Journal of Ecohumanism
2024
Volume: 3, No: 7, pp. 5127 – 5136
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i7.4620

Integrating Blockchain Technology with Internet of Things and Edge Computing to Achieve Security

Tejasvee Gupta[1], Hiren B Patel[2]

Abstract

The last decade has seen many advancements and emergence in computing technologies; Internet of Things (IoT) being one of the most successful among them. Huge data generation in IoT can be utilized for analysis and monitoring the behaviour of various patterns. In spite of wide adaptability, IoT has various challenges such as privacy, security and computational constraints. To address the later challenge, Edge computing can be a potential solution with great computational resources leading towards the improvement in performance in terms of latency, throughput and response time. However, privacy and security remain largely unaddressed along with the traditional limitations of a centralized approach. This brings into the usage of another technology viz. Blockchain that handles the issue of privacy and security through its inherent features such as immutability, transparency and decentralization. In this research, we intend to explore the option of possible integration of Blockchain technology with IoT to address these challenges.

Keywords: *Blockchain Technology, Internet of Things, Edge Computing.*

Introduction

The way people interact with things around them has changed from keyless entry into cars, to retail shopping at an Amazon Go store. International Data Corporation (IDC, 2019) predicts that there will be more than 40 billion IoT devices connected by 2025, generating about 80 zettabytes of data. This is greatly due to the penetration of IoT in various verticals like home, office, building, cities and horizontal industries like, health, retail, etc. For the common man, IoT can be used as a wearable device or in constructing smart homes, offices and various other sectors. Data generated from various IoT devices could be personal identification information, bank account data, environmental data, asset information, insurance record, health data, etc. Among which, some are very sensible and need to be handled very carefully from the privacy and security perspective. It is the role of the developer to design a trust model which the end users count on for their private and confidential data.

Traditional Cloud technology is used for the centralized management of the IoT technology. It works for most of the applications where latency and throughput are not the concerns. But when it comes to fast response and computing, the suitability of Cloud computing is a concern in IoT. This paved the way for Edge Computing – an architectural solution that brought compute powers closer to the end devices which results in improving the latency and throughput. Edge computing has improved the IoT capability in terms of efficient communication and computation to reduce latency. Though IoT has found a place in various sectors, yet it faces challenges like privacy, security and scalability that prevents its wide adaptability.

Blockchain technology, which is a distributed ledger technology, proves a viable solution for decentralized computing due to its features like immutability, fault tolerance and transparency (Wang et al, 2018). As each node in Blockchain carries a local copy of the ledger, which cannot be manipulated without changing all the local copies residing in separate blocks which is practically unfeasible. Also, Blockchain uses cryptography (e.g. hash function SHA) to construct a chain of blocks containing transactions, which makes it almost impossible to break or alter. Furthermore, entities communicating on Blockchain may interact with each other based on a predefined set of rules or agreement. Such an agreement can be implemented using Smart Contract that is nothing but a simple programming code to simulate the understanding between those entities. Smart contracts get automatically executed when a transaction happens and then enforce a kind of agreement which entities need to abide to. Failing to do so, transactions are invalidated. This

[1] LDRP Institute of Technology and Research, Sarva Vidyalaya Kelavani Mandal, India.
[2] Principal, Vidush Somany Institute of Technology and Research, Sarva Vidyalaya Kelavani Mandal, India.

Journal of Ecohumanism
2024
Volume: 3, No: 7, pp. 5127 – 5136
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i7.4620

technology can be a solution in edge computing, as the data transactions need to be authentic and secure. Access Control in IoT can be managed at decentralized edge node through Smart contracts.

Though, with limited power and resource constraints at IoT and edge devices, it would be a challenge to embed Blockchain. We, in this paper aim to integrate Blockchain in IoT and Edge computing and demonstrate that, not only the privacy and security concerns of Edge computing are resolved, but the performance is also not compromised drastically.

Blockchain is a set of blocks arranged as a chain that stores transactional information which are cryptographically linked. The data is stored in a distributed ledger, meaning each node in the network stores a local copy of the blocks. Each block stores the hash of previous blocks. Hash of each block is generated using a cryptographic algorithm (for instance, SHA256 in the case of Bitcoin). As each block stores the hash of the previous block, to change a transaction all subsequent blocks need to be modified which is almost impossible. Hence Blockchain is said to be decentralized, immutable, transparent and fault tolerant.

Decentralization, means the system is not controlled by a single- central entity. The blockchain is a distributed public ledger that stores the data in all the nodes in the network distributed geographically. There is no central database that holds the data, and thus, it removes the concerns that are faced by the centralized system. The data is replicated in many trusted nodes in the network so no loss of data to node failure is possible. Also because of its decentralized property, it reduces the computational overload on a single system and removal of third party brokerage in some applications that are widely used. The first example of benefiting from this was "The Bitcoin" cryptocurrency, which has gained huge popularity among the public, as there is no centralised authority to govern the currency. It's transparent as all the nodes in the network may have a copy of the Blockchain and everyone can see each and every transaction that has happened. Usually, this concept is used in cryptocurrency which keeps transparency in transactions for every user. Though the user is not known, and only the public address that is a cryptographic value is known, no one can ever trace the user unless you know someone's public address. Immutable because each block stores the hash of the previous block and the hash of each block is calculated. Using the transaction data of each block, it is almost impossible to change the transaction value back in time, as doing so will make the subsequent block invalid, and a hacker will have to make changes in all subsequent blocks and in all the nodes having the copy, which is almost impossible.

In the past decade IoT has gained huge popularity among people, industries, academics and researchers. It has changed the way humans interact with physical things, with the help of the Internet or some communication technologies. Right now, there is a small and distinct network of things connected to form a small IoT system. However, the future will see all the different networks connected through the Internet. IoT has occupied space in small household devices to large industrial machines. The increasing popularity has also drawn the attention of attackers, as the data may be private and confidential.

The general architecture(Sikder et al, 2018) of the IoT is mentioned in Fig 1. The lowest layer is the sensing layer or the actuator layer. This comprises sensors like GPS, camera, mic, speaker, thermal/heat, light, health, water, etc. Also the actuators are present in this layer that take actions like making sound, take photos, change temperature, change direction, sprinkle water, etc. These are small devices with limited compute, communication and power sources.

Journal of Ecohumanism
2024
Volume: 3, No: 7, pp. 5127 – 5136
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i7.4620

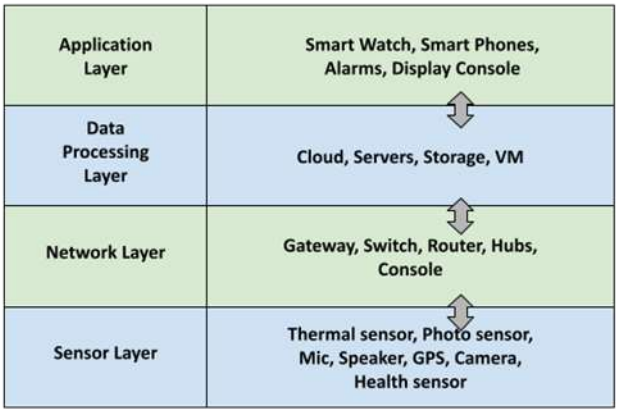

Fig 1. IoT Architecture

The next layer is the network layer which comprises gateway, switch, router, hubs, console, etc. The hubs, switches and consoles here are not the typical networking device. They are the interface between the sensors and Cloud servers. These devices may have dual communication technologies like IP network to connect to the Internet services and Bluetooth, Wi-Fi, RFID or other RF technologies to connect to the sensors or actuators. This is because not all sensors/actuators are having IP network capabilities. These devices not only act as an interface between two layers but also possess compute and analysis tasks.

The next layer is the data processing layer which is at a Cloud or an isolated VPN. This mainly comprises the storage, compute and analytics part. As IoT generates huge amounts of data, it needs to be stored for auditing and logging and is carried out at this layer. This layer has storage servers to provide such tasks. Also for compute and analytics, this layer has high end servers or individual VMs assigned for different tasks. According to the data received either from sensors or the application layer, processing is done and required action or report is sent to respective layers.

The last or the topmost layer is the application layer which normally comprises end user devices or automatic consoles. This layer has smart watches, cell phones, consoles for smart homes or buildings or cities, displays, etc. Cell phones and smartwatches act as sensors or actuators as well. They receive the information from the sensors and notify the user about the same. Also, necessary action is taken through applications, which is communicated back to the actuators at the lower layers.

With great strength, IoT also possesses some challenges(Farhan et al, 2017) that are topics of discussion for researchers. Network, resource constraint, security, fault tolerance and software development are some of them. The IoT devices are used to sense and generate data round the clock. These data need to be logged or reported, which requires network connectivity to send and receive data. As sensors may be at remote/unreachable locations, availability of network in those regions may be scarce or negligible. Though the currently used networking technologies like Wi-Fi, Zigbee, Bluetooth, RFID, etc have not failed the communication but has limited the reachability of these devices. So intelligent placement and proper technologies are required to be chosen for specific applications. The IoT devices normally consist of limited dimensions and are small enough to be portable. These devices have limited power, communication and compute resources. Due to these limitations, proper communication, that consumes less power, needs to be selected. Similarly, with reduced dimensions, the storage and compute devices are not present or are of limited capacity. As the devices are basically linked with personal devices or industrial devices, loss of data is also a concern. With great popularity, IoT has also attracted the attention of attackers. Due to resource constraint, embedding of security algorithms is not feasible for all applications. Some of the communication technologies are also easy targets for attackers and compromise the devices. Hence proper access mechanisms need to be used. Again IoT devices may suffer some faults, failing to respond or generate data. The reasons for this may not be easily known, as it might be because of power, communication or physical damage. And failing of any such devices may break the chain or itself causing loss of data. Sometimes it is easy to trace and replace the devices, however in some cases, it may not be possible or might lead to the

Journal of Ecohumanism
2024
Volume: 3, No: 7, pp. 5127 – 5136
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i7.4620

loss of resources in terms of time and money. Again, due to the limited resource present in the IoT, the compute resource or storage may be limited. So, the code governing the sensors also needs to be written in a very optimized way, abiding the resource constraints. Also the communication code and analytics code are present in the same hardware, sparing little space for storage. So, the optimized code is always application specific, as it requires changes from application to application.

Edge computing was evolved to bring the computational and storage capabilities closer to the IoT devices at the edge of the network, rather than the centralized Cloud platforms. Edge computing has highly reduced the latency, that is the time delay in networking between IoT devices and computational resources. Various IoT applications that require prompt response, like video processing, speech processing, artificial intelligence, augmented reality, etc. have benefited from the Edge computing paradigm.

Related Work

There has been mere work that proposes architectural solutions to overcome the IoT challenges by implementing Blockchain over the edge devices. One such architecture is (Pan et al, 2019) where an Edge-IoT framework named "EdgeChain", based on Blockchain and smart contracts is proposed. A permissioned Blockchain and an internal cryptocurrency used to link edge resource pools and IoT devices. EdgeChain uses a credit-based system to control the amount of resources that can be used by IoT devices based on priority, past behaviour and application type. Their experimental setup is used to compare the computational cost of running Blockchain with two other IoT applications and a natural language processing application. The results show that the Blockchain has the lowest CPU usage compared to other two applications.

Similarly, (K. Wright et al, 2018) also highlight the computational resource limitation that exists in IoT systems and how edge computing solves the computation problem. The authors propose a solution called SmartEdge: A smart contract for Edge Computing. In their experimental setup, they have used a Raspberry pi as a data node and a powerful desktop as a compute node. Smart Contract is also installed on the compute node. They execute a computationally intensive task on a data node in the absence of an Edge device that is a compute node and then the same task on an Edge device (compute node) using smart contract. Their results demonstrate how edge computing drastically changes the execution time and also how Blockchain doesn't affect the execution time too much.

(Ali et al, 2018) discuss how, with the increase in number of IoT devices and the data generated, may create a bottleneck at the Cloud for computation, that may result in latency issues. And hence computation can be shifted to the edge of the network. Though Edge servers may improve upon latency, however may still not provide complete security as delivered by centralized Cloud mechanism. This makes way for Blockchains due to its features like transparency, immutability and fault tolerance and provides a trusted decentralized environment. The authors propose a Cloud-blockchain hybrid architecture, which may be decided by application in different use cases to select traditional Cloud architecture or enhance the blockchain tier for security mechanisms.

The authors (Sahmim et al, 2019) predict that most of the transactions between virtual machines on Cloud and IoT devices occur over the Internet. The traditional client-server or publish subscribe mechanism may prove a single point of failure despite the high infrastructure cost. And hence, a blockchain based edge computing model will help to reduce the latency and improve upon security. The authors propose an architectural solution based on Blockchain and Edge computing called Smart Identity Wallet based Architecture.

The authors (Zhang et al, 2019) investigate the critical access control issues in IoT and how the traditional access control policies are not suitable for IoT due to its dependence on centralized server or identity. 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 in IoT. Their experimental setup, tests and proves the feasibility of their proposed work to achieve a trustworthy decentralized solution.

Journal of Ecohumanism
2024
Volume: 3, No: 7, pp. 5127 – 5136
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i7.4620

The authors (Ding et al, 2019) of this paper also discuss how the traditional access control technologies are not fit for IoT. The traditional centralized mechanisms may not solve the credibility issues of resource constrained IoT devices. They propose an attribute-based access control scheme using blockchain for IoT. They have used a consortium blockchain technology and the attributes are recorded in blockchain.

(Sun et al, 2021), discuss the disadvantages & limitations of using an IoT node as Blockchain node. Hence, they propose to integrate a permissioned Blockchain that is lightweight as the IoT systems are divided into multiple domains and each domain has its own Blockchain ledger. They demonstrate how their model avoids DDOS attack and uses policy decision points for deciding the policy decisions.

Novo, 2018 proposes an architectural solution for access management in IoT with generic and scalable solutions. The architectural solution uses a management hub node to manage the access control thing. The architecture uses the Blockchain technology for access management and uses a single smart contract to fulfil their cause.

The paper (Hu, 2022) compares the benefits of the Blockchain system to be used for Access control with the centralized mechanism. This also advocates how the access control data can be prevented from manipulation by using Blockchain technology and also maintains an audit/log that will help to maintain a list of malicious attempts to access unauthorized objects. The paper also shows some architectural solutions that are independent of the type of Access control model. The paper also says that the discretionary Access control model can be permissionless, but the NDAC will be a federated or permissioned Blockchain model that may act as a single point of failure.

The paper (Roy et al, 2023) proposes an architectural solution to improve access control by using Blockchain with IoT. Their model named BloAC is demonstrated with the benefit of outperforming the cloud-based access control model. The paper also depicts the possible attacks that the model can face on the Edge-IoT network. But as the single point of failure can be avoided and with more Edge-nodes the scalability can be handled as well as the response time may also improve.

In paper (Guo et al, 2023) proposes a Domain attribute based Access Control(DABAC) that uses the physical location of the IoT devices as a domain element. The gateway device is used for identifying the physical location of an IoT device. Smart contracts are used for Access control using predefined contracts. It uses 3 main contracts named user management contracts, device management contracts and Access control contracts. The only novel part of this paper is that it uses the location of devices as an extra feature for access control as an attribute metric.

All the above research is targeting the concern over the resource constraint of IoT devices that highlight the challenges of IoT such as low latency and performance. To overcome these challenges, Edge computing is introduced to solve the problem of low latency as the compute comes closer to the IoT devices. However, as Edge servers are not as powerful as traditional Cloud servers, security and privacy becomes a new challenge. We, in our research, are proposing an architectural solution where Blockchain can be embedded to overcome the privacy and security challenge of IoT.

Challenges Identified

The challenges that are identified in this paper are mainly the decentralized approach required for IoT, the computational capability restriction of IoT devices, privacy and security issues in Edge computing due to decentralized mechanisms, and access control of IoT devices. Some of the problems may be handled with Edge computing and some may require Blockchain features to develop a trustworthy and decentralized approach, though implementing Blockchain itself into IoT is also a novel challenge.

Journal of Ecohumanism
2024
Volume: 3, No: 7, pp. 5127 – 5136
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i7.4620

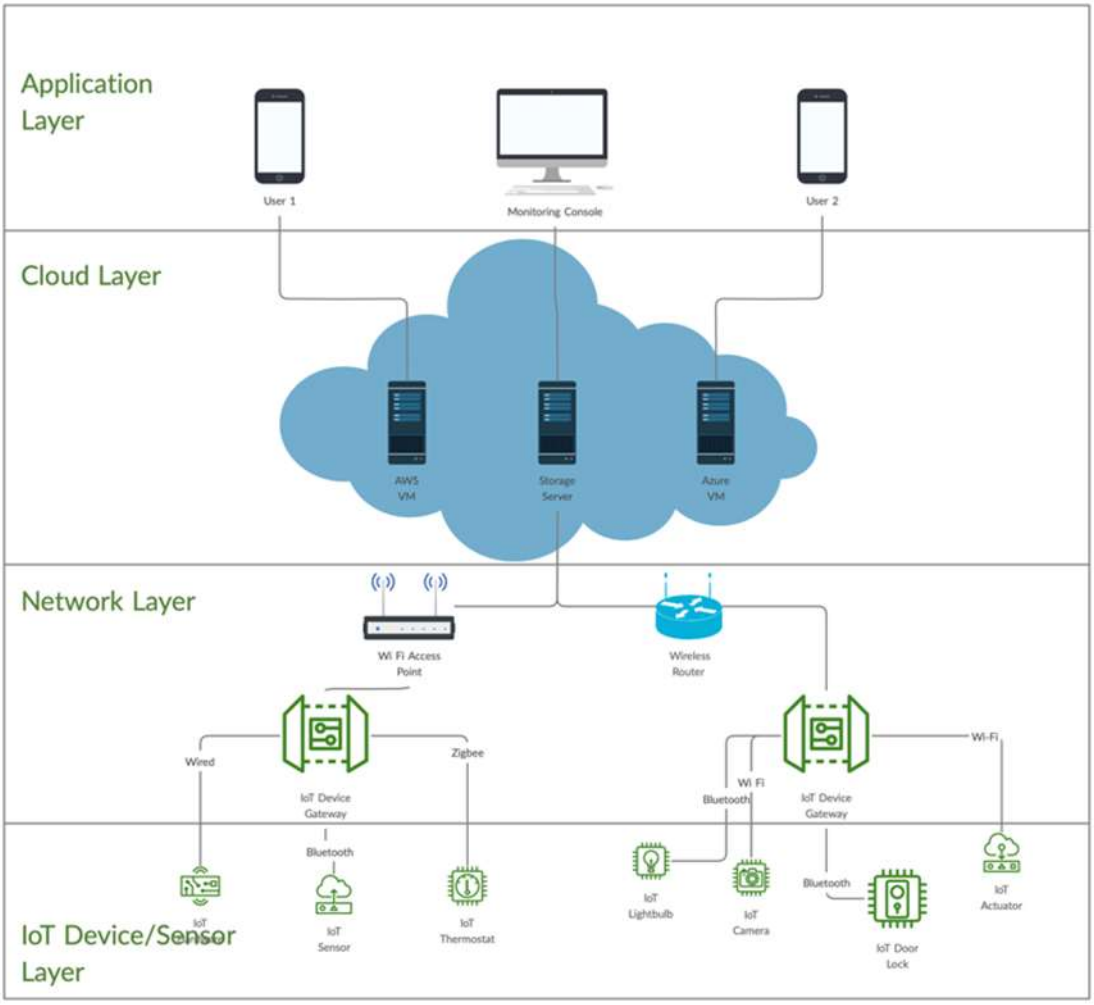

Fig 2. Iot Architecture Schematic Diagram

The schematic diagram of traditional IoT architecture is mentioned in Fig 2. In the figure it can be seen that on the lowest layer, are sensors/actuators laying individually or embedded with electrical devices. On the next layer, known as the network layer, is the typical networking hardware devices like access points, wireless routers as well as IoT gateway/hub which connect to the IP network, as well as also connect to the lower layer IoT devices using communication technologies like Wi-Fi, Bluetooth, Zigbee, etc. The third layer is the Cloud layer and is set up at private or public Cloud platforms, where analysis and data processing are performed. The topmost layer is the application layer, where the user directly interacts with the IoT system.

The schematic diagram of Edge computing in Fig 3 is depicting how the Edge layer is enhancing the performance of IoT applications, as it can be seen that the network layer is modified to have Edge servers at this layer, that enhances the performance in terms of low latency by bringing the compute task nearer to the IoT device layer, so that, the overhead of communication time between IoT layer and Cloud computing layer is reduced. Though the Edge servers are not as powerful as the Cloud computing servers but serve the purpose of IoT well in terms of analysis.

Journal of Ecohumanism
2024
Volume: 3, No: 7, pp. 5127 – 5136
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i7.4620

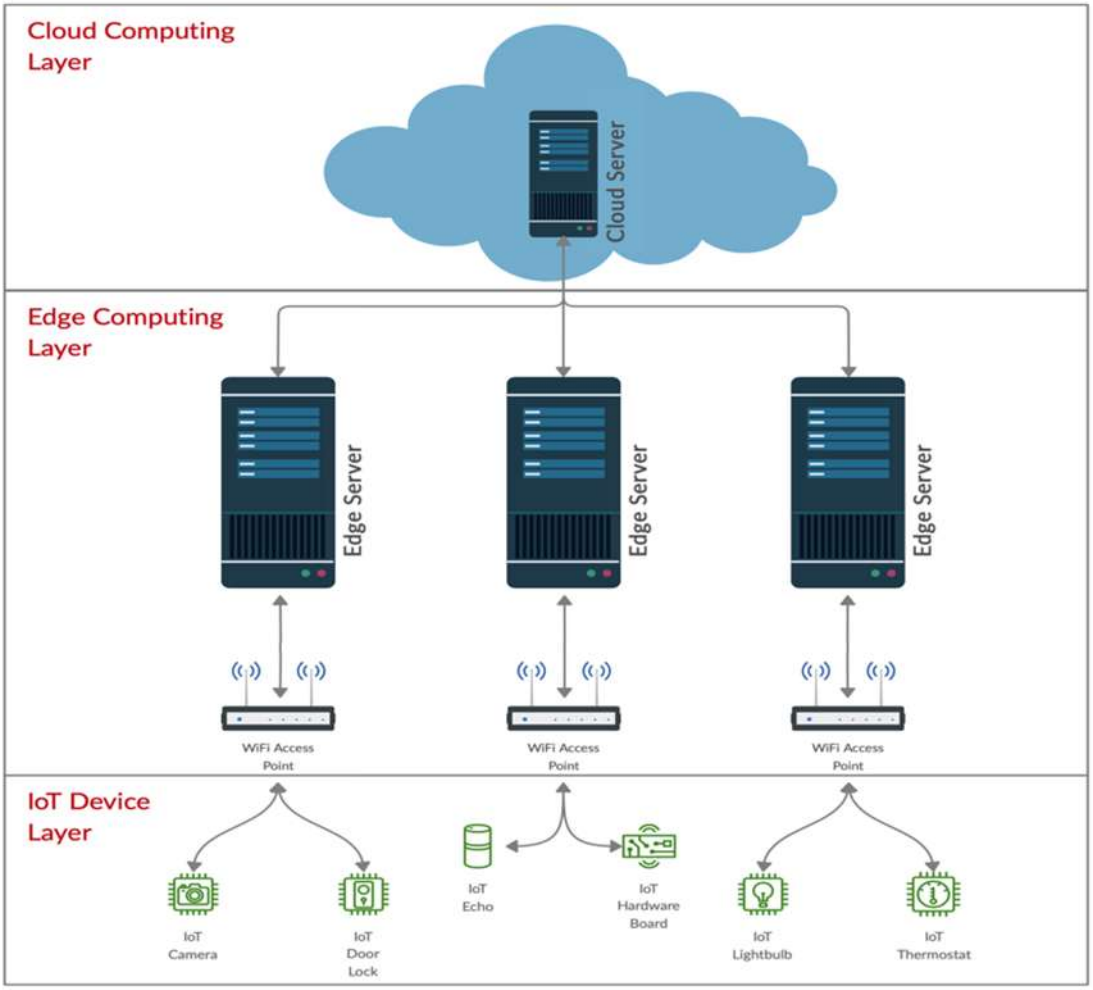

Fig 3. Edge Computing Schematic Diagram

Proposed Architecture

We propose our architecture depicted in Fig 4. Here, we embed the Blockchain and smart contract at the Edge computing layer, between the physical layer and the Cloud layer. The schematic diagram of the basic Edge Computing architecture is depicted in Fig 3. The edge layer acts as an interface between IoT devices and Cloud layer. The edge layer has a compute and storage device that provides local support to the IoT devices. Bringing compute devices closer to the IoT devices improves the performance like latency, throughput and response time.

Journal of Ecohumanism
2024
Volume: 3, No: 7, pp. 5127 – 5136
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i7.4620

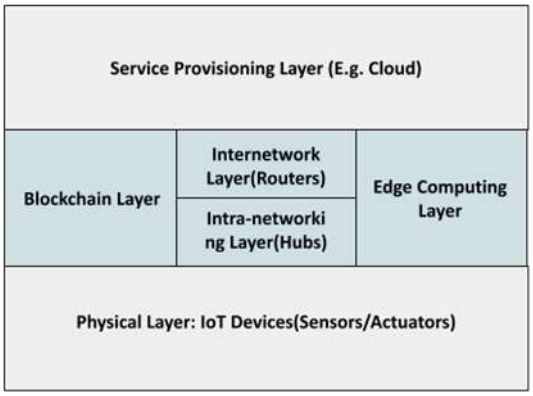

Fig 4. Proposed Architecture

Experimentations and Results

For the experimental setup we use the following devices:

A virtual machine on ParamShavak (CDAC, 2016 & PARAM Shavak, 2016) super computer as Cloud platform for Blockchain node.

A Cloud mqtt broker on EMQX Cloud MQTT (public MQTT broker viz. broker.emqx.io)

A system with i5 processor and 4GB ram working as an Edge node.

A mosquito client on a local system to publish mqtt messages working as a proxy to IoT devices.

Steps followed are as under:

A python script on Cloud server to continuously monitor for messages published by IoT devices.

On the edge node we implement blockchain and smart contracts. Also, the same python script installed on Cloud VM.

A local machine working as a mosquito client publishing on or off messages on behalf of IoT devices.

We have set up an experimental scenario, wherein an IoT device is triggered to generate a computational task for further processing to evaluate our claims. To start with, an IoT device, from the lowest layer, publishes a message which is subscribed and analyzed by the python script running on the Cloud server situated on the topmost layer. Subsequently, the response is published on mqtt broker which in-turn is received by the IoT device through subscribe mechanism. A response time is measured under two different criterions viz. (a) without Blockchain and (b) with Blockchain. The results are as follows:

Journal of Ecohumanism
2024
Volume: 3, No: 7, pp. 5127 – 5136
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i7.4620

```
creating new instance
connecting to broker
message received  on
Switch On time = 1629786403.3823147
message received  Open the door
Open command response time = 1629786403.6525722
message received  off
Switch off time = 1629786407.9621475
message received  Keep the door closed
Door closed response time = 1629786408.2736
```

Fig 5(a). Response time with IoT Cloud scenario(without Blockchain)

```
creating new instance
connecting to broker
message received  off
Switch off time = 1630035652.047476
message received  on9999
Switch on9999 time = 1630035655.1627934
message received  Open the door
Open command response time = 1630035655.7567222
message received  on1234
Switch on1234 time = 1630035659.2341316
message received  Open the door
Open command response time = 1630035659.8249264
message received  on
Switch On time = 1630035663.8532786
message received  Keep the door closed
Door closed response time = 1630035664.502801
```

Fig 5(b). Response time with IoT Cloud scenario(with Blockchain)

The following table illustrates the results described in Fig5(a) and 5(b).

Response Time (Sec)	Without Blockchain	With Blockchain	Difference
Response time on command "ON"	0.3294	0.5907	0.2613
Response time on command "OFF"	0.3114	0.6495	0.3381

Table 1. Response time with and without Blockchain

As can be seen in Table 1, introduction of Blockchain in existing scenarios does not increase the response time significantly. For instance, in case of ON command, the response time is increased by 0.26 seconds whereas, in case of OFF command, the response time is increased by 0.34 seconds. Hence, we conclude that with nominal compromise in terms of performance(response time), we can achieve significant security through Blockchain. It is further observed that Blockchain introduces an extra delay of ≈0.2 second per transaction which is almost negligible for long computational processes.

```
pragma solidity ^0.5.4;

contract TestBell {
    string s1 = "Open the door";
    string s2 = "Keep the door closed";
    function foo(string memory x) public view returns (string memory) {
        if (keccak256(abi.encodePacked((x))) == keccak256(abi.encodePacked(("1234")))){
            return s1;
        } else if (keccak256(abi.encodePacked((x))) == keccak256(abi.encodePacked(("9999")))){
            return s1;
        } else {
            return s2;
        }
    }
}
```

Fig 6. Smart Contract Code for Doorbell Application

Conclusion

Through this research, we have explored an option of integrating Blockchain technology in existing IoT networks with edge computing to address the concerns of security and privacy. Introduction of Blockchain technology would result in a slight compromise in performance. However, through our experimentation, with the help of Edge computing, we have demonstrated that with minimal compromise in terms of response time, we can achieve significant contribution in terms of security and privacy. Our empirical setup includes ParamShavak super computer as Cloud server, mqtt broker on Cloud VM, i5 system as an Edge node containing continuously running python script. In the future, one may work in two facets. First, access control(authentication) policies can be introduced in this existing mechanism to offer role-based or capability-based power to the stakeholders. Second, our prototype can be implemented in Healthcare,

Journal of Ecohumanism
2024
Volume: 3, No: 7, pp. 5127 – 5136
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i7.4620

Aviation, Agriculture, etc. wherein urgent response time is mandatory without compromising the security concerns.

Based on the above results and experimentation this work can be extended to induce Blockchain in the existing IoT network for proper logging and auditing the IoT commands in the Blockchain. This can be used for pattern recognition, schedule activities, access control or adding security to the IoT network.

References

Cdac (2016). World's first compact and energy efficient supercomputer launched by c-dac, june 2016, [online] available: http://cdac.inlindex.aspx?id=pk_pr_prs_r1223.

Guo, g. Shen, z. Huang, y. Yang, m. Cai and l. Wei, (2023). "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.

Farhan, laith & shukur, sinan & alissa, ali & alrweg, mohmad & raza, umar & kharel, rupak. (2017). A survey on the challenges and opportunities of the internet of things (iot). 1-5. 10.1109/icsenst.2017.8304465.

Hu, vincent c. (2022). Blockchain for access control systems. Nist ir 8403, national institute of standards and technology (u.s.), 26 may 2022, p. Nist ir 8403. Doi.org (crossref), https://doi.org/10.6028/nist.ir.8403.

Idc (2025). 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.

Pan, j. Wang, a. Hester, i. Alqerm, y. Liu and y. Zhao (2019). "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.

Wright, m. Martinez, u. Chadha and b. Krishnamachari (2018). "smartedge: a smart contract for edge computing," 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, 2018, pp. 1685-1690.

Ali, m. Vecchio and f. Antonelli (2018). "enabling a blockchain-based iot edge," in ieee internet of things magazine, vol. 1, no. 2, pp. 24-29, december 2018.

Novo, (2018). "blockchain meets iot: an architecture for scalable access management in iot," in ieee internet of things journal, vol. 5, no. 2, pp. 1184-1195, april 2018, doi: 10.1109/jiot.2018.2812239.

Param shavak (2016). Supercomputing solution in a box, june 2016, [online] available: http://www.cdac.inlindex.aspx?id=hpc_ss_param_shavak.

Roy, utsa; ghosh, nirnay (2023). Bloac : a blockchain-based secure access control management for the internet of things. Techrxiv. Preprint. Https://doi.org/10.36227/techrxiv.23282816.v1

Ding, j. Cao, c. Li, k. Fan and h. Li,(2019). "a novel attribute-based access control scheme using blockchain for iot," in ieee access, vol. 7, pp. 38431-38441, 2019.

Sun, r. Du, s. Chen and w. Li, (2021). "blockchain-based iot access control system: towards security, lightweight, and cross-domain," in ieee access, vol. 9, pp. 36868-36878, 2021, doi: 10.1109/access.2021.3059863.

Sahmim, syrine & gharsellaoui, hamza & bouamama, sadok. (2019). Edge computing: smart identity wallet based architecture and user centric. Procedia computer science. 159. 1246-1257. 10.1016/j.procs.2019.09.294.

Sikder, amit kumar & petracca, giuseppe & aksu, hidayet & jaeger, trent & uluagac, selcuk. (2018). A survey on sensor-based threats to internet-of-things (iot) devices and applications.

Wang, huaimin & zheng, zibin & xie, shaoan & dai, hong-ning & chen, xiangping. (2018). Blockchain challenges and opportunities: a survey. International journal of web and grid services. 14. 352 - 375. 10.1504/ijwgs.2018.10016848.

Zhang, s. Kasahara, y. Shen, x. Jiang and j. Wan, (2019). "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.