*Grenze International Journal of Engineering and Technology, January Issue*

# A Blockchain Approach towards Secure IoT Edge Network

Tejasvee Gupta[1] and Dr Hiren B Patel[2]
[1]LDRP Institute of Technology and Research, Kadi Sarva Vishwavidyalaya, India
[2]Principal, Vidush Somany Institute of Technology and Research, Kadi Sarva Vishwavidyalaya, India
Email: tejasveegupta@gmail.com

***Abstract*—The adaptability of IoT is common in everyday life of humankind with the presence of IoT in various sectors like health, supply chain, agriculture, industries and smart home. With its huge footprint in these sectors, the amount of data that it handles may be private data of people, industry data, health records and others is very large. The privacy and security of this data has been of concern for the last few years. The Iot faces this challenge of privacy, security and computational constraints due to the size of Iot devices. Currently, the centralized approach used is unable to address the privacy and security challenges as traditional approaches are not successful with IoT. To overcome the computational constraint Edge computing has paved the way but again fails to solve the privacy and security concerns as it depends on centralized mechanism only. To overcome these challenges, distributed and decentralized approaches are being explored. Blockchain which is known for its decentralized and secure features can be a potential solution to handle the privacy and security challenges due to its features such as immutability, security, transparency and decentralization. In this paper we would like to propose an architectural solution using blockchain with IoT to address the privacy and security concerns.**

***Keywords*— Iot, security, privacy, decentralization, Edge computing, Blockchain.**

## I. INTRODUCTION

The adaptability of IoT has seen huge rise over the past decade. Gartner [1] predicts 50 billion connected devices by 2025. The amount of data on which these devices operate will be enormous.
This is possible because IoT has penetrated into various verticals such as health, supply chain, agriculture, smart homes, etc.
The concerns raised are towards the privacy and security of this data as the device capability of the IoT domain is limited. Also, the traditional centralized mechanism which is currently used are for client-server architecture designed for human computer interaction and not for device to device architecture.
The IoT devices are mobile and dynamic in nature which may create security concerns as traditional centralized mechanisms do not cope with the dynamic nature of devices.
The traditional centralized mechanism has come up with an otp feature as an add-on security measure, but such mechanism does not work with the IoT devices.
The above concerns require a strong access control mechanism for Iot devices. The access control mechanisms are pre-approved rules that decide who gets to control the devices by maintaining an access control list.

*Grenze ID: 01.GIJET.11.1.27_3*

The traditional access control mechanism [2] like mandatory access control(MAC), discretionary access control(DAC), role-based access controlRBAC), attribute based access control(ABAC), authorization based access control(ZBAC) and capability-based access control(CapBAC) were basically designed for centralized architecture and are not a perfect fit for IoT devices. The centralized architecture may also act as a single point of failure and is a single point of attack for hackers. This advice for distributed and decentralized architecture for Iot domain. The Blockchain being known for its secured and transparent feature and a distributed architecture is most suited for the IoT domain. The rest of this paper discusses the various challenges and probable solutions through a thorough literature survey.

The rest of the paper is organized as follows. Section II discusses the related literature in the various research areas. Section III discusses the Access control schemes. Section IV discusses the challenges and solutions using Blockchain technology. Section V is our conclusion followed by Section VI that mentions the various references we have gone through for this research article.

## II. Related Work

As discussed above access control schemes are primarily designed for centralized architectures. To overcome this Ali et al. [3] present how IoT is shifting its computational capabilities from centralized cloud platform towards IoTEdge. However, IoT edge is not able to fulfill the privacy and security concerns of IoT and hence Blockchain is used due to its features like fault tolerance, immutability and transparency that help to solve the security concerns.

As with the increasing number of IoT devices and computation required, it is creating a bottleneck at cloud & results in latency issues. And hence computational capabilities need to be shifted towards the edge of the network. Though edge servers may improve the computation time and reduce latency, still it may not provide complete security as a centralized cloud platform. Blockchain here is a natural fit for the solution due to its efforts of developing trusted and secured decentralized services.

Wang et al[4] discuss how the challenges of IoT, that is scalability and security are solved by Edge computing and Blockchain technology.

They present a framework called Edgechain based on Edge computing and Blockchain for IoT using smart contracts. It uses a credit-based resource management system to control how much resources IoT devices can obtain from edge servers based on predefined rules on priority, application type and past behavior. The solution works for both legacy and non-legacy IoT devices. Legacy IoT devices have resource constraints and cannot implement Blockchain, while non-legacy devices may implement Blockchain.

Wright et al[5] highlight the computational resource limitation in IoT systems and how edge computing solves the computation problem. They propose a solution called SmartEdge: A smart contract for edge computing. They have shown an experimental setup with a single raspberry pi as data node and a powerful desktop as compute node. They implement a computational task to run on the data node itself standalone without an edge node and secondly using smart contracts on the edge node and compare the results to prove the effectiveness of edge computing.

Zhang et al[5] investigated the critical access control issues in IoT. How the traditional access control policies are not suitable for IoT as they rely on a centralized server. Their answer to the solution is Smart contracts of Blockchain. They propose a Smart contract-based architecture to grant access to a subject-object pair. It consists of multiple access control contracts to achieve distributed and trustworthy access control for IoT systems.

Sheg Ding et al[6] also argue on how traditional access control technologies are not a fit for IoT. With the increasing number of intelligent devices, IoT has gained much attention due to its connectivity over the internet. However, in this large network, the access management is complicated and lacks credibility due to centralization. So, the traditional access control technologies are not a fit for resource constrained IoT devices. Their contribution is Novel Attribute-based Access control scheme using Blockchain for Iot. The Blockchain is used to record the distribution of attributes. They use a consortium Blockchain technology.

Maesa et al[7] propose a system that uses XACML technique that is implemented in Bitcoin to announce the resource access rights based on Blockchain technology which enables the decentralized conduct of resource access permits among users.

Cruz aet al[8] also propose smart contract technology to achieve a Role-based access control scheme.

All the above-mentioned work has highlighted the concerns raised due to centralized access control mechanism and how it is unfit for the Iot domain. And how each one of them focus on Edge computing to improve performance and use Blockchain technology to achieve security. Each paper proposes an architectural solution and tries to justify their work with suitable experiments carried out.

## III. ACCESS CONTROL SCHEMES

Following are the access control schemes that work in traditional environments. However, their implementation in IoT with challenges are mentioned below

- Discretionary Access Control (DAC): The technique maintains a static access control list(ACL)[9]. The list is predefined, and access permissions are there forever unless they are manually revoked by manually altering the access control list. The list needs to be checked and updated in IoT as the devices may be added or removed from the network. So, in a dynamic environment DAC is not suitable for IoT networks. Also, as more users enter the network, ACL needs to be updated, so an administrator needs to continuously monitor the permissions for granting or denying access.
- Role-Based Access Control(RBAC): In this scheme also predefined access are granted to resources based on the role defined for a user[10]. But on a scalable and dynamic network the number of roles might increase and may create ambiguity on the roles that a user should be assigned. IoT devices may comprise various functionalities and offer a wide range of services[11], this may cause the administrator to create new roles often.
- Attribute-Based Access Control{ABAC): ABAC is the most successful schemes used in IoT network as it is adding an extra attribute to the roles defined. Various device attributes like device model , device ID, device location may be used as an extra attribute to grant access to the users. Also various projects use this scheme but the centralized architecture on which these schemes are deployed may be complex[12,13].
- Capability-Based Access Control(CapBAC): This scheme uses Policy Decision Point(PDP) and Policy Enforcement Point(PEP) to generate a token when a user requests a resource based on the capability. PDP generates the token and is evaluated by PEP. This was used at the IoT@work project in the European Union[14,15]. The model depends on centralized architecture to issue the certificate or verify the identity of the user.
- Blockchain-Based Access Control (BBAC): The distributed nature of Blockchain has helped it gain popularity in replacing centralized architecture mechanisms in IoT. Also, its features like immutability, transparency, security and privacy may be utilized to address the privacy and security challenges in IoT. BBAC uses two mechanisms mainly, transaction-based and smart contract-based[16]. The transaction-based approach uses the centralized architecture to generate tokens to grant access to requesters. So, most of the proposal work is on smart contract-based access control as mentioned in the above section.

## IV. CHALLENGES IDENTIFIED AND PROPOSED SOLUTION

The challenges that this paper identifies are firstly the resource constrained IoT device, which does not allow to embed strong security algorithms in them, the computation power of these devices is very limited making them dependent on cloud architecture.

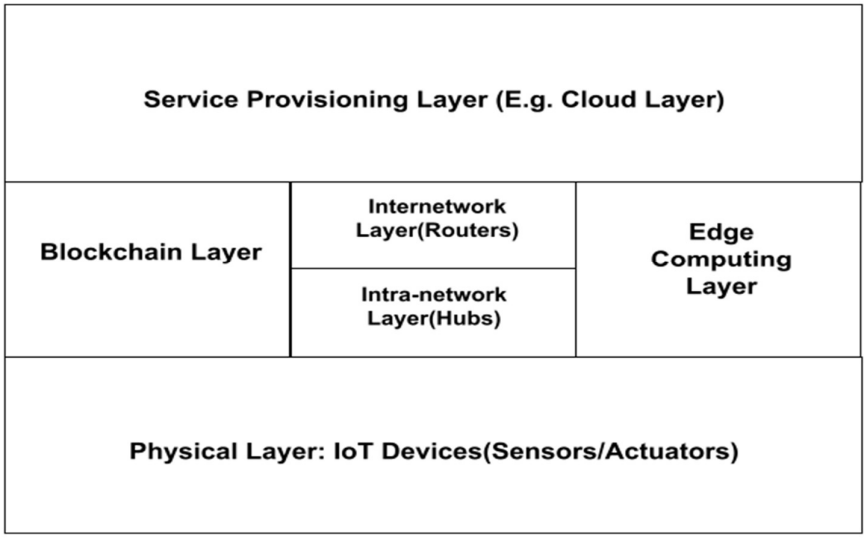


Figure 1. Blockchain embedded IoT-Edge network

And secondly the traditional centralized client-server architecture does not fit the needs of the IoT network. The literature survey shows that researchers are proposing architectural solutions to use Blockchain technology due to its decentralized distributed architecture. We would propose to use an Edge computing layer that would implement Blockchain and smart contracts. This Edge computing architecture will act as an intermediary between IoT devices and Cloud layer. As Edge devices are powerful, they will fulfill the compute constraints of the IoT device as well as the storage requirements providing local support to the IoT device. Bringing compute devices nearer to the IoT devices will improve the performance in terms of throughput, latency and response time. The Blockchain implemented on the edge devices will act as distributed nodes storing the data cryptographically making it secure as well as immutability property of Blockchain guarantee the integrity of data generated by IoT devices. Smart contracts deployed on these Blockchain nodes will manage the access control mechanism making the IoT architecture more secure. The architecture proposed is depicted in figure 1.

## V. Conclusion and Future Work

Based on our exhaustive literature review, we may conclude that the traditional centralized client-server architecture is a misfit for IoT architecture in terms of privacy and security. To overcome the challenges of IoT networks like computation and storage constraints, one may use Edge computing architecture to reduce the latency and improve performance. To overcome the privacy and security challenges, we propose to use a smart contract of Blockchain network embedded in the Edge computing layer as is proposed in the architecture shown. This research may be extended to compare the performance of the said architecture by experimental analysis with and without Blockchain architecture at the Edge layer.

## References


[1] IDC Press Release, The Growth in Connected IoT Devices Is Expected to Generate 79.4ZB of Data in 2025, According to a New IDC Forecast, July 2019.

[2] P. Samarati, and D. Vimercati,“Access control: policies, models, and mechanisms,”In:International school on foundations of security analysis and design, Springer, pp. 137–196, 2000.

[3] M. S. Ali, M. Vecchio and F. Antonelli, "Enabling a Blockchain-Based IoT Edge," in IEEE Internet of Things Magazine, vol. 1, no. 2, pp. 24-29, December 2018.

[4] J. Pan, J. Wang, A. Hester, I. Alqerm, Y. Liu and Y. Zhao, "EdgeChain: An Edge-IoT Framework and Prototype Based on Blockchain and Smart Contracts," in IEEE Internet of Things Journal, vol. 6, no. 3, pp. 4719-4732, June 2019.

[5] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang and J. Wan, "Smart Contract-Based Access Control for the Internet of Things," in IEEE Internet of Things Journal, vol. 6, no. 2, pp. 1594-1605, April 2019.

[6] S. Ding, J. Cao, C. Li, K. Fan and H. Li, "A Novel Attribute-Based Access Control Scheme Using Blockchain for IoT," in IEEE Access, vol. 7, pp. 38431-38441, 2019.

[7] D. D. F. Maesa, P . Mori, and L. Ricci, “Blockchain based access control,” in Proc. IFIP Int. Conf. Distrib. Appl. Interoperable Syst., 2017,pp. 206–220.

[8] J. P. Cruz, Y. Kaji and N. Yanai, "RBAC-SC: Role-Based Access Control Using Smart Contract," in IEEE Access, vol. 6, pp. 12240-12251, 2018, doi: 10.1109/ACCESS.2018.2812844.

[9] Albulayhi, K.; Abuhussein, A.; Alsubaei, F.; Sheldon, F.T. Fine-Grained Access Control in the Era of Cloud Computing: An Analytical Review. In Proceedings of the 2020 10th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 6–8 January 2020; pp. 0748–0755.

[10] Shan, T.L.; Ismail, S.A.; Azizan, A. Access Control Models for Cloud Computing: A Review. In Proceedings of the 2018 2nd International Conference on Telematics and Future Generation Networks (TAFGEN), Kuching, Malaysia, 24–26 July 2018; pp. 155–158.

[11] Ragothaman, Kaushik, et al. ‘Access Control for IoT: A Survey of Existing Research, Dynamic Policies and Future Directions’. Sensors, vol. 23, no. 4, Feb. 2023, p. 1805. DOI.org (Crossref), https://doi.org/10.3390/s23041805.

[12] Ouaddah, A.; Mousannif, H.; Abou Elkalam, A.; Ait Ouahman, A. Access control in IoT: Survey & state of the art. In Proceedings of the 2016 5th International Conference on Multimedia Computing and Systems (ICMCS), Marrakech, Morocco, 29 September–1 October 2016; pp. 272–277.

[13] Servos, D.; Osborn, S.L. Current Research and Open Problems in Attribute-Based Access Control. ACM Comput. Surv. 2017, 49, 65.

[14] Gusmeroli, S.; Piccione, S.; Rotondi, D. A Capability-Based Security Approach to Manage Access Control in the Internet of Things. Math. Comput. Model. 2013, 58, 1189–1205.

[15] Andaloussi, Y.; Ouadghiri, M.D.E.; Maurel, Y.; Bonnin, J.M.; Chaoui, H. Access Control in IoT Environments: Feasible Scenarios. Procedia Comput. Sci. 2018, 130, 1031–1036.

[16] Riabi, I.; Ayed, H.K.B.; Saidane, L.A. A Survey on Blockchain Based Access Control for Internet of Things. In Proceedings of the 2019 15th International Wireless Communications Mobile Computing Conference (IWCMC), Tangier, Morocco, 24–28 June 2019; pp. 502–507.

[17] Zhu, X.; Badr, Y. A Survey on Blockchain-Based Identity Management Systems for the Internet of Things. In Proceedings of the 2018 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), Halifax, NS, Canada, 30 July–3 August 2018; pp. 1568–1573.
[18] Sedgewick, P.E.; de Lemos, R. Self-Adaptation Made Easy with Blockchains. In Proceedings of the 2018 IEEE/ACM 13th International Symposium on Software Engineering for Adaptive and Self-Managing Systems (SEAMS), Gothenburg, Sweden, 28–29 May 2018; pp. 192–193.