An Access Control Mechanism and Decentralization Authentication in IOT Devices

Abhishek Kumar[1*], Anshul Mohan Gupta[1], Ashish Chaudhary[1], Rajorshi Sen[2]

[1]Computer Science Department, Stony Brook University, NY, USA
[2]Computer Science Department, Cotton College Assam, India

* Corresponding author
doi: https://doi.org/10.21467/proceedings.7.6.45

ABSTRACT

The Internet of Things (IoT) is an innovative technology that enables physical devices to be connected to the Internet, thus linking software services with the physical world. As the number of interconnected devices increases, conventional centralized authentication methods become bottlenecks and single points of failure, rendering them susceptible to assaults. The concept of an Access Control (AC) Mechanism and Decentralized Authentication in IoT Devices is to guarantee secure and streamlined interactions within the IoT ecosystem. So, AC systems govern the authorization of devices and users to access resources and carry out specific actions, hence preventing illegal usage and potential security breaches. Securing permitted AC inside the IoT is crucial for safeguarding privacy and ensuring safety. The main aim of this study is to analyze an AC mechanism and decentralized authentication in IoT devices. The study introduced a new framework that integrates IOTA (distributed ledger technology), having hierarchical identity-grounded encryption. This integration improves both the security along with scalability of IoT. The system demonstrates practical feasibility, with negligible variations in operational time, specifically in the processes of verifying access privileges, having a minimal deviation of 33.35%. This thorough security assessment seemed to offer a strong and precise comprehension of the system's ability to withstand and remain dependable in different hostile circumstances, guaranteeing its appropriateness for safe IoT environments. This study highlighted the significance of selecting the appropriate platform in IoT system architectures and offers valuable insights for implementing efficient, secure, and scalable IoT environments.

Keywords: IOTA; Security; Scalability.

1. INTRODUCTION:

The widespread adoption of IoT devices has fundamentally transformed multiple industries, such as healthcare, smart homes, industrial automation, and transportation, through the provision of improved connectivity and data-centric insights. Nevertheless, this rapid and exponential expansion has also brought quite noteworthy security obstacles [1]. Insufficient security measures in IoT deployments have resulted in a range of security concerns and problems as IoT utilization expands. The IoT functions through three primary layers, each vulnerable to distinct categories of attacks. So, at the perception layer, various types of attacks can occur, including denial-of-service (DoS), distributed DoS (DDoS), replay attacks, side-channel attacks, and false node assaults [2]. Within the network layer, various types of attacks can occur, including man-in-the-middle (MITM), DoS, eavesdropping, sniffing, and routing

Proceedings DOI: 10.21467/proceedings.7.6; Series: AIJR Proceedings; ISSN: 2582-3922; ISBN: 978-81-989164-9-5

attacks. These attacks have the potential to negatively affect data authentication, accessibility, privacy, and the efficiency of the application layer [3]. Security concerns might manifest at several stages within the framework, including communication across devices and the processing and storage of data. To mitigate these security risks, the design of the IoT includes a range of security measures. Authentication and authorization are essential and crucial needs in all stages to mitigate a variety of attacks [4]. As a result, solutions have been proposed that combine various frameworks to improve authentication and authorization, along with AC procedures across IoT devices and users.

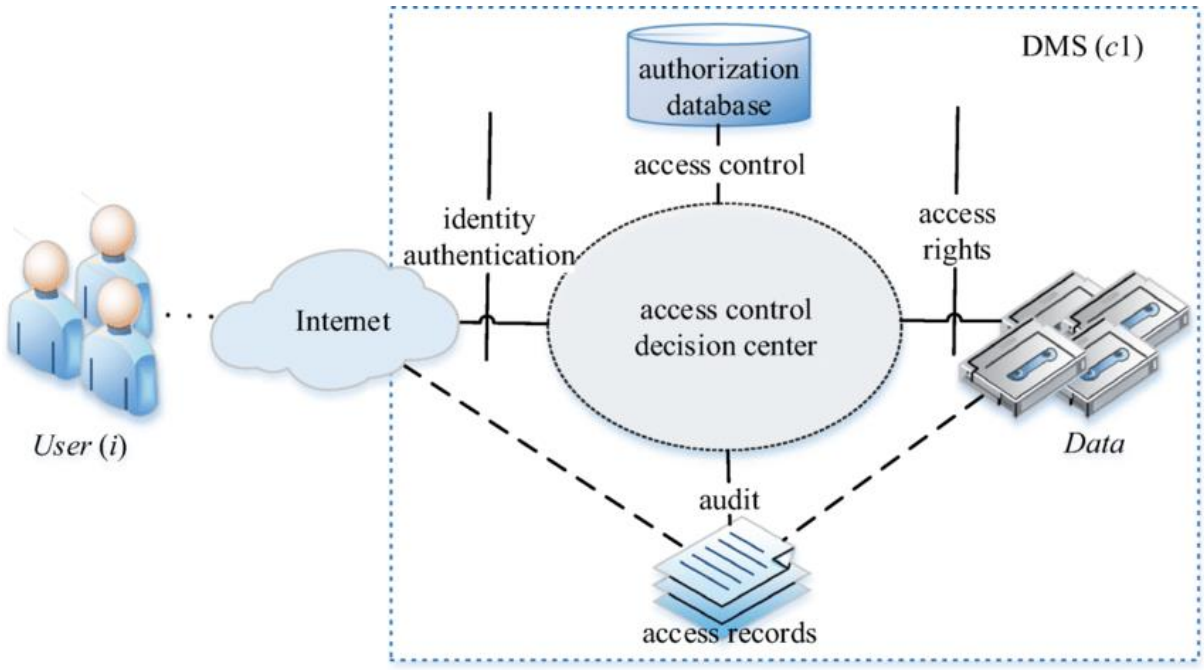

Figure 1: Traditional access control framework in Distributed IoT [5]

Conventional AC systems, which ascertain the entities or entities that can get entry to specific resources, frequently prove inadequate in the extremely dynamic and dispersed nature of IoT environments [6]. Centralized methods sometimes serve as bottlenecks and single points of failure, which makes systems more vulnerable to attacks and decreases their overall reliability. In addition, centralized authentication systems face difficulties in handling the large quantity and variety of IoT devices, resulting in scalability challenges [7]. Decentralized authentication methods, such as blockchain and decentralized identifiers (DIDs), have arisen as potential solutions to these difficulties. Decentralized authentication improves security and resilience against breaches by spreading trust across a network and eradicating the necessity for a central authority (CA). These technologies provide a system of identity management that is unchangeable and can be proven to be true, guaranteeing that only devices that have been verified can take part in the network [7]. The integration of strong AC techniques with distributed authentication seeks to establish a scalable, secure, and efficient framework for safeguarding IoT environments against unwanted access and cyber threats. Although there are potential advantages, there has been limited

Proceedings DOI: 10.21467/proceedings.7.6
ISBN: 978-81-989164-9-5

Series: AIJR Proceedings
ISSN: 2582-3922

exploration of the integration of various methods. This emphasizes the necessity for thorough research to create and assess scalable solutions that are specifically designed for the distinct requirements of IoT contexts.

1.1 Objectives of this study:

To identify and analyze security vulnerabilities and threats specific to IoT devices and networks. To fashion a comprehensive framework for AC and decentralized authentication in IoT devices. To evaluate the performance and scalability of AC mechanisms and decentralized authentication solutions in IoT environments. The subsequent part provides a detailed analysis of previous literature that is highly pertinent to the present study.

2. RELATED WORKS:

The table below provides an elaboration of previous research concerning AC mechanisms and decentralized authentication in IoT devices.

Table 1: Literature Review

AUTHORS AND YEARS	METHODOLOGY	FINDINGS
Ghaffari et al., (2020) [7]	This study examined the present state of blockchain and smart contract deployment in authentication and access control. After introducing AAC and blockchain technology, this study covered distributed ledger technology, access control, and authentication. To better grasp the state of the art, presented a taxonomy to classify existing approaches by kind, application context, and blockchain justification.	The paper's conclusion assessed the method's pros and weaknesses in security, resource usage, and privacy. It also addressed future work.
Da Xu et al., (2021) [8]	This chapter covers AC models and architecture in IoT systems based on recent research on security procedures. Blockchain Enabled, Decentralized, Federated, Capability-based Access Control (BlendCAC) is used to protect devices and services, along with information inside large-scale IoT systems, as a case study.	Experimental results showed that BlendCAC can provide a decentralized, scalable, lightweight, and fine-grained AC solution for IoT devices.

Proceedings DOI: 10.21467/proceedings.7.6
ISBN: 978-81-989164-9-5

Series: AIJR Proceedings
ISSN: 2582-3922

Alshehri et al., (2022) [9]	Through the use of the blockchain (DSA-Block) paradigm, which is capable of performing secure access control and data exchange, this research presented a dynamic, secure access control using the blockchain.	The suggested work achieves a significantly reduced computing overhead of 79%, while the current works Fabric IoT, Blockchain, and TLC-Block have considerably higher computation overheads of 96%, 90%, and 88%, respectively.
Noor et al., (2022) [10]	A structured literature evaluation of 81 publications on access control in IoT and blockchain technology was conducted to examine the issues of centralized access control in safeguarding IoT resources. This paper lays the groundwork for decentralized access control utilizing blockchain technology to secure IoT actuators and sensors in smart farming. A systematic literature review from four databases was conducted between 2018 and 2021 to inform this paper.	The study focused on blockchain technology, access control, key management, and a combination of these strategies. Highlighted are the potential impacts, gaps, methods, evaluation, trends, and challenges of decentralized access control.
Sivaselvan et al., (2023) [11]	This study introduced a novel and robust access control method for the Internet of Things (IoT) that is capable of scaling and ensuring security. By utilizing blockchain as the foundation of trust, the suggested system enables access control for IoT devices without requiring the resource-limited IoT devices to be included inside the blockchain network or store a significant quantity of blockchain data.	The findings showed that the transaction costs for all blockchain transactions are below the suggested gas limit of 3000000 gas. Furthermore, the transaction fees associated with contract functionalities on the Ethereum Mainnet are significantly lower than $3.
Kokila & Reddy (2024) [3]	A full assessment of IoT security challenges and threats is offered. After discussing security challenges, new and established solutions that aim to build trust in IoT applications are discussed.	Machine learning, fog computing, edge computing, and blockchain are among the technologies that enhance IoT's security.

Proceedings DOI: 10.21467/proceedings.7.6
ISBN: 978-81-989164-9-5

Series: AIJR Proceedings
ISSN: 2582-3922

2.1 Research Gap:

The research gap exists in the creation of strong AC mechanisms and decentralized authentication protocols specifically designed for IoT devices, which are frequently susceptible to security breaches due to insufficient security precautions during the design phase. The existing vulnerabilities in security, combined with the personal and sensitive nature of IoT data, highlight the need for immediate and efficient AC solutions. Additionally, the methodology primarily uses a CA for crucial system functions, including setup and key generation. Yet, this approach lacks a hierarchical organizational framework, which is needed for IoT hierarchical key delegation. While this technique prioritizes pre-generated secret keys and AC, it does not thoroughly explore key management. Also, the central authority paradigm ignores multi-authority system benefits, causing scalability along with resilience issues in varied IoT scenarios. This research builds on [12] by creating a decentralized system for hierarchical key management and distribution.

3. METHODOLOGY:

This section introduces the novel framework for the system, meticulously proposed to address the shortcomings revealed in the research gap of this study. The method revolves around combining hierarchical identity-grounded encryption alongside the IOTA framework, which involves transitioning from a CA to a more dispersed and hierarchical structure. The design is essential for the efficient distribution of secret keys and the management of key delegation inside IoT systems. The suggested solution is meticulously designed to tackle the inherent issues in IoT environments, with a specific emphasis on scalability, resource proficiency, and adaptability. So, the system architecture effectively decreases computational requirements by acknowledging the resource constraints of IoT devices alongside data owners (DOs). Unlike the centralized key generation approach, the suggested architecture assigns key functions such as token creation to higher authority levels (lvl.s), which is more suitable for the requirements of Industrial IoT domains. Delegating this task not only reduces the computing burden on DOs but also improves the system's ability to scale and adapt, which is crucial for dynamic IoT networks.

In addition, the suggested system utilizes IOTA for AC management, which is highly skilled in managing the growing count of devices along with users while guaranteeing the immutability and integrity of data. This study utilized IOTA's distributed ledger technology to mitigate vulnerabilities in Industrial IoT circumstances defined by recurrent device interactions and data transfers. This study guarantees data integrity and security by distributing the database over different IOTA nodes. Also, the IOTA Tangle is well-suited for securely managing large amounts of data in IoT systems due to its ability to store encrypted data, tokens, policies, and public keys, along with device serial numbers (DSN), as well as its fast throughput capacity. This complete strategy minimizes potential hazards and facilitates the establishment of safe, unchangeable, and traceable data management inside IoT networks.

Proceedings DOI: 10.21467/proceedings.7.6
ISBN: 978-81-989164-9-5

Series: AIJR Proceedings
ISSN: 2582-3922

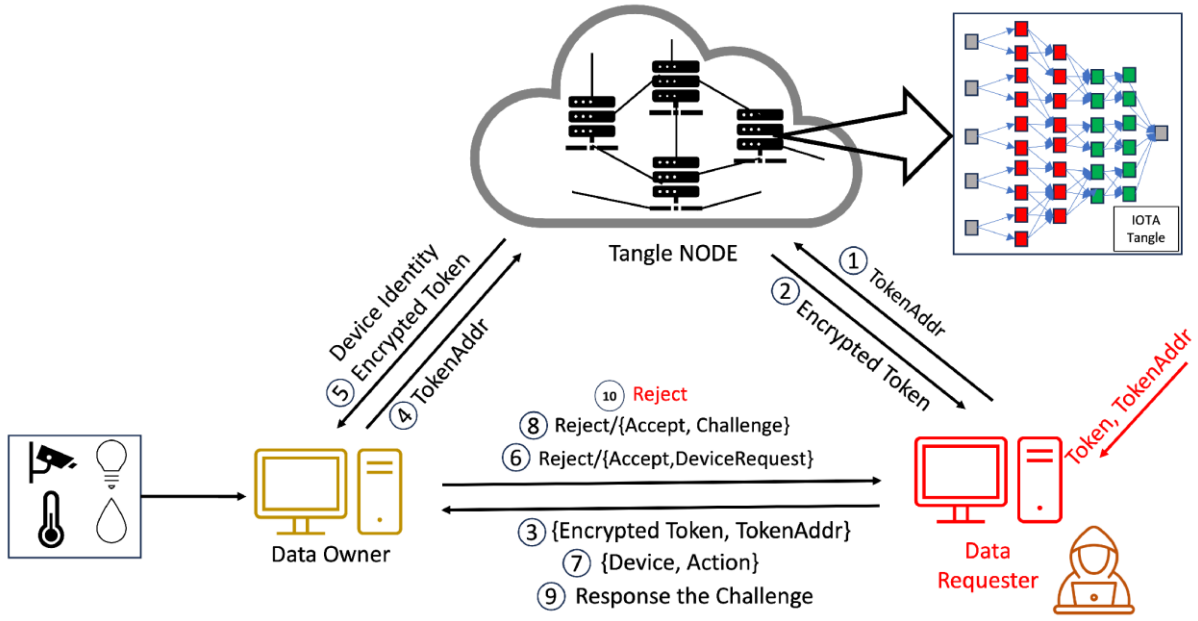

Figure 2: Proposed Methodology

4. RESULTS AND DISCUSSIONS:

The diagram below provides a comparative analysis of the computational expenses related to two important procedures: data encryption (shown in blue) and the ensuing transfer of these encrypted data right to the Tangle. So, the system's working was assessed by monitoring the duration of two crucial processes, access rights (ARs) authorization along with encrypted token upload. The metrics were measured at different levels of hierarchy, specifically Lv0, Lv1, and Lv2, along with Lv3, which indicate rising levels of complexity inside the system's structure.

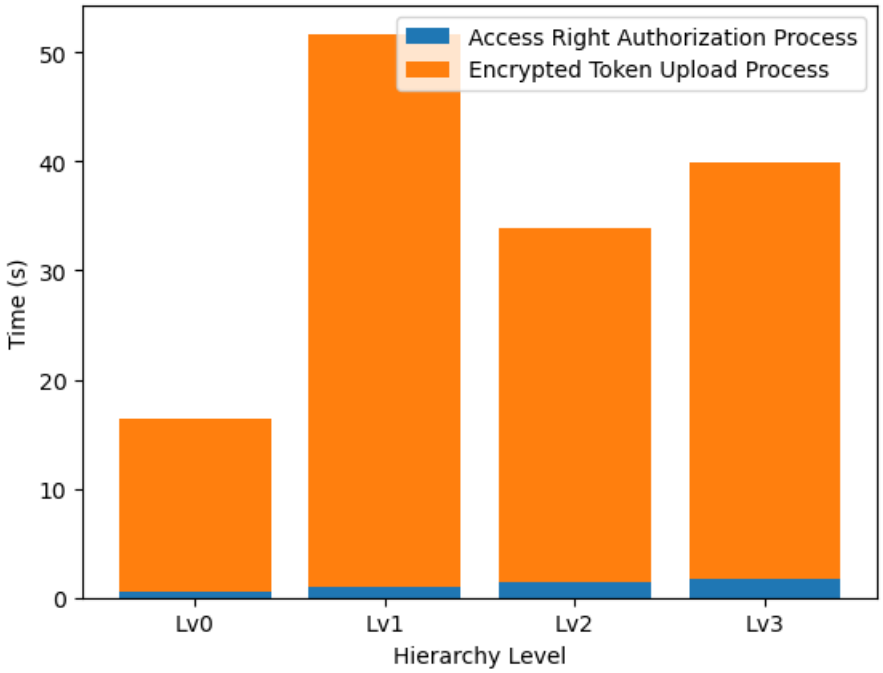

Figure 3: Access rights (ARs) authorization execution times on AWS for hierarchical levels: Lv0 - Lv3.

Proceedings DOI: 10.21467/proceedings.7.6
ISBN: 978-81-989164-9-5

Series: AIJR Proceedings
ISSN: 2582-3922

The encryption durations, depicted utilizing blue, progressively rose as the hierarchy level grew. The time required increased from 0.4949 seconds at Level 0 to 1.7942 seconds at Level 3. The trend observed indicates a direct correlation that demonstrates the increased computational burden associated with each subsequent level. In contrast, the upload times, depicted in orange, displayed a greater degree of variability. Lv1 had a notable increase at 50.6432 seconds. However, Lv2, along with Lv3, showed a decline, with durations of 32.3413 along with 38.1509 seconds, respectively. The observed non-monotonic behavior may be caused by oscillations in the network or variations in system loads throughout the uploading process.

The stacked bars inside the chart provide a clear representation of the total time bearing of both procedures at each level. The procedure of authorizing ARs consistently takes up a significant portion of the entire time. On the other hand, the process of uploading encrypted tokens is less consistent, indicating that it was the main factor causing variations in time across different tiers. To comprehend the impact of system hierarchy on encryption procedures, conducted a time measurement analysis to determine the duration required for ARs authorization directly on two distinct platforms: AWS along with Raspberry Pi 4. Also, the analysis was conducted across four system hierarchy levels, ranging from Lv0 - to Lv3. Also, the Raspberry Pi 4 demonstrated noticeably longer encryption time at every level of the hierarchy than AWS. More precisely, the Raspberry Pi 4 required 260.89%, 264.14%, and 267.85%, along with 257.19% additional time for the encryption procedure likened to AWS at lvl.s Lv0, and Lv1, and Lv2, along with Lv3, correspondingly. The percentages highlight a significant disparity in working across the two systems, with the Raspberry Pi 4 unswervingly taking more than 2.5 longer than AWS to do the identical encryption work.

The diagram below depicts a comparison examination of encryption durations, visually displaying the working of AWS along with Raspberry Pi 4 at different hierarchical levels.

Proceedings DOI: 10.21467/proceedings.7.6
ISBN: 978-81-989164-9-5

Series: AIJR Proceedings
ISSN: 2582-3922

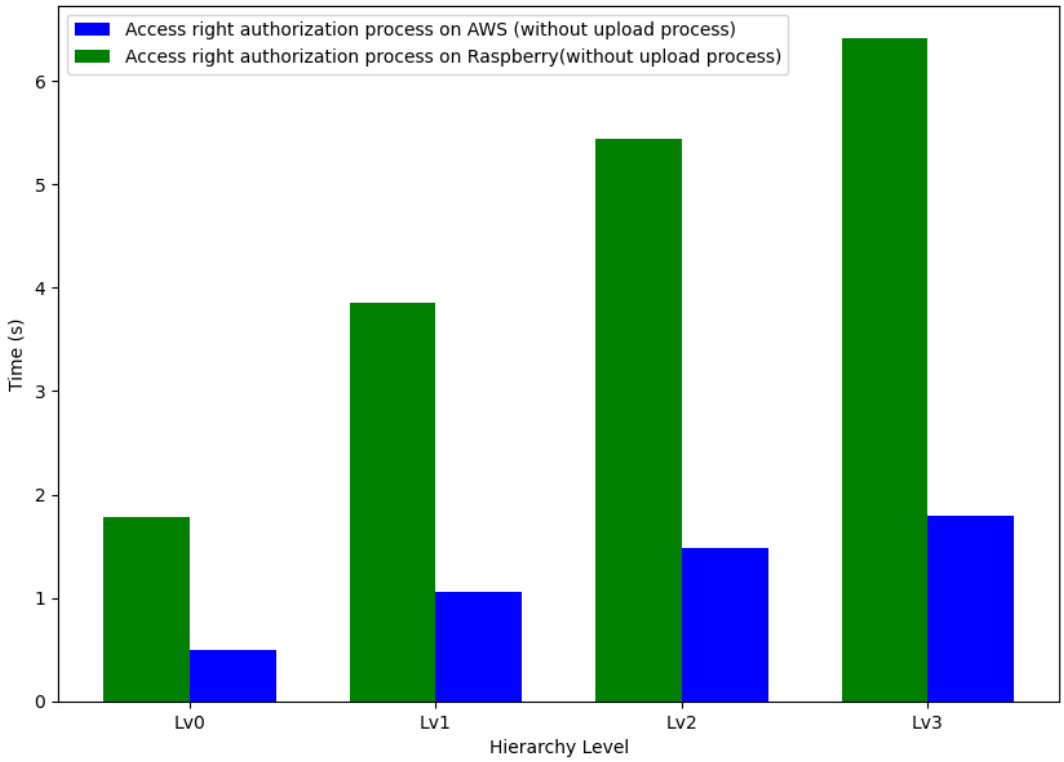

Figure 4: Comparing the execution times of access rights (ARs) authorization between AWS and Raspberry Pi 4.

The findings highlighted the need to improve optimization and refining performance, especially when it comes to establishing AR authorization inside cloud-grounded IoT environments. The IOTA framework protects the availability along with integrity of encrypted tokens by securely storing them, hence enhancing the system's resiliency. The collected data indicates a pressing requirement to improve the upload process, which becomes more crucial as the system expands. The system demonstrates practical feasibility, with negligible changes in operating time likened to Zhang et al.'s [12] methods, namely in ARs' verification procedures, having a minimal deviation of 33.35%. The predictable and manageable increase in authorization time contrasts with the enormous challenges posed by the inconsistent upload times in real-world deployment scenarios. These challenges have the potential to impact the system's total effectiveness along with reliability greatly.

5. CONCLUSION:

A thorough performance evaluation of the proposed system will provide valuable insights into its working efficiency and security resilience. The hierarchical system assessment reveals the scalability hurdles and emphasizes the necessity for platform-grounded optimizations inside IoT environments. Notably, there are substantial differences in execution time between AWS along with the Raspberry Pi 4, chiefly in the processes of ARs' delegation, authorization, and verification. Additionally, it is recommended that a comprehensive examination of the system's ability to withstand prospective security threats and attacks be conducted in future research.

Proceedings DOI: 10.21467/proceedings.7.6
ISBN: 978-81-989164-9-5

Series: AIJR Proceedings
ISSN: 2582-3922

REFERENCES:

[1] U. Khalid, M. Asim, T. Baker, P. C. K. Hung, M. A. Tariq, and L. Rafferty, "A decentralized lightweight blockchain-based authentication mechanism for IoT systems," Cluster Comput., vol. 23, no. 3, pp. 2067–2087, 2020.

[2] J. H. Kang and M. Seo, "Enhanced Authentication for Decentralized IoT Access Control Architecture," Cryptography, vol. 7, no. 3, 2023.

[3] M. Kokila and S. Reddy, "Authentication, Access Control, and Scalability Models in Internet of Things Security-A Review," Cyber Security and Applications, vol. 100057, 2024.

[4] M. El-Hajj, A. Fadlallah, M. Chamoun, and A. Serhrouchni, "A survey of Internet of Things (IoT) authentication schemes," Sensors (Basel), vol. 19, no. 5, p. 1141, 2019.

[5] N. Shi et al., "BacS: A blockchain-based access control scheme in distributed internet of things," Peer Netw. Appl., 2020.

[6] A. K. Malik et al., "From conventional to state-of-the-art IoT access control models," Electronics (Basel), vol. 9, no. 10, p. 1693, 2020.

[7] F. Ghaffari, E. Bertin, J. Hatin, and N. Crespi, "Authentication and Access Control based on Distributed Ledger Technology: A survey," in 2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), 2020.

[8] L. Da Xu, Y. Lu, and L. Li, "Embedding blockchain technology into IoT for security: A survey," IEEE Internet of Things Journal, vol. 8, no. 13, pp. 10452–10473, 2021.

[9] S. Alshehri, O. Bamasaq, D. Alghazzawi, and A. Jamjoom, "Dynamic secure access control and data sharing through trusted delegation and revocation in a blockchain-enabled cloud-IoT environment," IEEE Internet of Things Journal, vol. 10, no. 5, pp. 4239–4256, 2022.

[10] N. M. Noor, N. A. M. Razali, N. A. Malizan, K. K. Ishak, M. Wook, and N. A. Hasbullah, "Decentralized Access Control using Blockchain Technology for Application in Smart Farming," International Journal of Advanced Computer Science and Applications, no. 9, 2022.

[11] N. Sivaselvan, K. V. Bhat, M. Rajarajan, and A. K. Das, "A new scalable and secure access control scheme using blockchain technology for IoT," IEEE Transactions on Network and Service Management, vol. 20, no. 3, pp. 2957–2974, 2023.

[12] Y. Zhang, R. Nakanishi, M. Sasabe, and S. Kasahara, "Combining IOTA and attribute-Based Encryption for Access Control in the Internet of Things," Sensors (Basel), vol. 21, no. 15, p. 5053, 2021.

Proceedings DOI: 10.21467/proceedings.7.6
ISBN: 978-81-989164-9-5

Series: AIJR Proceedings
ISSN: 2582-3922