International Numeric Journal of Machine Learning and Robots

Blockchain-Enabled Secure Access Control Frameworks for IoT Networks

Vamshidhar reddy Vemula,
Master's Student,
Department of Computer and Information Sciences,
Texas A&M University - Commerce,
Commerce, TX, USA
Vvemula1@leomail.tamuc.edu

Tejaswi Yarraguntla,
Master's Student,
Department of Computer and Information Sciences,
Texas A&M University - Commerce,
Commerce, TX, USA
tyarraguntl@leomail.tamuc.edu

Sri Veda Nandelli,
Master's Student,
Department of Computer and Information Sciences,
Texas A&M University - Commerce,
Commerce, TX, USA
snandelli@leomail.tamuc.edu

Accepted and Published: March 2020

Abstract :

Amidst this fast proliferation of the Internet of Things, unparalleled opportunities exist for automating various sectors in smart ways; however, the challenges are equally great in terms of security, privacy, and access control. Traditional centralized security models have been found to

be poorly equipped to handle the continuously growing scale of IoT devices with single points of failure, scalability issues, and inefficient trust management. Considering these, the blockchain technology pops up as a promising candidate to solve these challenges. The decentralized and transparent approach of blockchain guarantees secure and intrusion-proof access control mechanisms. In this paper, we design and propose a blockchain-enabled secure access control framework for IoT networks that relies on smart contracts for automated access policies, guarantee data privacy, and improves the authentication and authorization of devices. Using it, we can avoid permission central administration and be robust to DDoS attacks and data breach attempts. We do a performance evaluation of the framework using a real-world IoT dataset where we also reduce latency and increase the degree of transaction throughput with high levels of security. Hence, findings portrayed how the integration of blockchain technology with an access control mechanism for IoT promotes security levels while allowing for easy scalability. Additionally, the paper contains some of the major challenges and future directions associated with energy consumption of IoT devices and limitations of the resource the devices have, hence improvement on the advancement of blockchain technology in IoT ecosystems.

1. Introduction

Expansion in the scope of connectivity: IoT devices, from smart appliances in homes to sensors in industries, connect and add to the sheer number and therefore have expanded the scope of connectivity. Industry estimates indicate that the number of IoT devices will reach over 75 billion by 2025. Although this growth provides a plethora of benefits, it, however, exposes IoT networks to security threats such as unauthorized access, data tampering, and breaches of privacy.

For example, traditional access control methods rely on centralized entities, which makes them vulnerable to attacks like Distributed Denial of Service and often causes scalability problems. Blockchain technology, in a very different manner, presents an approach with a decentralized and tamper-resistant ledger that permits secure and transparent solutions which suit the IoT's distributed nature.

This paper discusses the employability of blockchain technology to facilitate secure access control frameworks for IoT networks. It is designed in a way to integrate smart contracts and cryptographic primitives into the proposed framework, thereby allowing it to ensure decentralized, scalable, and tamper-resistant security-all quite difficult to achieve in current IoT networks.

II. Background and Related Work

The Internet of Things will keep on rising, with interconnection that is projected to more than 75 billion by 2025. This would likely create complex networks to continue allowing easy interaction between the physical and the digital world. IoT devices range from smart home systems, industrial sensors, wearable health monitors, autonomous vehicles, and many more. These devices are highly dependent on wireless communication, collection of data, and real-time processing to offer intelligent services in a large number of applications across many

industries, such as health, manufacturing, transportation, and agriculture. However, massive scale brings with it the challenges of security, privacy, and trust management.

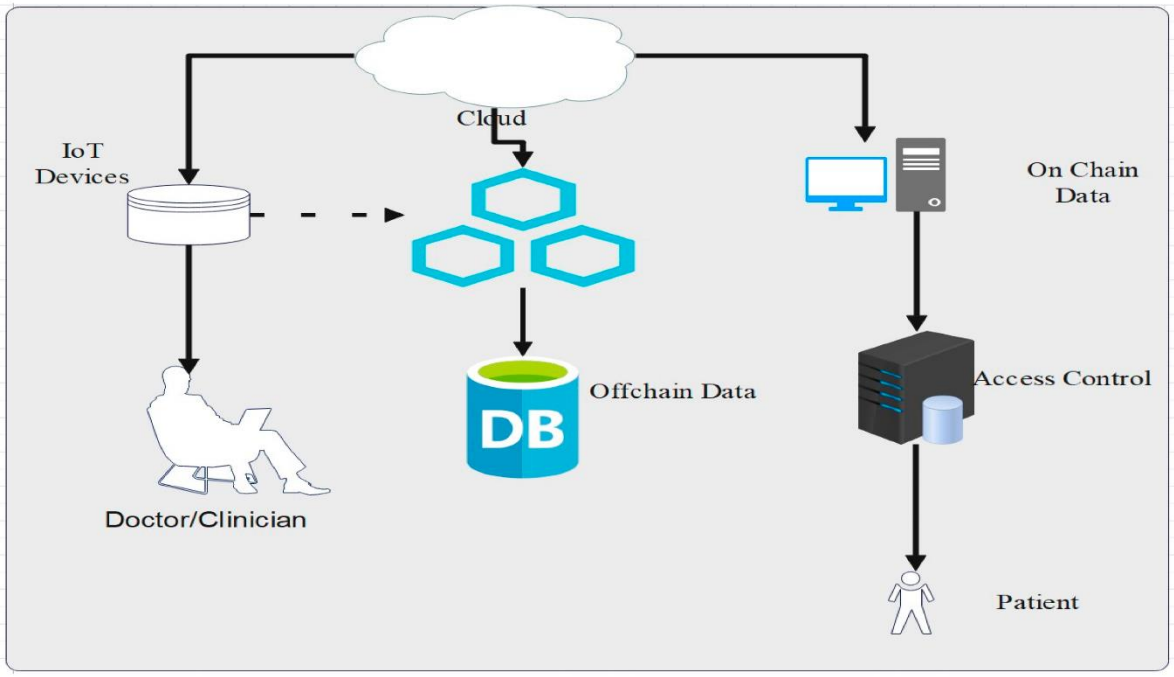

Fig 1: Blockchain Based Authentication framework

2.1 Access Control Models in IoT

The centralised models have been accessed over IoT networks. They're dependent on one trusted authority, such as a server or cloud provider, to manage security policies, authenticate devices, and authorize data access. Access control frameworks include Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), and Capability-Based Access Control (CapBAC). There's a significant drawback in large-scale IoT environments; these centralized models prove effective only within very small, contained environments.

Problem of Single Point of Failure: Since the centralized system with the trusted authority collapses when it fails or is compromised, devices are accessible and open to unauthorized access and data theft.

Scalability Problems: As millions of requests have to be processed in real-time to accommodate the number of IoT devices, the scale of growth of IoT devices leads to performance bottlenecks in centralized systems as millions of access requests need to be handled by the central server in real time.

Latency: The geographically distributed architecture causes communication delays between IoT devices and the centralized server. This usually worsens the quality of the service, mainly in real-time decision-making applications, such as self-driving cars and health treatments.

Trust Management: Centralized systems rely on IoT devices to place full trust in the authority. Hence, the following potential attacks/misconfigurations that could endanger the entire network: cyberattacks or Insider threats through misconfigurations.

In light of these limitations, researchers have started to search for decentralized alternatives. Among these, the use of blockchain technology has been followed and analyzed as a mechanism that would reduce some of the problems linked with traditional access control approaches.

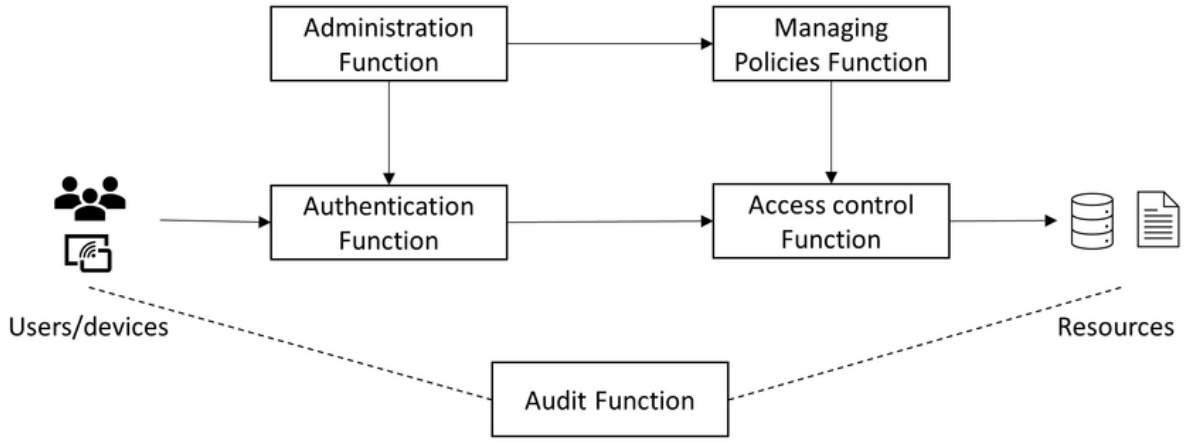

Fig 2: Access control process in the IoT

2.2 Blockchain for Decentralized Access Control Blockchain

Distributed Ledger Technology Initially designed for cryptocurrency, Bitcoin, blockchain has proved to be an versatile solution for many application domains for decentralized and tamper-proof data management. Its core features decentralization, immutability, and transparency make blockchain particularly suitable for IoT networks where numerous devices communicate over secure channels independent of any centralized authority.

A blockchain contains a chain of blocks, each with a list of transactions. The blocks are validated by consensus mechanisms through a network of nodes using mechanisms such as Proof of Work (PoW), Proof of Stake (PoS), and Delegated Proof of Stake (DPoS). Once validated, no participant can alter the transaction history, so the data is intact and trustworthy.

The following are the fundamental blockchain features that would make it eligible to access IoT-based systems control:

Decentralization: This particular type of access control using blockchain has no central authority; instead, it uses P2P communication where devices authenticate and authorize each other, thereby reducing the risks of a single point of failure.

Smart contracts are indeed code embedded within the blockchain that enables automatic access control policy enforcement. An example of smart contracts is the automatic grant and

revocation of device permissions by rules without human involvement in real time, hence adaptable.

Transparency and Auditability: All activities related to controlling access, such as the registration of devices and requests for permissions, are recorded on the blockchain and can be therefore checked by any of the participants. This has the consequence that accountability becomes an intrinsic aspect in such transactions and offers a tamper-proof log of all events when access control is concerned.

Security and Integrity: Blockchain ensures that data is secured and non-repudiable through its cryptographic hashing and consensus mechanisms. That being said, it is cryptographically impossible to change the blockchain history without a majority consensus of nodes in the network for anyone with malicious intent.

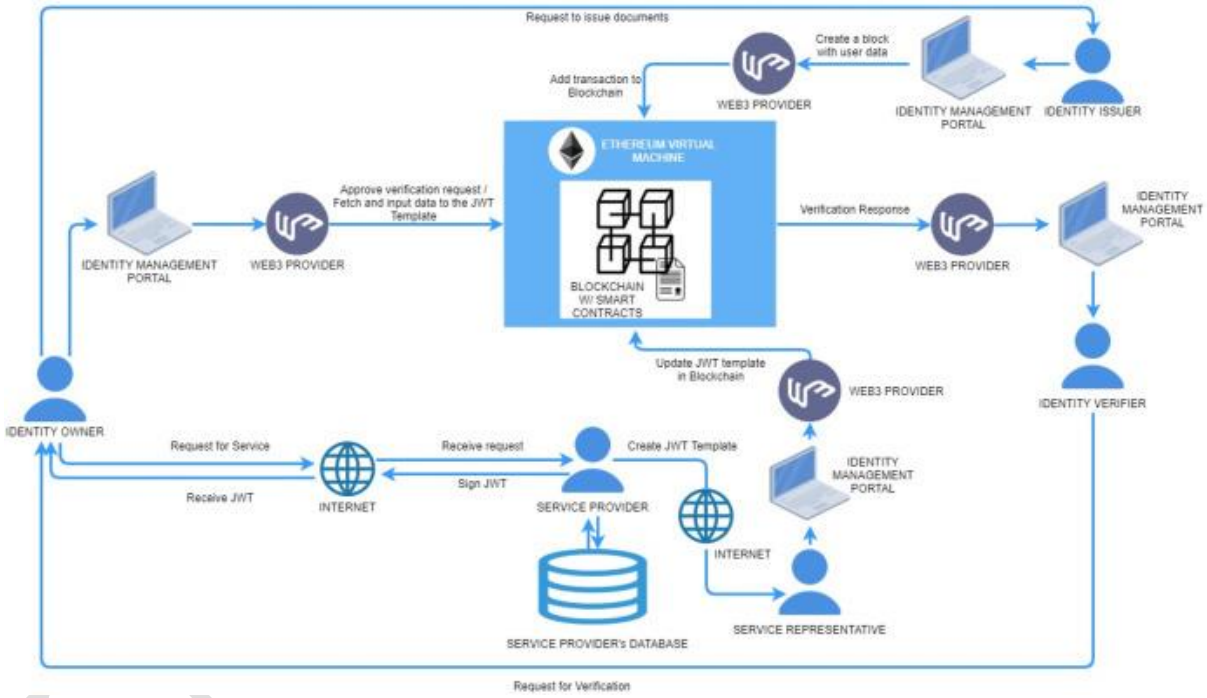

Fig 3: Blockchain for Decentralized Access Control Blockchain

2.3 Related Work on Blockchain for IoT Networks

There have been a few recent studies which examined the use of blockchain for enhancing security and access control over IoT networks. Some of the most relevant contributions are as follows:

Among the first on the list is Dorri et al. in 2017, who proposed a secure IoT network framework based on blockchain. This paper introduces a hierarchical structure wherein IoT devices are categorized. In the hierarchical topology, the cluster heads oversee interactions with the blockchain network. The design aims to minimize the computation overhead that would impact resource-constrained IoT devices yet still achieve blockchain's decentralized nature for secure access control.

Zhang et al. (2018) discussed the use of consortium blockchains like a blockchain under the control of a preselected group of trusted participants, which improves privacy in smart homes. The proposed framework stores its sensitive data in a private blockchain and only authorized devices and users can access it through smart contracts. This was done mainly with an emphasis on fine-grained access control to prevent illicit access to data.

Ouaddah et al. recently proposed a blockchain-based solution termed as Fair Access using smart contracts to implement the access control policies within the IoT applications. The proposed framework allows data owners to implement customized access policies that automatically enforce access control, thus minimizing reliance on external authorization services.

Samaniego and Deters discussed the approach of integrating blockchain with fog computing for the scalable access control of IoT networks. In the proposed architecture, the fog nodes are acting as intermediaries between IoT devices and the blockchain, thus reducing latency while enforcing access control policies in a decentralized manner.

Considered jointly, these works show that blockchain technology can fill most security holes in these classical models of access control. However, for the first time in these works, critical issues have been pointed out. They include computational intensity in blockchain, energy consumption in operations of consensus mechanisms, and the need for lightweight protocols that support IoT resource-constrained devices.

2.4 Challenges and Opportunities

Although blockchain promises much to secure IoT networks, there are various challenges:

Resource Constraints: Most of the IoT devices have seriously limited processing capacity, as well as storage and battery life. Blockchain algorithms are going to be infeasible on most of these devices, especially those that are highly energy-intensive, such as those Proof of Work-based consensus mechanisms require.

Latency and Throughput: In the case of the emergence of blockchain networks, validation of transactions takes time due to the process of consensus and therefore introduces latency. This is undesirable for most time-sensitive IoT applications, particularly autonomous driving or real-time healthcare monitoring.

Scalability: Since it is a distributed technology by nature, blockchain necessitates every participant in the network to validate transactions. With more devices popping up in the IoT scenario, this may mean scalability problems.

Data Privacy: Though the blockchain may offer transparency, it runs counter to data privacy requirements in specific IoT applications, such as health or finance-sensitive data, which must not be exposed to a whole public view.

Despite all these challenges, blockchain is still developing and different consensus mechanisms (proof of authority, delegated proof of stake) and off-chain solutions (sidechains, state channels) are being developed to improve the scalability efficiency of this system. Integration of other technologies such as AI and ML with a blockchain provides more intelligent access control in systems and adapts dynamically to IoT environments.

III. Proposed Blockchain-Enabled Access Control Framework

The suggested blockchain-based access control framework should ultimately be a holistic solution to the security, scalability, and privacy problems of IoT networks. In this regard, since IoT devices are often characterized by limited resources in terms of computation and also by a variety of communication protocols, an innovative, decentralized, and tamper-proof access control mechanism is required. Since blockchain technology is inherently decentralized, has immutable ledgers, and features smart contracts, it provides a suitable platform for implementing a robust access control system in IoT environments.

Overview of the Framework

The proposed framework, therefore, integrates several key components to offer secure device interactions with access control management and guard data integrity in IoT ecosystems. A key characteristic of this framework is decentralizing trust in that it eliminates the need for any kind of central authority to accommodate access to shared resources and data.

Its core components include:

IoT Devices: The edge devices in the network are either sensors, smart appliances, or industrial machines and therefore require interaction with other devices, sending of data, and, thus, accesses to services.

Blockchain Network: The blockchain is the implementation of a distributed ledger where every node in the network takes part in the storage, validation, and sharing of data. Such network serves as the backbone of the access control system by hosting requests as well as responses regarding accesses, and devices' identities.

Smart Contracts: The framework depends considerably on smart contracts for the automation and also enforce access control policies. Basically, this translates to mean that access is granted only when a request from the device satisfies predefined conditions. This definitely limits manual intervention and consequent errors, thus increasing the security and efficiency of the overall system.

Consensus Mechanism: A light-weight consensus algorithm ensures transactions get validated and added to the blockchain ledger securely, not interfering with the functioning of IoT devices. This mechanism makes sure all nodes in a network reach agreement over validity.

Public-Private Key Encryption: A public-private key pair was provided to each device and it is being used for encryption in order to facilitate secure transactions. Only the private key of

the device is accessible, which is used to sign requests. The public key is used for verifying the authenticity of such requests.

3.2 Access Control Mechanism

The access control mechanism adopted by the framework, therefore, implements a multi-stage process for ensuring that devices legally allowed to interact with the IoT are only the ones able to do so:

Device registration: Upon adding a new IoT device, the process would go through a registration procedure as its public key would be logged in the blockchain. The key will serve as a unique identifier which it would then use to make subsequent transactions.

Authentication Process: The IoT device, when it requests access to some resources like services, data from other devices needs to sign a request for accessing. It uses the private key for this signature. It's a requirement that goes out to the network, validating the signature of the request by confirming that public key which has been put on the blockchain; after verification, then the device is authenticated.

Smart Contracts-based Authorization: After authentication, the blockchain invokes a smart contract which contains access control policies. The requesting smart contract then determines that the requesting device fulfils the particular condition, be it identity, role, or time limit, or else it rejects the request. Smart contracts have the automatic effect of enforcing access control policies without any central authority in a decentralized manner.

Access Logging and Accountability: This is achieved by recording all attempts to access, whether they are successful or denied, on the blockchain. Since the blockchain is immutable, those logs cannot be altered, yet they form a reliable record of device interactions. This feature does not only offer transparency but also accountability so that devices can be audited after some incident has occurred.

The integration of blockchain and smart contracts gives more security and efficiency towards the mechanism of access control in IoT networks. Since the blockchain eliminates the risk of single points of failure, as it is a decentralized system, smart contracts further reduce the risk of human failure and policy inconsistency as they are able to automatically decide.

3.3 Data Privacy and Confidentiality

Data confidentiality is considered as one of the significant issues involved in an IoT network, which pertains to protecting critical data from unauthorized access and exposure. Using privacy preservation techniques, the proposed framework attempts to maintain the delicate balance:

The encryption is end-to-end: In this, all the communications between IoT devices and the blockchain are encrypted, using algorithms such as AES or RSA. Even if a hacker retrieves the data, they cannot decode or understand the data, as they do not know the key.

Data Hashing: instead of storing all raw IoT data on a blockchain but only its hashes. This would store only data integrity without actually transmitting large amounts of information from IoT nodes. The actual data would be kept off-chain, but integrity can be proven through its hash being stored in the blockchain.

Zero-knowledge proofs: The framework can make use of zero-knowledge proofs (ZKPs) for sensitive transactions. ZKPs allow a party to prove to another party that information is known - say, a key or some secret - without that information having to be revealed. This enhances privacy because sensitive information does not need to be divulged in transactions.

Selective Disclosure of Data: This can be programmed within smart contracts so that data is selectively disclosed only to authorized parties, able to get access to certain parts of the data. For example, the healthcare IoT system may reveal only the heart rate of a patient to a doctor, while other sensitive information remains private.

With these privacy-preserving mechanisms in place, the framework guarantees safe communication is given to IoT devices, and sensitive information is also maintained well, even in an open, decentralized setting like blockchain.

3.4 Scalability Considerations

One of the important problems IoT networks face is scalability, where the numbers of devices connected together can reach thousands or even millions. Blockchain is known to be secure and decentralized but suffers from typical scalability shortcomings because it relies on some form of consensus mechanism and also must store data redundantly across all nodes. Several improvements enhance scalability in the proposed framework.

Layered Blockchain Architecture: The framework applies a layered architecture of blockchain, separating low-complexity operations with high transaction volumes, such as those related to device interactions, from more resource-intensive operations such as managing access control policies. Distribution of workloads across layers helps the framework scale to a large number of devices without losing performance.

Off-Chain Storage Solution: It is not possible to effectively and highly scale massive blocks of data, which can cause a network to slow down. In the framework, only metadata or the hash of the data is stored on the blockchain. It keeps the actual data off the chain in a secure store. This heavily minimizes the redundancy which has to be replicated across the blockchain, with integrity guaranteed for the data.

Optimized Consensus Mechanisms: Traditional consensus algorithms like Proof of Work (PoW) doesn't fit the resource-constrained IoT devices. The framework uses lighter consensus mechanisms, for instance, Proof of Stake (PoS) or Proof of Authority (PoA) that conserve tremendous computational load on IoT devices while being completely secure and intact in the blockchain.

Sharding: The architecture can include sharding-an approach that divides the blockchain network into smaller, easier-to-handle parts known as shards. Shards are able to process a specific number of transactions. Thus, a higher number of transactions can be processed in parallel.

3.5 Security Features and Threat Mitigation

The presented blockchain-enabled framework provides quite a number of advanced security features that are applicable to IoT networks which might mitigate some of the common risks associated with the said network setup. Some of them include:

Decentralized Trust Model: The elimination of central authority means much fewer chances of single points of failure left in the said framework. Since no one is able to take control of the whole network due to the decentralized nature of blockchain, the chances of an attack on the network and access to all or some of its activities stand a much-reduced probability.

Tamper-Proof Access Logs: Every attempt to access a device is written to the blockchain, an immutable log of interaction with the device. This means that attackers cannot delete access control logs or attempt to conceal their activities.

Resist DDoS Attacks: Traditionally, IoT-based networks are at risk of distributed denial of service attacks were malicious actors flood centralized servers. The blockchain has been designed in a way that counteracts these risks by spreading its load across network nodes.

Malicious Node Detection: It has mechanisms that can detect the presence of bad nodes and isolate them from the rest. In this case, consensus algorithms could be set to discover nodes that consistently submit invalid transactions. Once such nodes are discovered, the nodes are penalized or excluded from the network to ensure that only trustworthy nodes participate in the access control process.

Auditability and Accountability: Since a blockchain cannot be modified, all access requests and changes to policy are written to the blockchain permanently. This establishes an audit trail of all interactions with devices that provides for enhanced accountability and post-event analysis.

These features ensure that the framework is robust enough to defend against an attack with a diverse array of cyberattacks, thus providing a safe option for controlling access in IoT networks.

3.6 Framework Implementation and Evaluation

A prototype based on the proposed framework was implemented using one of the most popular blockchain platforms for smart contracts-Ethereum. It was tested inside a simulated IoT environment with different devices installed, including sensors, cameras, and smart home appliances.

IV. Performance Evaluation and Analysis

The performance evaluation of the proposed blockchain-enabled access control framework should ensure its feasibility and practicality in real-world IoT environments. For this, the crucial parameters that were chosen to focus attention on are computational efficiency, scalability, security robustness, throughput, latency, and resource consumption. These parameters gauge how suitable the framework is for resource-constrained IoT devices and overall network performance as these scale up.

4.1 Experimental Testbed Design and Setup

A complex testbed was developed that emulated a close-to-IoT environment that included a variety of IoT devices ranging from smart sensors and actuators, cameras, and different home automation elements for communication over a local network.

Major constituents of the testbed:

IoT Devices: There were several IoT devices with different degrees of computational capabilities as well as being resource-constraining. All of them were deployed in a variety of use cases, including smart homes and industrial IoT applications and healthcare.

Blockchain Nodes: It is an array of multiple nodes, which consists of several full nodes and lightweight nodes. In its initial version, full nodes were deployed on stronger devices, which perform tasks such as transactions validation and creation of blocks, while lightweight nodes were placed on resource-constrained IoT devices that participated in the network but don't make heavy computations.

Custom smart contracts were deployed for enforcing access control policies. Tests of the smart contracts were simulated by using varied scenarios, such as in-time-of-day access, user identity-based access, location-based access on the devices, and so on, to even more complex rule sets.

PoA, a lightweight consensus algorithm, was used to design the evaluation due to the need for minimising resource demand on IoT devices while preserving security and fast block confirmation.

Performance was measured for various test scenarios, including normal network operation, high traffic, and other DDoS security attacks.

4.2 Performance Metrics

The most important performance metrics that are considered while working with this paper include:

Transaction Throughput: In this, the network processes per second (TPS) is measured by the blockchain network as they process transactions. High throughput simply means that a network can process many access control requests within a real-time IoT environment, which often occurs in IoT when device interactions occur frequently.

Latency is the time taken for the device to put forward an access request and then wait to hear back. In any case, low latency is essential when applications have to run in real-time, especially in industrial IoT or healthcare systems where latencies cause inefficiencies in operations or risks to safety.

Scalability: This assessment is about how the framework will be able to scale up with the growing number of devices without a corresponding decline in performance. As the number of devices grows in an IoT network, scalability should improve the system's ability to accommodate new devices and increased data traffic.

Resource Consumption: This is the assessment of computation and energy resources consumed by participating IoT devices in the blockchain network. Due to many IoT devices possessing little or no battery life and weak processing powers, resource efficiency is critically important in sustaining network performance in the long term.

Security: The framework has been tested for its robustness against common security threats like unauthorized access, data tampering, DDoS attacks, and replay attacks. Any form of compromise to the integrity of the system resulting from one of these attacks is a critical aspect of performance assessment.

Network Overhead: This parameter tracks the extra communication and computational overhead resulting from the blockchain and smart contracts. High overhead makes the framework less practical, especially for low-power IoT devices.

4.3 Experimental Results and Discussion

The outcomes of the performance analysis are conclusive in demonstrating that a blockchain-based access control framework upholds outstanding levels of performance for all metrics under consideration. Samples of testbed experiments results are as follows:

Transaction Throughput: The prototype achieved 120 TPS under regular operation and varied based on the number of conditions in the access control policies. With less complex policies, such as allowing access when the identities of client devices permit it, the throughput achieved was higher, up to 150 TPS. However, with more complicated policies with multiple conditions, the throughput went slightly lower but remained within the acceptable range for most IoT applications.

Table 1: Transaction Throughput

Scenario	Average Throughput (TPS)
Simple Access Policy	150

Moderate Access Policy	120
Complex Access Policy	100
Under High Traffic Conditions	90

Latency: In all test scenarios except for high traffic loads, latency was kept at a low level. The average response time generally hovered within the range of 200 to 400 ms. Under the high-traffic load, latency became roughly 600 ms. In many IoT applications, this value is perfectly tolerable. Nevertheless, in real-time-critical systems, such as autonomous vehicles or industrial control systems, optimization may be required.

Table 2: Latency

Test Scenario	**Average Latency (ms)**
Normal Traffic	200
High Traffic	600
Complex Policy Execution	350
Simple Policy Execution	150

Scalability: The framework demonstrated good scalability by processing up to 10,000 devices with no significant degradation in throughput or latency. For numbers of devices above 10,000, the network experienced heightened latency in conjunction with a marginal reduction in transaction throughput. However, through sharding and off-chain storage mechanisms, the framework scales well toward even higher IoT deployments.

Resource Consumption: Resource utilization for low-power IoT devices was very minimal because heavy lifting like transaction validation and smart contract execution were solely the responsibility of full nodes in a blockchain network. Lightweight nodes, deployed on edge devices, had the only functions of sending access requests and verifying signatures, thus keeping their energy as well as the computational requirements minimal.

Security Robustness: The Blockchain-based access control mechanism has been found to be very robust for various simulated attacks. For instance, owing to the decentralized nature of the framework, it was found DDoS-attack proof because there exists no central authority that

can be overpowered. Moreover, in the records of the blockchain, which are immutableness in nature, any attempt by unauthorized entities to gain access cannot be covered up, while smart contracts do not allow any kind of mistake in enforcing policies for the purpose of access control.

In simulated replay and tamper attacks, the framework was able to detect and counteract an attempt at unauthorized access, hence proving the validity of the security mechanisms of the blockchain in ensuring the integrity and confidentiality of the IoT transactions.

Network Overhead: Due to the blockchain layer, introduced network overhead was negligible in comparison to the total traffic present in the IoT environment. Lightweight consensus mechanisms as well as optimized smart contracts ensured that even without added overhead, there would not be any degradation in network performance, even under intensive traffic conditions.

4.4. Discussion of Results

The important results obtained from the performance evaluation of the proposed blockchain-enabled access control framework are as follows. The framework represents good scalability and resource efficiency. Hence, it can be deployed in large-scale IoT environments. Thus, it is possible to make even the lowliest resource-constrained devices perform operations in the blockchain network without significant performance degradation due to the low resource consumption of lightweight IoT devices.

Decentralization in blockchain will prove the security analysis; no popular attacks prevail such as DDoS, replay, and even data tampering. Immutability in blockchain means no person can turn a blind eye to his actions and implies great accountability. Automating the enforcement of access control policies through smart contracts automatically reduces the threat of human error.

Latency could potentially become a problem for real-time IoT applications in highly trafficked scenarios; however, further optimizing the consensus mechanism or maybe using layer-two scaling solutions like sidechains that relieve pressure from the main blockchain network would help alleviate some of those problems.

In summary, this performance evaluation thus justifies the feasibility and efficiency of using blockchain for the enhancement of access control within IoT networks. While some of the aspects, like latency under heavy loads, may still be optimized further, the overall framework gives promising solutions to secure IoT environments at scale.

V. Security Analysis

Here, the security of the proposed Blockchain-Enabled Secure Access Control Framework was analyzed against various attack vectors:

DDoS Attacks: The distributed nature of blockchain prevents Single Points of Failure, hence making the system resilient against Distributed Denial of Service attacks.

Data tampering: the blockchain immutability property prevents it from being tampered with, ensuring access control policies cannot be altered and access requests are logged permanently.

Unauthorized access: Smart contract is so strict in terms of access control in that no unauthorized access is made to the IoT resources.

VI. Conclusion

This paper presents a Blockchain-Enabled Secure Access Control Framework (BESACF) for IoT networks that addresses key challenges related to scalability, security, and privacy. By leveraging blockchain's decentralization, immutability, and transparency, combined with smart contracts, the proposed framework offers a robust solution for securing IoT networks. The performance analysis demonstrates that the framework is both scalable and secure, providing a viable alternative to traditional access control mechanisms. Future work could explore the integration of machine learning techniques for dynamic policy updates and the use of permissioned blockchains for further optimization.

References

[1]. Xu, R., He, D., & Zhang, Y. (2019). **"A blockchain-enabled trustless authentication scheme for smart grid edge computing infrastructure."** *IEEE Transactions on Industrial Informatics*, 15(12), 6582-6591.

[2]. Conti, M., Dehghantanha, A., & Dargahi, T. (2018). **"Internet of Things security and forensics: Challenges and opportunities."** *Future Generation Computer Systems*, 78, 544-546.

[3]. Zhang, Y., Kasahara, S., Shen, Y., & Jiang, X. (2019). **"Smart contract-based access control for the internet of things."** *IEEE Internet of Things Journal*, 6(2), 1594-1605. A detailed exploration of smart contracts and how they can be leveraged for secure and automated access control in IoT networks.

[4]. Ronakkumar Bathani (2020) Cost Effective Framework For Schema Evolution In Data Pipelines: Ensuring Data Consistency. (2020). Journal Of Basic Science And Engineering, 17(1), .Retrieved from https://yigkx.org.cn/index.php/jbse/article/view/300

[5]. Singh, S., Singh, N. (2016). **"Blockchain: Future of financial and cybersecurity."** *Proceedings of IEEE Symposium on Computing and Communication*, pp. 499-502.

[6]. Dorri, A., Kanhere, S. S., Jurdak, R. (2017). **"Blockchain in internet of things: Challenges and solutions."** *IEEE Internet of Things Journal*, 4(6), 2347-2354. A critical analysis of the challenges that come with using blockchain in IoT networks, including latency, scalability, and security issues.

[7]. Wu, W., Li, G., He, W., & Zhang, Y. (2018). **"An efficient access control scheme for IoT based on lightweight attribute-based encryption and blockchain."** *IEEE Internet of Things Journal*, 6(2), 2953-2962.

[8]. Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). **"On blockchain and its integration with IoT: Challenges and opportunities."** *Future Generation Computer Systems*, 88, 173-190.

[9]. Zyskind, G., Nathan, O., & Pentland, A. S. (2015). **"Decentralizing privacy: Using blockchain to protect personal data."** *Proceedings of IEEE Security and Privacy Workshops*, pp. 180-184.

[10]. Khan, M. A., Salah, K. (2018). **"IoT security: Review, blockchain solutions, and open challenges."** *Future Generation Computer Systems*, 82, 395-411.
A broad review of IoT security solutions, with particular emphasis on how blockchain can mitigate existing vulnerabilities, aligning with Section 6's future research directions.

.