**Journal of Information Systems Engineering and Management**
2025, 10(39s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

**Research Article**

# Access Control for Smart Home System using Smart Contracts at Edge Computing devices to enhance Security and Performance

Tejasvee Gupta[1], Dr Hiren B Patel[2]
[1]*LDRP Institute of Technology and Research, Sarva Vidyalaya Kelavani Mandal, India*
[2]*Principal, Vidush Somany Institute of Technology and Research, Sarva Vidyalaya Kelavani*

**ARTICLE INFO**

Received: 12 March 2025

Revised: 10 April 2025

Accepted: 17 April 2025

**ABSTRACT**

The rise of Internet of things technology has been exponential in the last few years. With its wide range of applications like smart home, healthcare and industries it is associated with huge amounts of data generation. The involvement of data that may be private or sensitive has introduced challenges like privacy and security as the most researched challenges. The traditional centralized access control policies are not best suited in IoT inviting decentralized mechanisms. The Blockchain technology intrinsic features help to solve this problem. Also as Blockchain technology involves computing which is also an IoT concern due to latency issues Edge computing fills this gap of bringing computing closer to IoT nodes. As discussed earlier in our research the integration of Blockchain does not quantitatively affect the performance of IoT. As the traditional access control policies like attribute-based access control(ABAC), role-based access control(RBAC) and capability-based access control(CBAC) use centralized mechanisms, custom access control policy for distributed environments is required for IoT. In this research, we propose a hybrid of ABAC and RBAC that is embedded in Blockchain nodes over edge devices to achieve a better access control mechanism than using a traditional single access control model. Features of both role-based and attribute-based access control mechanisms are combined to grant access to IoT devices. Through our experimentation we intend to show that through negligible performance changes that are less than 300 milliseconds delay, we can improve the security in IoT. We say that security is improved as all the transactions of users accessing IoT devices either to retrieve the data or modify the state of the device are passed through smart contracts and logged in Blockchain. Any illegal access to the IoT device is denied and users are penalized.

**Keywords:** Internet of Things (IoT), Edge Computing, Blockchain, Smart Contracts, Access Control, decentralization, security, performance.

## INTRODUCTION

Internet of things(IoT) is a technology that has silently penetrated the life of common people as well as industries. Say it wearable devices for health monitoring or smart healthcare devices, smart home application or Industrial IoT(IIoT), the internet of things has secured its place in various sectors. The sole purpose of IoT is to generate or monitor the data. This data may be personal or sensitive as well as general purpose data like weather reporter or census monitoring. When it comes to private or sensitive data, privacy and security are the challenges of IoT that have been identified by various researchers. Access control is the mechanism to provide privacy and security in IoT technology.

The conventional access control methods like attribute-based access control(ABAC), role-based access control(RBAC) and capability-based access control(CBAC) are commonly used in various technologies[1]. But these technologies are not best suited for IoT systems as they rely on centralized control mechanisms. The centralized architecture may face challenges like data leak, single point of failure or latency issues for IoT technology.

Also the IoT devices are resource constrained like limited power, memory and size making it difficult to embed security solutions in such small devices. Also the latency and performance challenges of IoT has invited the Edge

computing technology to resolve the performance issues. Also a distributed architecture may help eliminate the challenges of centralized architecture. So here Blockchain technology that is known for its distributed, fault-tolerant, immutable and other various features may fill the gap of centralized architecture. As edge computing architecture brings the computing power closer to the IoT node, it may be used as a distributed Blockchain node that will enhance the security features of IoT technologies. Blockchain technology uses the distributed ledger technology making the data immutable that will prevent data from being corrupted. Also, the cryptographic technique used in Blockchain technology makes the data secure.

In our earlier research, we have demonstrated through experimentation that integrating Blockchain with IoT enhances the security as the transactions use smart contracts to gain permission for access to the IoT devices. [Statement on how smart contracts provide security] The smart contracts were loaded into the Blockchain for recording all the transactions and the transactions are immutable. Also the performance of IoT was hardly compromised as compared to IoT systems without Blockchain by increasing the latency by only 300 milliseconds.

The access control mechanism can be embedded in the smart contracts and transactions for IoT devices will need to use these smart contracts for access permission. As the access control policies are shared on Blockchain it would be impossible to manipulate these policies.

In this paper, we propose a hybrid access control policy that uses ABAC and RBAC to create policies that will be stored on Blockchain and will use smart contracts to validate the access to IoT devices based on the access control policies saved on the Blockchain. Section 2 gives a brief explanation on the literature review we carried out. In section 3, we propose our research contribution through architecture, tables and flowchart. Section 4 depicts the experimentation and results of our research work. Finally, in section 5 we conclude our research and state the future work. At the end, we finish our paper by providing the list of references used in this research.

## RELATED WORK

In our earlier research, we have focussed on the challenges of IoT viz. privacy, security, and the computing capacity of resource-constrained IoT devices. The proposed solution to the later challenge was introducing edge computing as suggested in various research. And for the earlier challenges, most research articles propose architectural solutions using Blockchain technology. In this paper, we carried out a literature survey focussing on the access control in IoT and using Blockchain smart contract to embed the access control rules.

Ragothaman et al[2] in their research carried out a comprehensive survey on various Access control methods in Iot, identifying the challenges of deploying the traditional access control mechanism in IoT. Their research points out why the traditional access control methods are not fit for IoT. The authors conclude in their research that due to the heterogeneous nature of IoT devices,on-size-fits-all solutions of access control cannot be applied to IoT and a hybrid and dynamic approach to handle access control in IoT should be chosen, or tailored-fit solution should be developed for IoT domains.Kim et al[3] in their paper highlights the need for a security solution for smart home system. They suggest the use of Blockchain based solutions, but as the existing proof of work(POW) mining algorithm requires high computational power which the IoT devices lack, they propose a lightweight POW algorithm that can be solved by thin IoT devices. Gugueoth et al[4] in their paper identifies the various security threats like access control, ddos attack, impersonation, eavesdrop attack and routing attack. These attacks may lead to leakage of private data in IoT. The potential solution can be implementing Blockchain with IoT. Their research concludes that Blockchain can be a probable solution to handle the security and privacy issues and highlights the challenges that may be faced in integrating Blockchain with IoT. Chukwu and Ayorinde in [5] also highlight the challenges of IoT using centralized authority for computing and storage that may be hampered by single-point-of-failure. Hence they in their article compare the different Blockchain models like public, private and consortium Blockchains and conclude that consortium Blockchains may be best suited with Iot to solve the privacy and security challenges. Albulayhi et al[6] highlights the ineffectiveness of centralized models in IoT when huge data will be generated due to the exponential growth of Iot. They propose a light-weighted Blockchain integrated Iot solution to handle the Iot data effectively. Their proposal uses a single smart contract and simple publish/subscribe data transaction model to keep the system light-weighted. In their experimentation they use a simulation tool as an Iot device, a node-js script working a gateway interface and ethereum platform for Blockchain technology. The results conclude minimum latency after

Journal of Information Systems Engineering and Management
2025, 10(39s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

integrating Blockchain technology with IoT. Zaidi et al[7] in their research highlight the overhead created on centralized access control models and conflicts due to same role users trying to access various devices with increasing numbers of users and devices. They propose a framework implementing Blockchain and smart contract along with fabricated role-based access control on a hyperledger fabric framework. Through their experimentation they achieve better response time in comparison to SoD. Merlec et al[8] in their research propose a smart contract-enabled context aware access control for Blockchain enabled Iot. Their work identifies contextual information like user profile, date, time, location, resource to make access control decisions written in smart contracts that enforces access control policies and grants access to only authorized users. It uses the consortium Blockchain model eliminating the need for traditional centralized authority. The implementation is carried out on Hyperledger Besu Blockchain. Moosavi et al[9] in their research review the use of Blockchain for security challenges by various researchers in their work. They present a systematic study of consensus mechanisms, smart contract usage and Blockchain integration with other software. They conclude that Blockchain may be most suited with Iot to overcome the security challenges. They also cite the drawbacks of using Blockchain technology with IoT viz latency and power consumption. A probable solution may be using POA(proof of authority) consensus technique to reduce power consumption, and sharding to reduce latency. Zhang et al[10] in their research identify the need for a stronger security solution for smart home networks due to the exponential growth of the smart home industry that may generate huge amounts of private data. They propose a smart home access control system using Blockchain technology. They use smart contract based access control mechanisms with hybrid access control models based on ABAC.

The above research all focuses on none other than one goal: security of private and sensitive data in IoT through Blockchain. All of the above research also highlights the challenges of integrating Blockchain with Iot and the latency issues of IoT. The latency issue can be solved with Edge computing and implementing Blockchain on Edge devices will also take the overhead of computing power needed for Blockchains. As well as using well designed access control schemes that can be written as smart contracts will secure the manipulation of access control policies.

## METHODS

In our earlier research, we proposed an architecture where Blockchain and smart contracts are to be embedded on edge computing nodes. These nodes are distributed in nature and by putting the smart contracts on these nodes, we tend to avoid a single point of failure which happens in a centralized mechanism. This would bring computing of Blockchain also closer to IoT edge nodes as well as the transaction latency will also be reduced. Through experimentation, we concluded that the performance is barely affected when we introduce Blockchain in IoT in presence of Edge nodes.

In this research, we propose to use a hybrid access control policy based on RBAC and ABAC. We embed the access control policies in smart contracts to make access control decisions. As shown in Fig 1, the smart contracts holding the access control rules and policies are stored over the Blockchain network. Whenever a user requests for access to an IoT device, a tuple <User ID, Device ID, Command> is created (Table 1) and passed as a transaction in Blockchain. The edge device creates another tuple <Time Stamp, Group ID> (Table 2) and calls the smart contract with access control policies. Based on the result (Grant/Deny) from smart contract, the transaction is updated in Blockchain as a log and the user either gets a successful transaction or failed attempt. In case of a success, IoT sends an acknowledgement and status of the device is updated on the user side. The IoT device and user registration is very crucial for access control rights. The registration of both the cases happens as explained.

### User Registration

1. Users may register themselves by using their mobile numbers that become their user ID (Table 1).
2. Users may be owners of smart homes or just a sub user like a family member or guest.
3. In the case of smart home owners, users will have to create their smart homes (Table 3) and rooms for their homes. By default, they become the super owners of their home and they may add/remove other sub owners like family members, house help, etc.
4. Smart home owners are only allowed to add devices in the system by registering them.

**Journal of Information Systems Engineering and Management**
2025, 10(39s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

**Research Article**

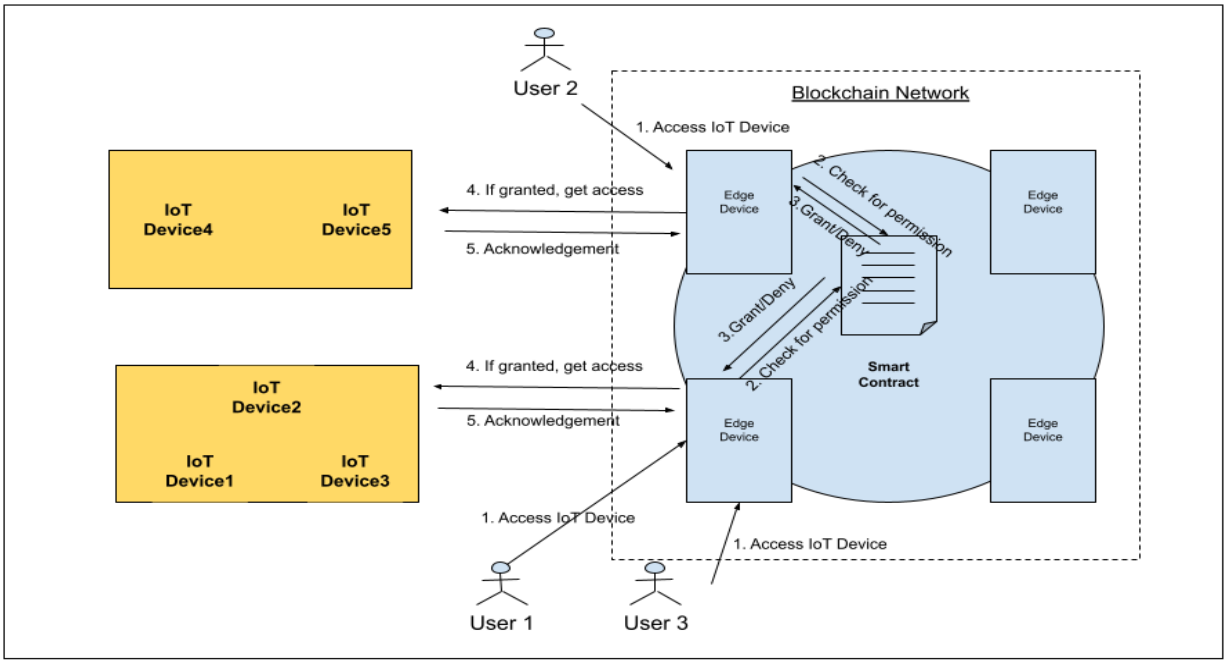


**Fig 1: Proposed Smart Home Scenario.**

| User ID | User Name | Password | Timestamp |
|---|---|---|---|
| 942xxxxx27 | Tejasvee | 123456 | 1702625900 |
| 832xxxxx16 | Goldy | 777777 | 1702712300 |
| 960xxxxx63 | Hardik | 999999 | 1702798700 |

**Table 1: User Master**

**Device Registration**

1. A device master table will store the details of the devices added in the smart home system(Table 2 Device Master).
2. Devices can only be added/removed in the system by smart home owners or super owners.

The traditional RBAC model uses a coarse grained access control for Iot as RBAC assumes that the roles can be classified cleanly. Though it helps to eliminate the role of a centralized admin to verify the users each time, but when a better fine grained system has to be built as in case of IoT where time or the number of times a device can be accessed by a user, RBAC fails to provide the necessary mechanism. Whereas in ABAC, the attributes to be defined for the objects may be heterogeneous in Smart Home applications as there are various different appliances and devices to be controlled. A uniform set of attributes does not fit for all the devices when the number of devices increases.

| Device ID | Smart Home ID | Group ID | Device Detail | Label | Timestamp | Allowed Users |
|---|---|---|---|---|---|---|
| Fan001 | 942xxxxx27_SH01 | 942xxxxx27_SH01_BR_01 | Fan | Fan1 | 1702885100 | {User_ID1, User_ID2,...} |
| AC002 | 832xxxxx16_SH01 | 832xxxxx16_SH01_DR_01 | AC | AC 1.5 | 1702895900 | {User_ID1, User_ID4,...} |

**Table 2: Device Master**

**Journal of Information Systems Engineering and Management**
2025, 10(39s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

**Research Article**

| Smart Home ID | User ID | Label | RoomsLabel:RoomID | Timestamp |
|---|---|---|---|---|
| 942xxxxx27_SH01 | 942xxxxx27 | MyHome01 | {Master_Bedroom:942xxxxx27_SH01_BR_01, Kitchen:942xxxxx27_SH01_KR_01} | 1702863500 |
| 832xxxxx16_SH01 | 832xxxxx16 | MyHome01 | {Drawing_Room:832xxxxx16_SH01_DR_01} | 1702867100 |

**Table 3: Smart Home Master**

Thus we propose a hybrid model consisting of RBAC and ABAC, roles and attributes mentioned in Table 4(Access Control Role and Attribute Master) are used to assign roles to different user ids for different smart homes. A Role Grant master table will decide who may assign roles to whom(Table 5: Role Grant Master). We may further fine grain the access control by adding a token which will be generated upon device request by a user and will be expired upon successful completion. As that is out of scope of our work at this time, we have included it in the future scope of our work, so that our work may be extended by a more fine grained approach.

| Access Control | |
|---|---|
| **Role-based** | **Attributed-based** |
| • Super Owner<br>• Owner<br>• Family Members (Adult)<br>• Family Members (Minor)<br>• Maid / Help<br>• Security<br>• Guest | • Device ID<br>• User ID<br>• Command<br>• Time |

**Table 4: Access Control- Role and Attribute Master**

| Role Granting Authority | Role Gaining Authority |
|---|---|
| Super Owner | Owner |
| Owner | Family Members |
| Family Members (Adult) | Maid |

**Table 5: Role Grant Master**

As we also propose a penalty for users who are defaulters and trying illegal access to devices and are denied access. Each smart home owner gets virtual currency as and when he registers a smart home and adds devices. Let say 200 currencies, and each transaction costs 10 currencies. So when a smart home owner adds users to access their smart home , he lends them say 20 currencies for t hours time. If the user doesn't access the smart home or make a transaction the currency is automatically returned back to the smart home owner. If the user makes successful attempts, then also 10 currencies are going into the smart home owners account. But upon failed transactions or illegal access requests the currencies are deducted as well as the smart home owner is notified. The owner may also revoke the access permission as well as the access control mechanism also applies a penalty over repeated deny requests. This may also be considered as a token used in capability based access control which is valid for a limited period of time. The penalty system used prevents DDOS attack and token system prevents the MITM attack making our system proof to both kinds of attacks. Table 6 shows the feature comparison of our proposal with other research proposals.

Journal of Information Systems Engineering and Management
2025, 10(39s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

| Other proposals | ABAC | RBAC | CBAC | Distributed Access control | Scalability | DDOS proof | MITM proof |
|---|---|---|---|---|---|---|---|
| **Zhang** | No | No | No | Yes | NA | Yes | No |
| **DABAC[12]** | Yes | No | No | Yes | No | Yes | No |
| **Bouras[1]** | No | No | Yes | Yes | Yes | Yes | No |
| **Our Proposal** | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

**Table 6: Feature Comparison**

The stakeholder master table(Table 7) is maintained to assign access to devices. This table stores the access to each device by various users. A User ID may have different roles for different Smart Home IDs as shown in Table 7(Stakeholder Master).

| Role | Smart Home ID | User ID | Device ID | Group ID |
|---|---|---|---|---|
| Super Owner | 942xxxxx27_SH01 | 942xxxxx27 | Fan001 | 942xxxxx27_SH01_BR_01 |
| Owner | 942xxxxx27_SH01 | 832xxxxx16 | Fan001 | 942xxxxx27_SH01_BR_01 |
| Family Member | 942xxxxx27_SH01 | 960xxxxx63 | Fan001 | 942xxxxx27_SH01_BR_01 |
| Super Owner | 832xxxxx16_SH01 | 832xxxxx16 | AC002 | 832xxxxx16_SH01_DR_01 |

**Table 7: Stakeholder Master**

The flow of the system is shown in Figure 2. Whenever a user makes a request to a device, the system checks if a valid user id has made a request. Upon validating the user, the device to be operated is validated and the smart contract to make the access control decision is called. If the user is permitted to access the device the permission is granted and the transaction is executed.

## EXPERIMENTATIONS & RESULTS

We conduct experimentation in 2 scenarios. In scenario1, we implement traditional IoT mechanisms without using Blockchain and smart contracts. And in scenario 2, we conduct the experimentation by implementing Blockchain smart contracts with IoT as per our proposed architecture. For both the scenarios the results of the latency is compared to discuss the performance of both the systems and is mentioned in Table 8.

**Journal of Information Systems Engineering and Management**
2025, 10(39s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

**Research Article**

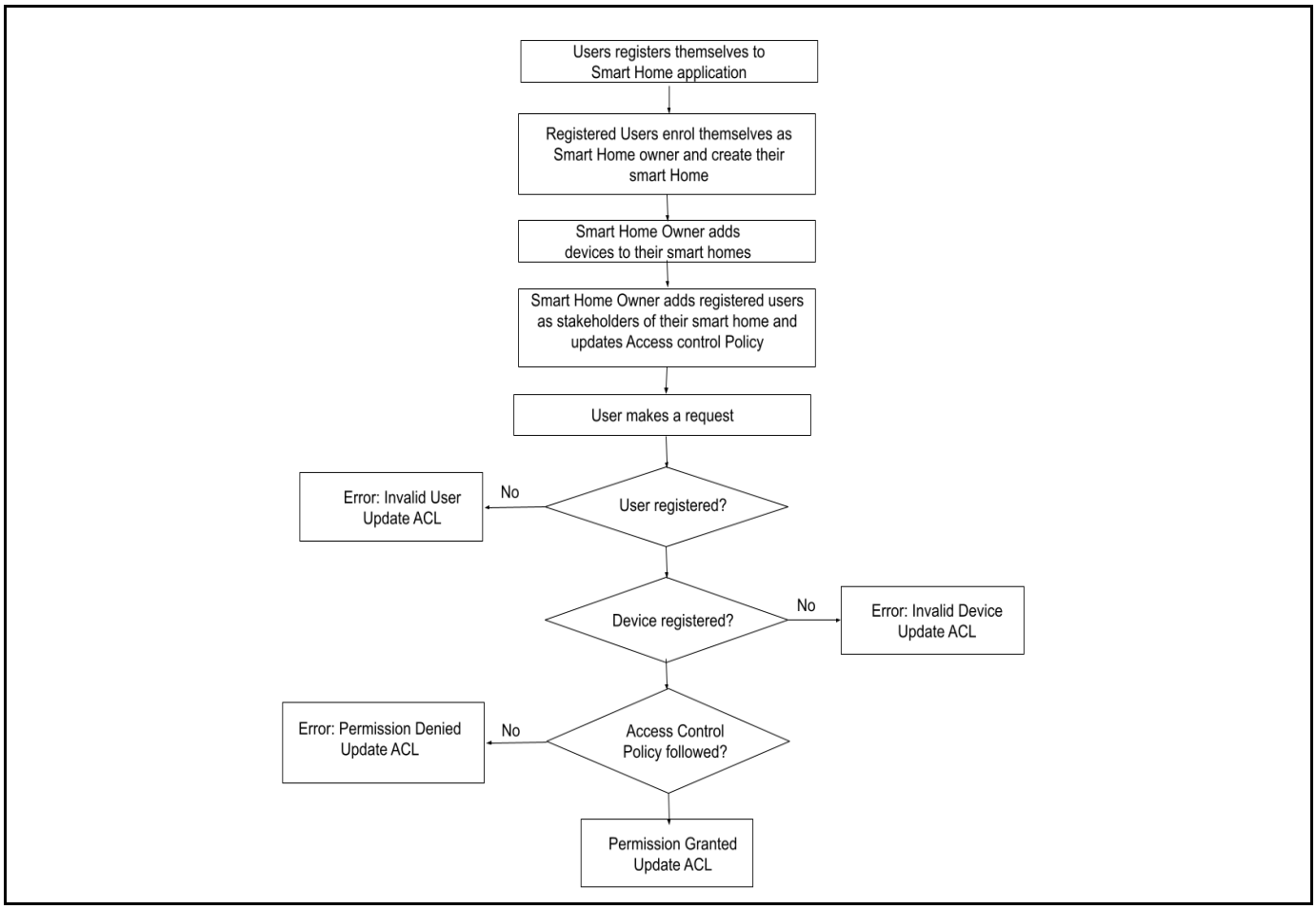


**Fig 2: System Flow**

The hardware and software tools that we used are: an ESP8266 NodeMCU to be used as a smart IoT device, a Cloud mqtt broker on EMQX Cloud MQTT (public MQTT broker viz. broker.emqx.io), ParamShavak supercomputer as the cloud server for Smart Home backbone, a laptop workstation working as an IoT Smart Home user interface to access IoT devices. For Blockchain smart contract implementation we use another laptop workstation working as an edge device and a Blockchain node. Truffle tool to implement Ethereum Blockchain network.

| | **Latency (ms) (only1 active user)** | **Latency (ms) (8 active user)** | **Latency (ms) (16 active user)** |
|---|---|---|---|
| Scenario 1 | 539 | 549 | 554 |
| Scenario 2 | 599 | 608 | 607 |

**Table 8: Performance Results**

The user case of Smart home that we are using is a smart switch board that can be triggered to switch on or switch off the Fan or AC of the room upon receiving the command from the user. The user initiates the command to manipulate the status of the device(Fan or AC), after checking the permission from the access control list, the access is granted or denied. For both the cases of valid and invalid access the experimentation is done and the response time is measured for performance comparison. Same experimentation is carried out for both the scenarios. The comparison results in performance is shown in Fig 3. We have also performed scalability analysis to check how our

**Journal of Information Systems Engineering and Management**
2025, 10(39s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

**Research Article**

architecture behaves in case the number of users increases. With exponential growth in the number of users in the system is stable and latency has increased by 10 percent only for our proposal in compared to the traditional centralized IoT network.

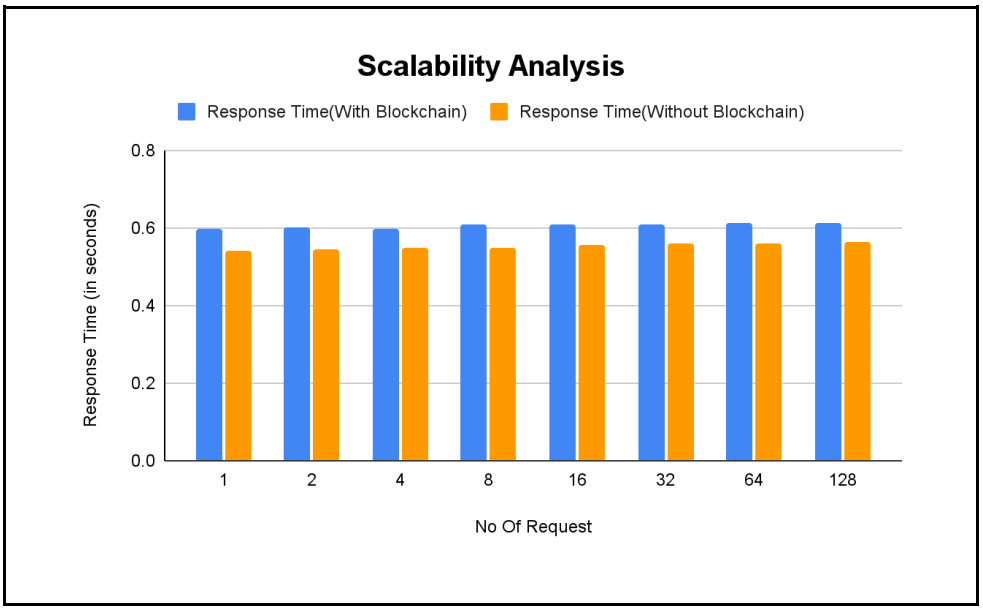


**Fig 3: Scalability Analysis**

Fig 4 shows the storage overhead when the number of participants in the system increases. The size of the shared json file that stores access control information keeps on increasing with the number of participants. Fig 5 shows the performance analysis when the system executes the traditional way without Blockchain in comparison to our proposed architecture with Blockchain.

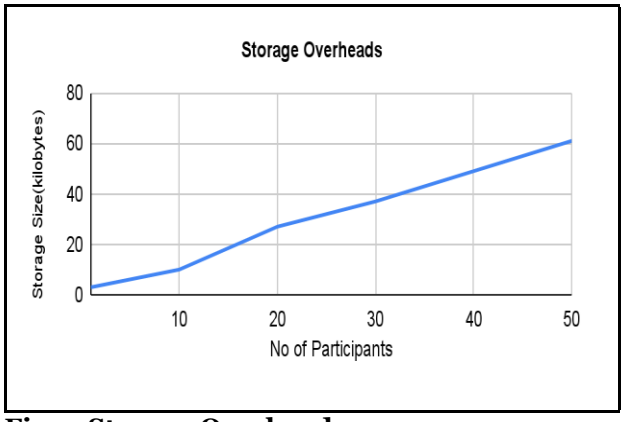


**Fig 4: Storage Overhead**

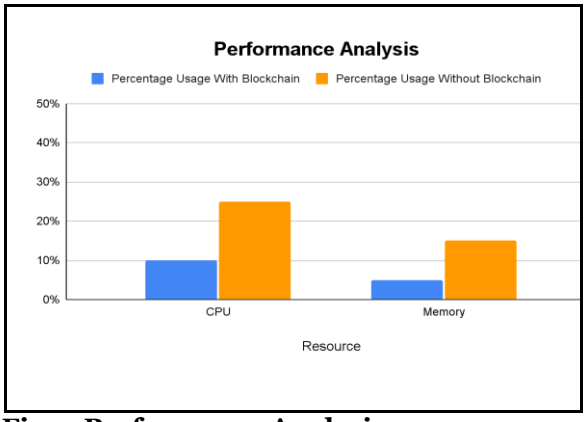


**Fig 5: Performance Analysis**

Fig 6 shows the transaction cost in gas when the access contract is deployed on the Blockchain. As of now, we have implemented only 1 smart contract that is used to grant or deny access to the users for requested devices. The comparison with transaction cost of other proposals from different researchers is shown in the figure. Zhang et al[11] consumes 2543479 gas to deploy the Access Control Contract, 1380781 gas to deploy the Judge Contract and 1559814 gas to deploy the Register contract. Cruz et al[13] uses 1813010 gas to deploy RBAC based smart contracts. Guo et al[12] consumes 1648152 gas to deploy User Management contract, 1440233 gas to deploy Device Management contract and 2060477 gas to deploy Access Control Contract. While our proposal consumes 839205 gas to deploy Access Control Contract.

**Journal of Information Systems Engineering and Management**
2025, 10(39s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

**Research Article**

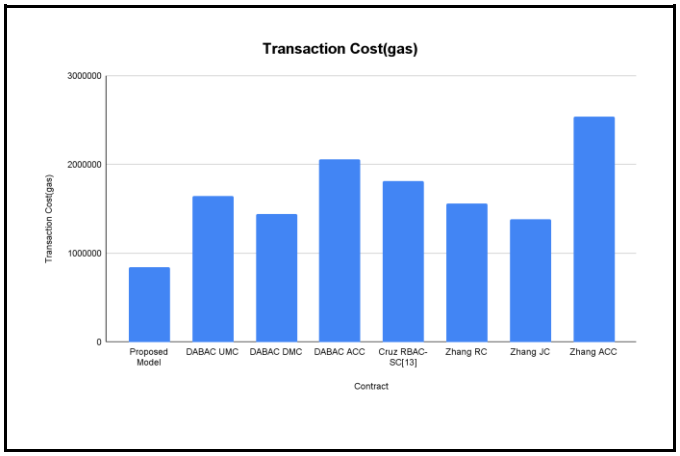


**Fig 6: Transaction Cost**

## CONCLUSION & FUTURE WORK

The work demonstrated in this paper is coarse grained. For a fine grained approach, one can add the capability-based access control approach and use Tokens [Hash: House ID, User ID, Device ID, Permission, Time_From, Time_To]. Token verification is carried out at the local level / edge device for the sake of improving performance. Upon expiration of the token, all such transactions would be stored to Access Control Log in one-go. Penalizing the defaulter trying to access restricted devices by restricting them to initiate a transaction also enhances the security as the DOS attack will be avoided. One may choose any or all of the above approaches to design and implement a fine-grained system.

## REFRENCES

[1] Bouras MA, Xia B, Abuassba AO, Ning H, Lu Q. 2021. IoT-CCAC: a blockchain-based consortium capability access control approach for IoT. PeerJ Computer Science 7:e455 https://doi.org/10.7717/peerj-cs.455.
[2] Ragothaman, K.; Wang, Y.; Rimal, B.; Lawrence, M. Access Control for IoT: A Survey of Existing Research, Dynamic Policies and Future Directions. Sensors 2023, 23, 1805. https://doi.org/10.3390/ s23041805.
[3] D. Kim and J. Lee, "A Reverse Hash Chain Path-Based Access Control Scheme for a Connected Smart Home System," in IEEE Consumer Electronics Magazine, vol. 10, no. 1, pp. 93-100, 1 Jan. 2021, doi: 10.1109/MCE.2020.3031064.
[4] Gugueoth, V., Safavat, S., Shetty, S., & Rawat, D. (2023). A review of IoT security and privacy using decentralized blockchain techniques. Computer Science Review, 50 , 1-16, Article 100585. https://doi.org/10.1016/j.cosrev.2023.100585.
[5] Chukwu, Chuka & Ayorinde, Olumuyiwa. (2022). Blockchain Technology for IoT Security in Smart Homes. 10.13140/RG.2.2.30777.65128.
[6] Albulayhi, A.S.; Alsukayti, I.S. A Blockchain-Centric IoT Architecture for Effective Smart Contract-Based Management of IoT Data Communications. Electronics 2023,12,2564. https://doi.org/ 10.3390/electronics12122564.
[7] T. Zaidi, M. Usman, M. U. Aftab, H. Aljuaid and Y. Y. Ghadi, "Fabrication of Flexible Role-Based Access Control Based on Blockchain for Internet of Things Use Cases," in IEEE Access, vol. 11, pp. 106315-106333, 2023, doi:10.1109/ACCESS.2023.3318487.
[8] M. M. Merlec and H. P. In, "SC-CAAC: A Smart Contract-Based Context-Aware Access Control Scheme for Blockchain-Enabled IoT Systems," in IEEE Internet of Things Journal, doi: 10.1109/JIOT.2024.3371504.
[9] Moosavi, N.; Taherdoost, H. Blockchain Technology Application in Security: A Systematic Review. Blockchains 2023,1,58–72. https:// doi.org/10.3390/blockchains1020005.
[10] Wentai Zhang and Huaizhi Yan 2021 J. Phys.: Conf. Ser. 1971 012049 DOI 10.1088/1742-6596/1971/1/012049.
[11] 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.

**Journal of Information Systems Engineering and Management**
2025, 10(39s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

**Research Article**

[12] F. Guo, G. Shen, Z. Huang, Y. Yang, M. Cai and L. Wei, "DABAC: Smart Contract-Based Spatio-Temporal Domain Access Control for the Internet of Things," in IEEE Access, vol. 11, pp. 36452-36463, 2023, doi: 10.1109/ACCESS.2023.3257027.

[13] Cruz, Jason Paul & Kaji, Yuichi & Yanai, Naoto. (2018). RBAC-SC: Role-based Access Control using Smart Contract. IEEE Access. PP. 1-1. 10.1109/ACCESS.2018.2812844.