

Fog node and IoT user secure data access: Because of the proliferation of the Internet of Things (IoT), large data volumes are being generated by the interconnection of many devices and sensors. Some computing models at the edge devices are required because of latency, bandwidth, and storage constraints in the cloud. Expanding cloud computing, fog computing extends certain services to the end user. Fog computing provides end-users in the IoT with computation, storage, and network resources. Several fog nodes communicate and are autonomous monitoring at the edge through the fog nodes or servers. Rather of transmitting data to the cloud, the fog network collects and distributes data via routers, thereby lowering traffic between access points. Reduced network delays and rapid access to neighbouring network resources may be achieved by increasing service levels in the presence of fog. Cyber infrastructure services may be provided to a large variety of users in very close proximity thanks to a three-layer Edge-Fog-Cloud network. Fog computing architecture is shown in Figure 1.

ISSN: 2057-5688

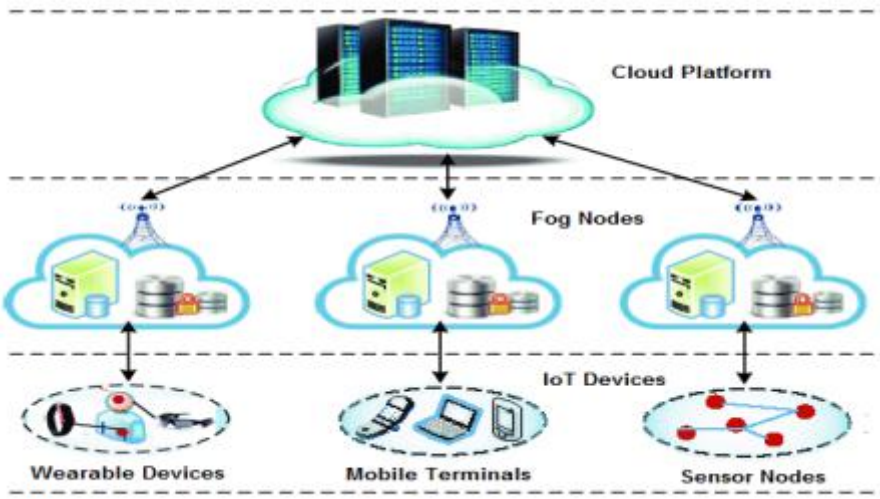

Figure 1: Three Layer Architecture

This three-layered architecture offers data transaction between the user, objects, and method with senses nearby. Data storage, network access, and ready-made applications to the edges of the cloud and fog networks, but Fog is very similar to edges and allows accessibility over a wide area. Since the fog is a middle layer in three-layer architecture, it is essential to extend the defence mechanism over all layers to ensure data security for and from resource-bound edges [12]. The current state with an untrusted cloud network where it is essential to encrypt and evaluate data on encrypted data to secure confidential data stored on Fog nodes. But the latest solution to the cloud cannot match in with the fog environment. There are other studies in this area to address security and privacy issues. But the alternative for distributing resource-constrained apps such as IoT applications is still a little lightweight.

The fog node/servers that pretend to be completely legal, and when not authenticated, connect to edges. For example, fog controller may be a cheat but still monitor the instances of fog. The man-in-the-attack device in fog is unreliable as it can bypass or overwrite the gateway with a fake one. The incorrect one can manipulate interactions with users to carry out more attacks. As fog computing adds an extensive range of end-users, networks and services, an important issue to attend is authentication and data security. As mentioned earlier PKI, is one of the current approaches. This approach is tough to apply for end-users on a broad scale. Fog users cannot use their wireless-tools (mobile phones and tablets) to

ISSN: 2057-5688

implement extensive digital signatures and public-key encryption. Therefore, they have to connect to a network. Login approach doesn't suit multiple users. It takes a long time to tackle the biometric solution. Authentication methods like key sharing with Diffe-Hellman are slow because of modulo computations.

IV. Secured Communication Between Fog And IOT

The cryptographic mechanism applied to protection of end-to-end data to protect the data security of end-users and fog nodes. The end-user requests the service from anywhere, it is difficult for all end-users and the fog nodes to have the same symmetric key built in to maintain data confidentiality. Furthermore, because of the enormous number of end-clients, the entire network key update is required when a user is compromised, which severely increases the network's overhead calculation and communication within a short time. In [175], an asymmetric key is used to compromise keys between nodes and is eventually used to encrypt inter-node collaborative data using the symmetric key. When negotiating with a fixed node, only one key negotiation is needed, which can minimize overhead computation and delay in negotiation. However, one key at a time is the best approach in general, because having only a single key over the life span of the correspondence decreases the secrecy. A new one-time-key establishment protocol has been proposed in [176] which can use to communicate with three parties. This protocol only has to exchange information four times. After the performance review, the protocol's coordination and computing costs were decreased by about 20% compared with other protocols.

Secured communication not only preserves personal security but also maintains the quality of the data. The storage space of end-users is small, and for a long time, it is difficult to store all the data obtained. The data were transmitted to the satellite fog node or cloud to ensure that the data used efficiently. If the data are transfered to other organizations, the end-user lacks control of the data and cannot avoid the alteration of the data by other nodes. If the end-user wants data previously stored in the fog node or server, the validity of the downloaded data becomes difficult to check.

Network Model: The Fog is a cloud extension as an intermediary layer for stable and low latency connectivity as support for edges provided. The 3-layered architecture involves Cloud

ISSN: 2057-5688

Servers (CS) at the application layer. One server among these service providers in the Registration Authority (RS) is responsible for registering users managed by this particular cloud. Under this RS, there are number of Fog (F) which include fog servers/nodes denoted as ƑS = (ƑS1…….. ƑSn). Let IU be IoT user, and there may be many users named as IU = (IU1, IU2; …). Any of them has limited processing facilities and tiny memory that serviced to smart phone users. Such fog servers of a fog F are linked to cloud to support the services and functionality of cloud features to end-users. Fog servers join and leave the fog at any time, dynamically. Yet the operation must be provided to a customer at all times. This versatility of fog servers needs to be accessible to users so that they go with a new server for shared authentication without re-registration process. Any change in the fog server list shall not induce any user-side complexity. Figure 2 shows the general system architecture of fog nodes.

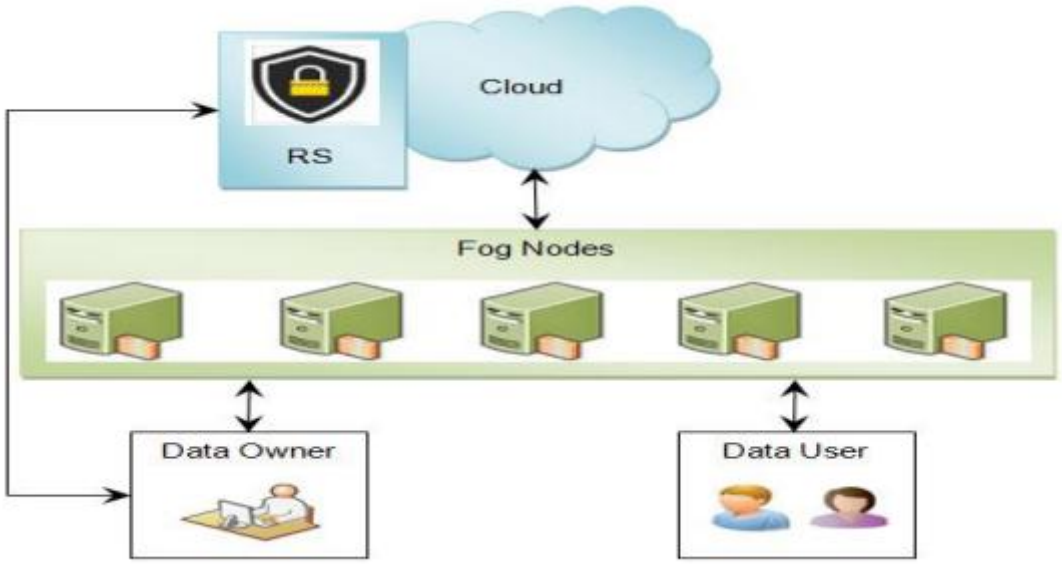

Figure 2: General Architecture of fog nodes

Authentication: This section explains the authentication process. Figure 3 shows the authentication process. Key Generation: In this step, the RS, Fog Server and Users generated the public and private key pairs. Key Exchange: In this step, RS and Fog Server exchange the public keys and Fog Server and users exchange the public keys. Authenticate: Based on the generated key RS authenticate the Fog Server, and Fog Server authenticates the Users.

ISSN: 2057-5688

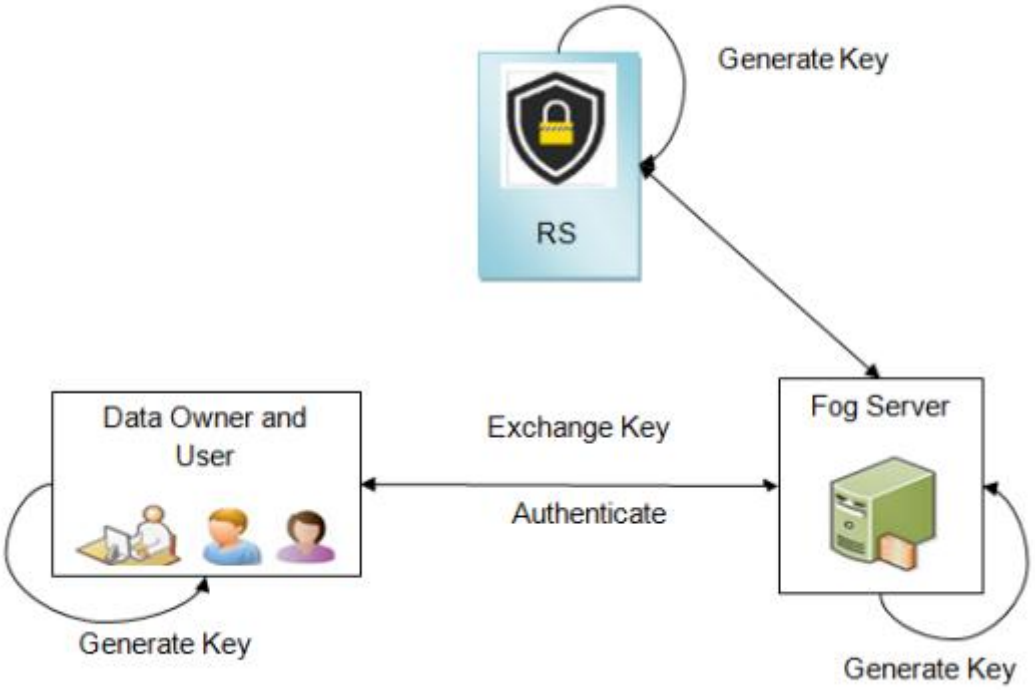

Figure 3: Authentication Process

V. Experimental Results

This section explains the security and performance analysis of the proposed work. The time taken for authentication of both the Fog nodes and IoT user algorithm includes SHA function and AES encryption and AES decryption process shown in Table.

Table 1: computation time difference between IOT user and fog server

Entities	SHA1 (ms)	AES Encryption	AES Decryption	Total time (ms)
IOT user	0.17	1.021	2.012	3.114
Fog Server	0.05	1.06	2.011	3.044

ISSN: 2057-5688

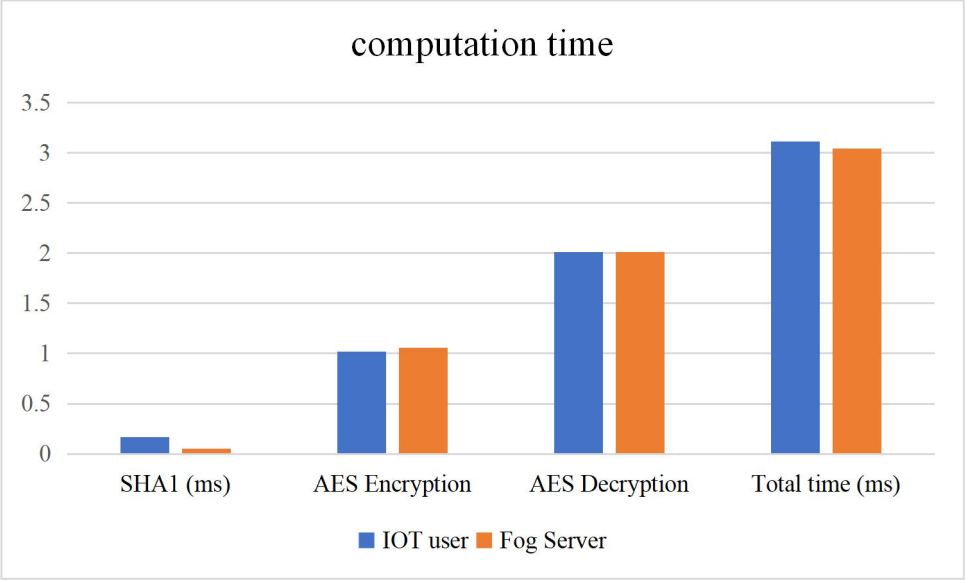

Figure 4: Authentication time difference

This chapter solves the authentication between user and fog based on this concept, particularly when new fog server joins the network. They were using the encryption/decryption process improve the security of confidential outsourcing data. The user produces secure index encryption and data encryption which is then decrypted by the user and servers permitted. The research resulted in fine-grained user authorization with limited key exchange, focused on access policies. This scheme eliminates essential security costs, and thus only one key per user is stored by the system, thereby minimizing storage space and is ideal for fog devices participating in the fog network. The chapter indicates the schemes are excellent in fog setting for IoT applications.

VI. Conclusion

A privacy-preserving authentication scheme based on blockchain with cloud data storage was accomplished effectively for the WSN enabled IoTs. Initially, the process of registration and certification for all sensor nodes was performed by BS. After completing the certification process, all the key parameters were stored in Untameable Key Mechanism (UKM) controlled by the cluster heads. Further, the cluster heads broadcast the collected information from its members to BS and the information is then separated into two parts, i) key parameters and ii) sensed information. The large amount these sensed data was then shared

ISSN: 2057-5688

with cloud for more reliable and efficient storage. The key parameters were further recorded on emerging blockchain technology to improve the immutability and transparency of the obtained data. The certification revocation process successfully eliminated malfunctioning sensor nodes. The proposed scheme accomplished better results in terms of detection accuracy, certification delay and computational overheads. The simulated results and comparative analysis demonstrate that the proposed algorithm achieves 19.33% better results in terms of average of detection accuracy. Sharing large amount of information into cloud storage ensured reliability and effectiveness of the proposed scheme. In future, we shall try to optimize the data management and resources of the framework for effective results.

VII. Future enhancement

Semantic-based method of access control extended to the next level of security by having the history of the user's request and by designing fine-grained policies. The proposed system to be implemented with heterogeneous devices in a real social network is needed to study other factors such as trust. o The IoT uses sensor-based embedded devices to communicate with others, providing users with a broad variety of applications and services. The energy consumption is one of the main issues in IoT and Fog. Another future direction is to develop energy-efficient communication among devices at the edge of the IoT network.

VIII. References

[1] R. Singh, D. K. Singh, and L. Kumar," A review on security issues in wireless sensor network," vol. 2, no. 7, pp. 28–34, 2010.

[2] H. Cai, B. Xu, L. Jiang, and A. V. Vasilakos, "IoT-Based Big Data Storage Systems in Cloud Computing: Perspectives and Challenges," IEEE Internet of Things Journal, vol. 4, no. 1, pp. 75–87, 2017.

[3] M. Wang and Q. Zhang, "Optimized data storage algorithm of IoT based on cloud computing in distributed system," Computer Communications, vol. 157, pp. 124–131, 2020.

[4] C. Feng, M. Adnan, A. Ahmad, A. Ullah, and H. U. Khan, "Towards Energy-Efficient Framework for IoT Big Data Healthcare Solutions," Scientific Programming, vol. 2020, pp. 1–9, 2020.

ISSN: 2057-5688

[5] M. Asiri, T. Sheltami, L. Al-Awami, and A. Yasar, "A Novel Approach for Efficient Management of Data Lifespan of IoT Devices," IEEE Internet of Things Journal, vol. 7, no. 5, pp. 4566–4574, 2020.

[6] P. Maiti, J. Shukla, B. Sahoo, and A. K. Turuk, "Efficient Data Collection for IoT Services in Edge Computing Environment," in Proceedings - 2017 International Conference on Information Technology, ICIT 2017, 2018, pp. 101–106.

[7] M. Adel Serhani, H. T. El-Kassabi, K. Shuaib, A. N. Navaz, B. Benatallah, and A. Beheshti, "Self-adapting cloud services orchestration for fulfilling intensive sensory data-driven IoT workflows," Future Generation Computer Systems, vol. 108, pp. 583–597, 2020.

[8] J. Xiong et al., "A secure data deletion scheme for IoT devices through key derivation encryption and data analysis," Future Generation Computer Systems, 2019.

[9] T. H. Chen and W. K. Shih," A robust mutual authentication protocol for wireless sensor networks," ETRI Journal, vol. 32, no. 5, pp. 704–712, 2010.

[10] N. Bruce, Y. J. Kang, H. R. Kim, S. H. Park, and H. J. Lee," A security protocol based-on mutual authentication application toward wireless sensor network," Lecture Notes in Electrical Engineering, vol. 339, pp. 27–34, 2015.

[11] Y. A. Abdulrahman, M. Kamalrudin, S. Sidek, and M. A. Hassan," Internet of things: Issues and challenges," Journal of Theoretical and Applied Information Technology, vol. 94, no. 1, pp. 52–60, 2016.

[12] SK Lo, Y Liu, SY Chia, X Xu, Q Lu, L Zhu, H Ning, Analysis of blockchain solutions for IoT: A systematic literature review, IEEE Access, vol. 7, 2019, pp. 58822-58835.

[13] R. V Kulkarni, S. Member, A. Forster, and G. K. Venayagamoorthy," Computational Intelligence in Wireless Sensor Networks: A Survey," Communications Surveys & Tutorials, IEEE, vol. 13, no. 1, pp. 68–96, 2011.

[14] A. H. Bagdadee, M. Z. Hoque, and L. Zhang," IoT Based Wireless Sensor Network for Power Quality Control in Smart Grid," Procedia Computer Science, vol. 167, pp. 1148–1160, 2020.

ISSN: 2057-5688

[15] J. Wang, Y. Cao, B. Li, H. jin Kim, and S. Lee," Particle swarm optimization-based clustering algorithm with mobile sink for WSNs," Future Generation Computer Systems, vol. 76, pp. 452–457, 2017.

[16] Z. Song-Juan and Y. Jian," Distributed data storage strategy in wireless sensor networks," International Journal of Online Engineering, vol. 12, no. 11, pp. 52–57, 2016.

[7] L. Buttyan, D. Gessner, A. Hessler, and P. Langendoerfer, "Application of wireless sensor networks in critical infrastructure protection: challenges and design options Security and Privacy in Emerging Wireless Networks," IEEE Wireless Communications, vol. 17, no. 5, pp. 44–49, 2010.