International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v11i5.6604
***Article Received**: 22 February 2023 **Revised**: 29 March 2023 **Accepted**: 18 April 2023*

Blockchain-Empowered Security Enhancement IoT Framework in Building Management System

Uma Tomar[1], Dr. Parul Gandhi[2]
[1]Research Scholar-FCA
Manav Rachna International Institute of Research and Studies Faridabad, Haryana, India Uma.tomar@gmail.com
[2]Professor-FCA
Manav Rachna International Institute of Research and Studies Faridabad, Haryana, India
Parul.fca@mriu.edu.in

Abstract — Centralized architectures, like the cloud model, have their advantages, but they also come with drawbacks, such as higher upfront costs, longer deployment times, and a higher probability of catastrophic failure. Building Management Systems (BMS) is an application that can adopt Internet of Things (IoT) designs and services. However, implementing IoT in a highly modular environment with various moving parts and interdependencies between stakeholders can create security issues. Therefore, this paper proposes a system design using Blockchain technology as a means to protect and control the system, which includes the integration of IoT and BMS technologies. This paper has also included broad discussion on current Blockchain based IoT solution and its IoT limitations in Building Management Systems.

Keywords - Building Management System, Catastrophic failure, Decentralized platforms, IoT, Blockchain technologies**.**

I. INTRODUCTION

All The Internet of Things (IoT) is a concept that refers to the interconnection of all kinds of devices with the Internet. IoT is expected to have a significant impact on our daily life in the near future. The IoT has been around for quite some time now, but it has only recently started to gain momentum and become more mainstream. In recent years, we have seen an explosion in the number and variety of devices that are being connected to the Internet at any given moment. New possibilities and risks have emerged in the digital ecosystem as a result of the increased integration of IoT and digital technologies into the smart city environment (Hämäläinen, M., 2020). However, buildings are the lifeblood of every city, and it only seems sense that they would play a major part in the ecologies of smart cities. The information about a building obtained through Building Information Modelling (BIM) can serve as the foundation for IoT platforms and services in the integrated digital ecosystem, supplementing the smart devices and services. These are already present in smart cities along with combined data that are collected through intelligent applications. The architecture of integrated BIM and IoT technologies may have security vulnerabilities that might be remedied by using Blockchain technology (Nguyen, D. C. *et al* 2020)

A. Aim

This research aims at analysing the effectiveness of Blockchain-empowered security enhancement IoT framework in Building Management System Applications.

Objectives

- To examine why Blockchain is so important for Internet of Things (Io T) safety, privacy, connectivity, and administration (Torky and Hassanein, 2020).
- To analyse the current barriers of BMS integrated construction projects.
- To analyse the effectiveness of Blockchain in similar applications or sensor networks in Building Management System.

B. Research Significance

This paper will discuss Blockchain-enabled IoT security improvement in Building Management System Applications. The author has discussed IoT solution limitations, Blockchain and IoT applications, Blockchain's IoT device integration benefits, and covers questions like Why Blockchain-Based IoT Integrated Framework, and Value Realization. However, major limitation of this research paper includes inadequate field- based data and information safety regarding the effectiveness of BMS system in the workplace. This is because this research is completely based on secondary data.

II. LITERATURE REVIEW

This paper will discuss Blockchain-enabled IoT security

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v11i5.6604
***Article Received**: 22 February 2023 **Revised**: 29 March 2023 **Accepted**: 18 April 2023*

improvement in Building Management System Applications. The author has discussed IoT solution limitations, Blockchain and IoT applications, Blockchain's IoT device integration benefits, and covers questions like Why Blockchain-Based IoT Integrated Framework, and Value Realization. However, major limitation of this research paper includes inadequate field- based data and information safety regarding the effectiveness of BMS system in the workplace. This is because this research is completely based on secondary data.

C. Qos MANAGEMENT SYTEM IN IoT ENVIRONMEN

This paper will discuss Blockchain-enabled IoT security improvement in Building Management System Applications. The author has discussed IoT solution limitations, Blockchain and IoT applications, Blockchain's IoT device integration benefits, and covers questions like Why Blockchain-Based IoT Integrated Framework, and Value Realization. However, major limitation of this research paper includes inadequate field- based data and information safety regarding the effectiveness of BMS system in the workplace. This is because this research is completely based on secondary data

. $\frac{\Sigma_{I=1}^{t \cdot x \cdot COuni}}{tx \cdot count} < 1 m_{in}$ ..... (1)

It shows the satisfied constraints of implementing the Blockchain in Building Management Application System. This whitepaper gives an overview of a framework that would use blockchain technology, a decentralized technology, for the access control of Internet of Things in order to meet the need for more workable solutions. The main benefits of implementing blockchain technology are increased transparency, increased security, enhanced traceability, increased efficiency, decreased costs, and lack of involvement from third parties. Since blockchain allows for the movement of data in a trustless way, it may be useful for IoT due to its immutability, auditability, and accountability.

$$\frac{\sum_{j=1} \Sigma_{i=1} e_i}{12} < 5 \quad \text{.....(2)}$$

With the help of this fragment of equation (2), the certain time-interval has been discussed. Having the transaction

history recorded in the Blockchain and kept by all of the nodes makes for a highly auditable system. Reliability, security, accountability, and scalability are just some of the areas where the decentralized nature of Blockchain might help the Internet of Things (Patil *et al.* 2021).

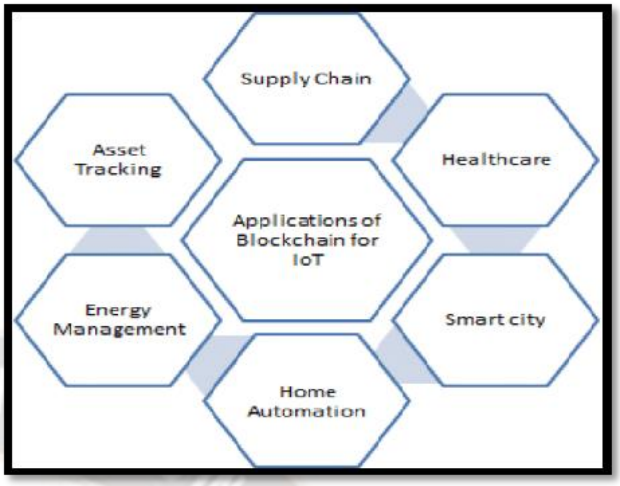

Fig1: Application of Blockchain for IoT
(Image source:Patil et al.2021)

D. LIMITATION OF CURRENT IoT SOLUTION

In the IoT, data cannot be trusted completely outside of the domain of the data owner since there is no way to know for sure that it is not manipulated before being shared, sold, or used for the profit of other parties(Huang et al. 2019). All IoT devices tend to be smart as they make decisions on own or from a central control unit but never from the user itself.

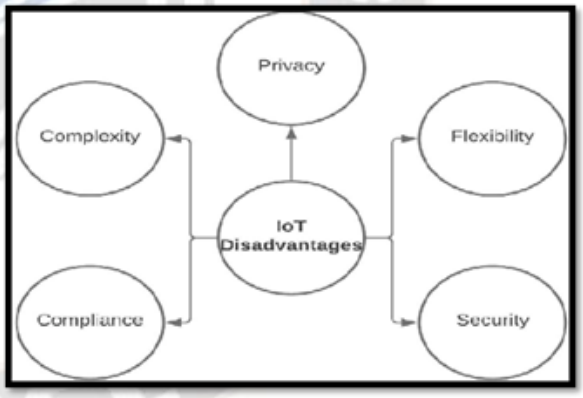

Fig 2: Limitation of IoT
(Image source: Kollolu, 2020)

E. THE SMART CONTRACT FOR MANAGING AUTHORISED AGENTS

Blockchain's distributed ledger and verifiable transactions make IoT integration promising. This aids access control. This schematic depicts how blockchain-based access control may be implemented for IoT gadgets. This smart agreement form is used to control the participants in each subset in order to prevent confining management authority to a single organization. Blockchain-based IoT access control solutions solved the problems of resources planning, access rights transfer, permission compliance, attribute management, and

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v11i5.6604
***Article Received**: 22 February 2023 **Revised**: 29 March 2023 **Accepted**: 18 April 2023*

scalability (Sun *et al.* 2021). The actions include the additions, deletions, and replacements of agents, all of which must be done after the shared nodes have completed their agreement process. This kind of arrangement has one subspace connected to each of them. Figure 2 also summarises few limitations of IoT. IoT devices' limited battery, memory, and processor power need resource management. Transferring access rights means transferring control permissions. Enforcing edge IoT device access control delegation requires such fetch of such permissions (Xu *et al*. 2018). IoT systems also need custom permission enforcement. Access control systems must handle policy flexibility, given IoT system unpredictability and attribute management which is equally critical. Attributes may manage entity identification (ambiguity in observations from physical and digital data) at scale without a distinct concrete identity. Finally, owing to the resilience and dynamicity of data and resources, especially for edge IoT/fog nodes, IoT access control must be scalable (NOVO,2018)

F. ADVANTAGE OF BLOCKCHAIN AS A CENTAL BLOCKCHAIN HUB

Blockchain technology may be the answer to the privacy and trust concerns that have plagued the Internet of Things (IoT) (Ahamad *et al.* 2022). Each community Caricom in the networked structure is defined, for instance, a subspace for connecting different service categories. Internet of Things businesses need a panacea, and Blockchain technology delivers one. It might be used to keep track of the many devices that are now linked to one another, which would help with managing finances and bringing everyone closer together. Working in the Internet of Things sector will benefit greatly from these price cuts. Each subdomain operates independently and is linked to a main centre. The suggested design, which comprises of decentralized networks chosen at the outset of the system, has this centre as its most trusted component. It operates a permissionless cryptocurrency that is in charge of preserving QoS security and managing node behaviour across all associated Blockchain subnets. The hub of Blockchain works in a simplest method, it works as a publicly eligible ledger.

$$y^2 = x^3 + ax + b$$

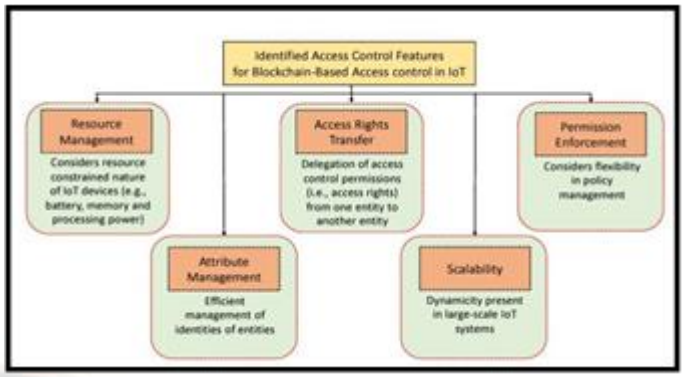

Fig-3, Blockchain-based access control in IoT

To enable the construction of smart buildings, Building Management Systems (BMS) are combined with a control and networking infrastructure made up mostly of smart devices like alarms, cameras, RFIDs, miles, and sensors. Mobile devices and computer-network infrastructure are vital to the Internet of Things. (The IoT applied to autonomous structures) The BMS regulates life-sustaining infrastructure including heating, cooling, electricity, lights, alarms, and sprinklers.

Connected Cameras in smart buildings might potentially exchange information with the IoT (Torky and Hassanein, 2022). To be effective in an IoT context, blockchain-based solutions must be tailored to both the nature of the problem at hand and the nature of the underlying infrastructure in which access control is being deployed. It has been found that Blockchain data is immutable and verifiable, it might be useful in expediting administrative tasks, such as managing who has access to what. Due to the Blockchain's immutability, rogue nodes cannot alter access controls (Hebert and Di Cerbo, 2019). Since all data access and communications between nodes are recorded on the blockchain, compliance with the requirements may be reviewed at any moment. The ledger will record any unauthorized data access or attempted data access, allowing the data's or resource's owner to see and halt any potentially harmful action.

……(3)

The equation y^2 = x^3 + ax + b is an equation in two variables x and y, which defines a type of mathematical object called an elliptic curve. The variables x and y can be any real numbers or complex numbers. Without a central hub, devices might have more faith in the network as a whole. The implementation of cryptographic algorithms inside blockchains has the potential to strengthen the secrecy of users' monetary data (De Moraces Rossetto et al.200). Companies are beginning to

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v11i5.6604
***Article Received**: 22 February 2023 **Revised**: 29 March 2023 **Accepted**: 18 April 2023*

move their emphasis to the actual implementation of Blockchain technology, and during this transition, they have come to the realization that integrating Blockchain technology into already existing business processes or developing a whole new system is not a simple task. In light of this, Building Management Systems (BMSs) are the most suited wager that companies can make. Businesses may benefit from BMSs in two ways: first, by using Blockchain technology; and second, by gaining access to specialised tools built by independent developers to boost the effectiveness of their Blockchain applications. BMSs provide both of these advantages in the form of Decentralised applications (DApps). Combining blockchain technology, which is made possible by the Internet of Things, with properly crafted incentives will push the development of new consumer data management.

G. DEVELOPING QoS ARCHITECTURE IN IoT

Combining Cloud computing, the Internet of Things, and building information modelling might increase potential security threats. When used in any of these contexts, blockchain technology creates an immutable record of transactions that can be accessed and used in the future. The tasks of questioning typically focus on punctuality and serviceability; if a task requires real information, it inevitably obtains the actual data postponement; if a task requires non- real-time data, it worries the accuracy of the data; an assignment for regulation, on the opposite hand, concentrates on punctuality and the accuracy of the data. The possibility for a safer, more centralised, and private business environment is enhanced when Building Information Modeling (BIM) is combined with Blockchain Technology (blockchain). Proof-of- ownership functions, such as rights issuance, proof-of- provenance functions, such as record keeping through a transparent immutable ledger, and a decrease in human mistakes and deviations are all made possible by Blockchain technology. The Internet of Things is extensively used, so each program every time focuses on a particular region. The duties of an Iot platform can be split into three categories: query, management, and tracking which includes recurring and event documents like those for tracking the environment. To top it all off, it is expected that the BMS-related data would be stored in the cloud in a readily accessible repository for the duration of a facility's life cycle for the sake of maintenance. When a number of different BMS models are brought into a BMS, a number of potential security concerns arise. The BMS model is a digital representation of the building that contains information about its layout.

H. POSSIBLE VALUE REALIZATION

Blockchain technology improves IoT security and scalability with immutable ledgers. To prevent hackers from accessing blockchain-stored IoT data, further security is needed (Bult, 2019). Data is safe with Blockchain encryption. Blockchain transactions may be monitored by authorized parties. Data breaches may be detected and remedied. Bitcoin's Blockchain can organize billions of devices and speed up transactions. Distributed ledger technology handles massive transactions as the number of connected devices rises. Blockchain might reduce Internet of Things gateway protocol, hardware, and communication costs by enhancing stakeholder trust. Smart contracts on the Blockchain allow parties to execute contractual agreements according to predefined criteria.

III. RESEARCH METHODS

- Blockchain Implementation
- Adding new nodes to the Blockchain
- Use-case Implementation and Deployment

I. Blockchain Implementation

In this section author is putting into operation the decentralised and interconnected architecture for the Internet of Things that is founded on Blockchain technology. As more and more devices are added, the security of the Internet of Things (IoT) will deteriorate if there is not a solid framework in place that is built from the ground up. Our focus is on developing a strategy for the architecture, deployment, and standardisation of blockchain-based Internet of Things software that is required to be aligned in the construction project efficiently (Dey and Shekhawat, 2021).

It permits efficient administration of data and information relevant to construction-related aspects, such as the structure, and user behaviour, such as access, mobility, response, etc. Between Building Management Systems (BMS) and BMS models, Blockchain may be used to restrict who is allowed access to data and information about a building. Each individual structure that is a component of the BMS is handled as if it were its own independent node (Alam, 2022).

Whitelisted in the Blockchain database is the static IP address that is allocated to each node, and only these assigned IP addresses are permitted to communicate with the Blockchain

(Firouzi *et al*. 2022). In order to separate the Blockchain logic from the rest of the operating system, it is created as a Docker image. This image includes all of the necessary software and dependencies for the Blockchain logic to be

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v11i5.6604
***Article Received**: 22 February 2023 **Revised**: 29 March 2023 **Accepted**: 18 April 2023*

executed. All of the decision-making procedures that are associated with the Internet of Things devices are going to be carried out on the Blockchain in the form of smart contracts.

The capabilities that are built into Blockchains help with resource management in many different ways. These include the transfer of access rights from one entity to another, the effective implementation of access control regulations, the maintenance of characteristics, and the resulting development of scalability in fog nodes. For the purpose of forming judgements on access control, these qualities are necessary. As a result of this, Blockchain technology has the potential to serve as a central hub for the safe, verifiable, and decentralised flow of data across a wide variety of Internet of Things devices. By centralising the management of distributed computing and storage, the blockchain might be used by low- power Internet of Things devices to expedite the approval process for local authorizations. In this way, the blockchain network may provide a central guarantee of the legitimacy of the authorization chain, while edge IoT devices check the security settings (Rebello et al.2019)

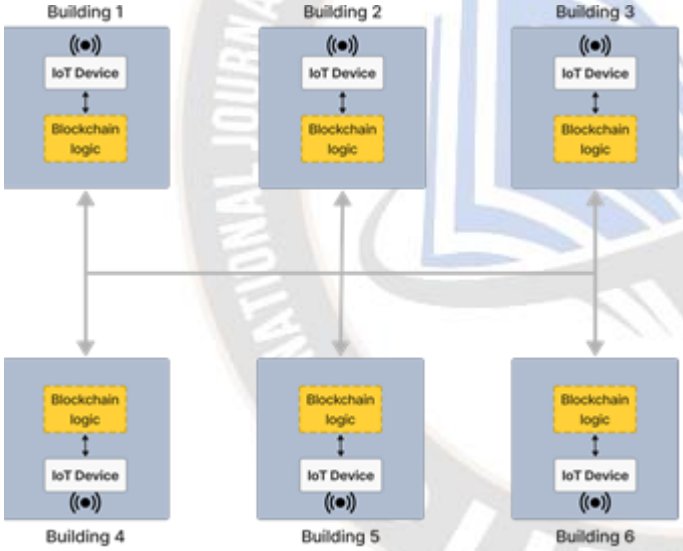

Fig. 5 Integrated BMS, IoT and Blockchain technologies in the proposed system design

J. Adding new nodes to the Blockchain

Adding nodes to the blockchain network is a must for any further development (the nodes being individual building that are a part of the building management system). It is crucial that the computational burden of implementing multiple cryptographic protocols be kept to a minimum.

As we know that before implementing any attributes or metrics, it is necessary to add nodes to the Blockchain network (the nodes being individual building that are a part of the building management system).

To achieve this, the comprehensive procedure stated below needs to be executed:

A Docker Image containing the entire blockchain logic is generated by the BMS committee.

- To add a building (the individual node) to the network, it must be assigned a static IP address.
- This IP address is privately sent to more than 50% of the nodes over an encrypted LAN channel as a digitally signed JSON file containing instructions to add this IP address to the whitelist.
- Once the IP address is added to the whitelist on the blockchain database distributed across all the nodes, the new building can start the admission process.
- The new nodes send a FETCH request to the blockchain. If the request is from a whitelisted IP address and HASH of the request headers matches the allowed HASH code, the blockchain replies to the request with Dockerfile.
- This Dockerfile of the new node is used to generate a Docker image which then finally creates a Docker container running the blockchain logic in an isolated environment.
- The creating of this Docker container is followed by a broadcast message in the blockchain confirming the successful creating of the new node.
- Upon successful authentication of this message, the node is finally assigned as a part of the blockchain network followed by a successful admission broadcast which tells the new node to start doing its thing.

The following detailed method must be carried out to accomplish this goal: The blockchain's whole functionality is packaged as a Docker Image that is created by the BMS committee. A permanent Internet Protocol address must be given to a structure before it can be added to the network. More than half of the nodes get this IP address in a digitally signed JSON file over a secure LAN connection with explicit instructions to whitelist this address. The admissions procedure for the new building may begin after the IP address has been added to the whitelist in the blockchain database shared by all the nodes. This new node's Dockerfile is used to make a Docker image, which is used to make a Docker container, which runs the blockchain logic in its own, secure, isolated environment (Whaiduzzaman *et al.* 2022). After this Docker container is created, a blockchain broadcast message is sent to verify that the new node was successfully created. After this message has been authenticated, the node will be added to the blockchain network and will receive an admission broadcast instructing it to begin processing transactions.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v11i5.6604
***Article Received**: 22 February 2023 **Revised**: 29 March 2023 **Accepted**: 18 April 2023*

K. Use-case Implementation and deployment : Proposed Architecture

A business considering implementing a blockchain and IoT solution to a problem might "start small" by researching relevant current apps and settling on a framework for creating their own (Novo et al. 2018). Fig. 7 shows the layer-based design of the proposed IoT blockchain stage, stretched out from past work. This is all there is to it secluded design, where each layer is separated from the others, permitting engineers to supplant or add new modules without influencing the remainder of the framework. The actual layer of IoT comprises of different associated gadgets with correspondence, processing and information stockpiling abilities. The essential capability of the network layer is steering the executives, as actual gadgets themselves don't have a worldwide Web Convention (IP) and must self-put together. This layer likewise contains different modules for offering types of assistance like organization the board, security the executives, and message dealers. The IoT Blockchain Administration Layer contains all modules that sort out normal administrations that give different elements of blockchain innovation, like character the board, agreement, and distributed (P2P) correspondence. A conveyed record is an agreement of reproduced, shared, and synchronized computerized information spread across a blockchain network, permitting all members in the organization to have their own duplicate of the record. It likewise gives a solid extra room to recording gadget setup and gathered information given by actual sensors. Changes to the record are reflected in all duplicates in minutes or even seconds. A record can be tolerant, contingent upon whether anybody or just approved individuals can peer and approve exchanges.

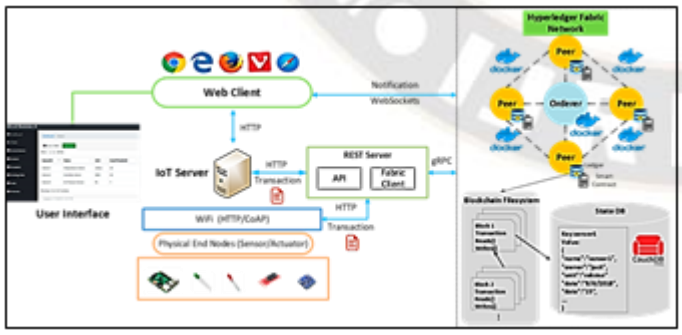

Fig.6 IoT blockchain platform implementation and use case deployment

The large information investigation module makes Blockchain an effective method of online information stockpiling. A lot of conditional information from different gatherings is put away in organized records, making it an optimal hotspot for top to bottom examination. Admittance to a solitary organization can be conceded to these gatherings, making it helpful to get to these subtleties. Savvy contracts are carried out by outer client applications to oversee access and changes to the record with a kind of code that is called. It is commonly introduced and started up on each companion in the organization. Occasion the executives sends an occasion at whatever point another block is added to the record or set off when a predefined condition in a shrewd agreement is met. The Programming interface uncovered the administrations given by the Blockchain network as administrations that client applications can get to and deal with the organization. The top layer is the application layer where information from the actual gadget is pictured and different connection points are accommodated controlling and controlling the gadget.

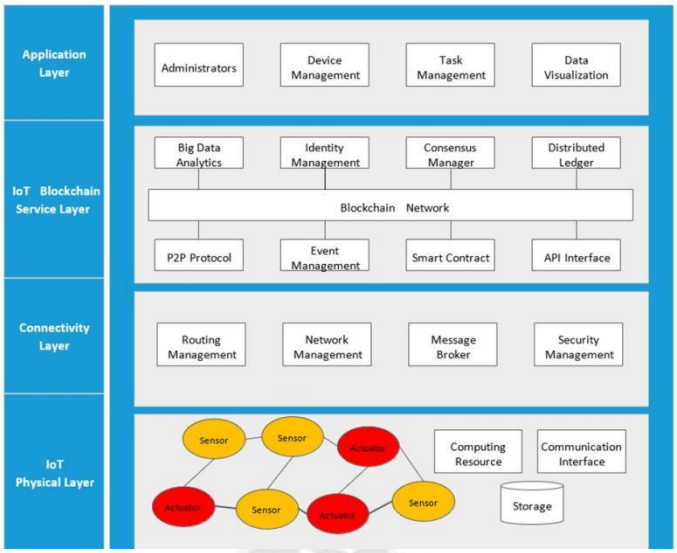

Fig.7 Layer-based IoT blockchain platform architecture

When it comes to connecting devices in IoT networks, several well-known protocols are often employed. The Blockchain must be guarded using less resource-intensive encryption methods. For scalability issues, parallel Blockchain is the way to go (Huang et al. 2019). Recent initiatives have emphasised scalability as an important topic in need of rapid, efficient solutions. The increasing number of networked gadgets has been demonstrated to have a negative impact on system efficiency in a number of research efforts. This highlights the need for more research funds to develop the science of scalable, trustworthy connectivity without compromising performance (Ahmad et al. 2021). Although Blockchain-based systems may be made to use less energy using a variety of techniques, they still fall short of more efficient options. Adding Blockchain nodes with a lot of computing power to an IoT network

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v11i5.6604
***Article Received**: 22 February 2023 **Revised**: 29 March 2023 **Accepted**: 18 April 2023*

improves system resilience but also increases energy consumption.

IV. CONCLUSION

In conclusion, Blockchain-empowered security enhancement IoT framework has the potential to revolutionize Building Management System (BMS) applications by improving the security and reliability of the system. This technology enables secure and decentralized data storage, which can reduce the risk of data tampering and hacking. By using Blockchain technology, BMS can ensure that all data is encrypted and only accessible to authorized parties. The use of smart contracts in Blockchain technology can automate many BMS processes, such as energy consumption management and predictive maintenance. Moreover, the IoT framework integrated with Blockchain technology can provide real-time monitoring and data analysis to improve the energy efficiency of buildings, reduce energy consumption and costs. The technology can also improve the occupant's experience by ensuring a comfortable and healthy indoor environment.

REFERENCES

[1] Ahamad, S., Gupta, P., Acharjee, P.B., Kiran, K.P., Khan, Z. and Hasan, M.F., 2022. The role of blockchain technology and the Internet of Things (IoT) to protect financial transactions in the cryptocurrency market. Materials Today: Proceedings, 56, pp.2070-2074. Ahmad, W., Rasool, A., Javed, A.R., Baker, T. and Jalil, Z., 2021. Cyber security in IoT-based cloud computing: A comprehensive survey. Electronics, 11(1), p.16.

[2] Alam, A., 2022. Platform Utilising Blockchain Technology for eLearning and Online Education for Open Sharing of Academic Proficiency and Progress Records. In Smart Data Intelligence (pp. 307-320). Springer, Singapore.

[3] De Moraes Rossetto, A.G., Sega, C. and Leithardt, V.R.Q., 2022. An Architecture for Managing Data Privacy in Healthcare with Blockchain. Sensors, 22(21), p.8292. Dey, K. and Shekhawat, U., 2021. Blockchain for sustainable e-agriculture: Literature review, architecture for data management, and implications. Journal of Cleaner Production, 316, p.128254.

[4] Firouzi, F., Farahani, B. and Marinšek, A., 2022. The convergence and interplay of edge, fog, and cloud in the AI-driven Internet of Things (IoT). Information Systems, 107, p.101840.

[5] Hämäläinen, M. (2020). A framework for a smart city design: Digital transformation in the Helsinki smart city. In Entrepreneurship and the Community (pp. 63-86).

[6] Springer, Cham.

[7] Huang, J., Kong, L., Chen, G., Wu, M.Y., Liu, X. and Zeng, P., 2019. Towards secure industrial IoT: Blockchain system with credit-based consensus mechanism. IEEE Transactions on Industrial Informatics, 15(6), pp.3680-3689.

[8] Kollolu, R., 2020. A Review on Wide Variety and Heterogeneity of IoT Platforms. The International journal of analytical and experimental modal analysis, analysis, 12, pp.3753-3760.

[9] Novo, O., 2018. Blockchain meets IoT: An architecture for scalable access management in IoT. IEEE internet of things journal, 5(2), pp.1184-1195.

[10] Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2020). Integration of blockchain and cloud of things: Architecture, applications and challenges. IEEE Communications surveys & tutorials, 22(4), 2521-2549. Patil, P., Sangeetha, M. and Bhaskar, V., 2021.

[11] Blockchain for IoT access control, security, and privacy: a review. Wireless Personal Communications, 117(3), pp.1815-1834.

[12] Patnaik, R., Padhy, N. and Srujan Raju, K., 2021. A systematic survey on IoT security issues, vulnerability, and open challenges. In Intelligent System Design (pp. 723-730). Springer, Singapore.

[13] Rebello, G.A.F., Camilo, G.F., Silva, L.G., Guimarães, L.C., de Souza, L.A.C., Alvarenga, I.D. and Duarte, O.C.M., 2019, May. Providing a sliced, secure, and isolated software infrastructure of virtual functions through blockchain technology. In 2019 IEEE 20th International Conference on High-Performance Switching and Routing (HPSR) (pp. 1-6). IEEE.

[14] Shrestha, R. and Kim, S., 2019. Integration of IoT with blockchain and homomorphic encryption: Challenging issues and opportunities. In Advances in Computers (Vol. 115, pp. 293-331). Elsevier.

[15] Sun, S., Du, R., Chen, S. and Li, W., 2021. Blockchain- based IoT access control system: towards security, lightweight, and cross-domain. IEEE Access, 9, pp.36868-36878.

[16] Torky, M. and Hassanein, A.E., 2020. Integrating blockchain and the internet of things in precision agriculture: Analysis, opportunities, and challenges. Computers and Electronics in Agriculture, 178, p.105476.

[17] Whaiduzzaman, M., Barros, A., Chanda, M., Barman, S., Sultana, T., Rahman, M.S., Roy, S. and Fidge, C., 2022. A Review of Emerging Technologies for IoT-Based Smart Cities. Sensors, 22(23), p.9271.

[18] Xu, R., Chen, Y., Blasch, E. and Chen, G., 2018, May. A federated capability-based access control mechanism for the internet of things (IoT). In Sensors and Systems for Space Applications XI (Vol. 10641, pp. 291-307). SPIE.