Vol 5, Issue 12, December 2025 www.ijesti.com E-ISSN: 2582-9734
International Journal of Engineering, Science, Technology and Innovation (IJESTI)

Enhancing IoT Security Through Blockchain Based Access Control and Smart Contract Defense Mechanisms

Dr. Abhishek Tarafder

Email - abhishek.tarafder@gmail.com

ABSTRACT

Because the IoT is very popular, it has become a big problem to store a lot of IoT data while keeping people's privacy protected. In general, the access control mechanism's job is to keep those who aren't supposed to have access from acquiring private information. However, traditional methods of controlling who may access data have several big issues. For example, they can only manage relatively coarse-grained access control, which can cause difficulties with centralisation and trust. This article proposes a framework for secure IoT settings that is built on the blockchain and employs smart contracts as a way to protect against these problems. The recommended model uses Ciphertext-Policy Attribute-Based Encryption (CP-ABE), which is an attribute-based encryption mechanism, to make sure that access control is both context-aware and very precise. A hybrid blockchain design that combines public and consortium blockchains makes authentication, transparency, and scalability better. Smart contracts make it possible to automate permission, enforce security rules, and get rid of the need for a central authority. The proposed method enhances security, transparency, and resilience, as per experimental evaluation, while maintaining appropriate computational and transaction costs.

Keywords: *Blockchain, Smart contract, Access control, Security, Attribute.*

I. INTRODUCTION

When it comes to interacting with our physical environment, the Internet of Things (IoT) has changed everything. Internet of Things (IoT) systems enable data transmission across diverse devices, opening up new possibilities for use in smart homes, smart factories, smart cities, and industrial automation. New concerns, especially with regard to security and privacy, are brought forth by these platforms. There are a lot of devices in IoT systems that might not have a lot of RAM, CPU, or battery life, which makes it hard to use the usual security measures. There is a need to secure IoT systems since they may store sensitive information that should not be accessible to unauthorised parties.

Secure and private Internet of Things (IoT) devices may soon be a reality thanks to blockchain technology. Blockchain technology eliminates middlemen in data verification and sharing by creating a distributed ledger. The encryption used by a blockchain ensures that transactions cannot be intentionally altered or removed once recorded. For Internet of Things (IoT) systems that include several parties with competing interests, this makes blockchain technology a promising solution for security.

When it comes to protecting the Internet of Things, access control measures are king. By verifying the credentials of the asking users or services, access control can approve or reject their requests to access resources. A resource's access policy may specify who has permission to use it, when, and what they can do while they're there. The Internet of Things (IoT) and blockchain technology, when combined, could provide several benefits for distributed ledger security. Still, implementing efficient access control in Blockchain-enabled Internet of Things (BIoT) systems is no picnic. We need a strong, context-aware approach to safeguarding the security and privacy of resources in BIoT systems because current access control mechanisms like DAC, RBAC, ABAC, and PBAC aren't always up to the task of dealing with the ever-changing and context-dependent nature of IoT environments.

There are trust, scalability, and security issues caused by the centralisation of current access control systems. A centralised system has one potential weak spot—the authority or organization in charge of making decisions and enforcing access controls—that might be the focus of an attack. Also, because of how concentrated control is, these systems could be difficult to scale to support a huge number of people or devices. Better security, decentralisation, and resilience may be achieved by utilising smart contracts and blockchain technology in BIoT access control systems. Smart contracts are digital agreements recorded on a blockchain with the ability to carry out predetermined tasks in response to the occurrence of certain events. For this reason, smart contracts offer a decentralised and automated way to govern access to the Internet of Things (IoT), manage permissions, and enforce restrictions.

II. REVIEW OF LITERATURE

Senturk, Arafat & Terazi, Selami. (2023) A new partnership between Blockchain and the Internet of Things (IoT) has arisen to solve issues with data integrity, transparency, and security in IoT devices. Distributed and decentralised ledger technology (blockchain) guarantees secure data transfer between Internet of Things (IoT) devices and safeguards against data tampering. Smart contracts allow for automatic and trusted transactions, which improves the security and openness of Internet of Things applications. When it comes to improving the trustworthiness and efficiency of the IoT ecosystem, Blockchain is an essential tool. In this research, we summarise previous work that has shown how Blockchain technology might improve Internet of Things (IoT) security and offer some recommendations for moving forward. An Internet of Things (IoT) cop monitoring framework with advanced security features is one of the suggested solutions. Other options include scalable frameworks for secure transactions in dynamic applications, frameworks based on Hyperledger Sawtooth for secure logging of industrial activities, and specialised access control mechanisms like Trust-Based Access Control Mechanism (TABI). Further efforts to strengthen the security of the Internet of Things include authentication systems, security models, and access control protocols that are built on the blockchain. While the majority of published works address present difficulties in integrating the IoT with Blockchain, they do highlight potential avenues for further study. We provide a quick overview of these studies and include the essential ones in a table. The goal is to provide the groundwork for future professionals in this area in this way.

Barazanchi, Israa & Hashim, Wahidah. (2023) Due to their decentralised nature, limited processing capacity, and reliance on centralised security mechanisms, the rapidly expanding Internet of Things (IoT) devices present substantial security concerns. Problems with traditional Internet of Things (IoT) security systems include a lack of scalability, a single point of failure, and susceptibility to distributed denial of service (DDoS) assaults. Additionally, they need feasible security measures. The distributed, irreversible, and transparent blockchain technology has recently surfaced as a possible answer, offering superior protection for Internet of Things (IoT) settings. To lessen the impact of potential security breaches in IoT networks, this research suggests a blockchain-based security approach. For the most fundamental tasks, like authenticating devices, checking data integrity, and controlling access, the system relies on smart contracts. In order to maximise network availability, decrease connection latency, boost device dependability speeds, and decrease power consumption, the research primarily aims to build IoT security solutions. When compared to current Internet of Things security protocols, the survey findings reveal substantial improvements. With a detection rate of 95% for unauthorised access and support for 1000 devices—double the capacity of existing models—the blockchain-based solution enables device authentication in 0.1 to 2 seconds. It is ideal for real-time Internet of Things applications since the technology lowers transaction latency to 1–5 seconds and energy usage to 0.2–2 joules.

Algarni, Sultan et al., (2021) Internet of Things (IoT) security and privacy concerns are many due to the decentralised structure of the network and its exponential growth. One of the biggest problems with the present methods of handling access control is that they are centralised, involve a third party, and have limitations in

terms of scalability and availability, which can lead to a performance bottleneck. Consequently, this study suggests a new way to handle the distribution of a blockchain-based, multi-agent system for safe access management of the Internet of Things (IoT) that is both lightweight and decentralised. Constructing Blockchain Managers (BCMs) to enable secure communication between local IoT devices and to safeguard IoT access control is the primary goal of the suggested approach. Secure data transfer between cloud computing, fog nodes, and Internet of Things devices is another benefit of the system.

Samanta, Ashis et al., (2021) A smart contract (SC) is an electronic agreement between two or more unnamed parties that does not rely on a third party to mediate the transaction. Code in the form of an agreement that may be executed automatically. The blockchain is where smart contracts operate. Because of this, the code and the agreement are permanently archived on a publicly accessible, distributed database. Financial services, healthcare, management, and the Internet of Things are just a few of the many potential digital economy use cases for smart contracts. Two of the most popular open-source advanced blockchain systems utilised across industries are Hyperledger and Ethereum. There are still many unresolved and important technical difficulties with blockchain, including privacy, security, accuracy, and verifiability. An extensive literature review on smart contracts is conducted in this study. Our presentation also includes a case study of a university examination system with a data structure that is diverse. With this deployment, we have a thorough grasp of the smart contract architecture and have been able to identify and assess the smart contract state-of-the-art's shortcomings.

Muneeb, Muhammad et al., (2021) Automating business operations in response to events generated by Internet of Things (IoT) sensors, data streams, or other applications is possible with the help of smart contracts. Future business-to-business (B2B) transactions may be mechanised by using a smart contract management system that is built on the blockchain. Business process re-engineering may benefit greatly from blockchain technology, which greatly improves workflow processes, particularly in scenarios involving several parties. This article introduces a smart contract management system that can be used by several organisations. It allows users to design, implement, and execute smart contracts. In the first section of this research study, we examined various smart contract management systems that are currently available. These systems differ in key aspects that businesses consider when choosing a system. Part two lays out our suggested architecture for a smart contract management system that runs on the blockchain. Smart contracts built on the blockchain can be executed at the organisational level as well as by decentralised autonomous organisations (DAOs). In the suggested architecture, SBlockchain and TBlockchain are two distinct blockchains. While TBlockchain holds all the data created by smart contracts, SBlockchain is used to store smart contracts themselves. Furthermore, in order for certain events to be executed, smart contracts contain conditions and clauses. Using applicable use-cases, we have provided a detailed description of the framework's components and how they are implemented.

Ali, Jawad et al., (2018) Despite the IoT's meteoric rise in the IT sector, its enormous size, decentralised architecture, and resource-constrained devices have kept it linked to a number of privacy and security issues. When it comes to the privacy and security of the Internet of Things (IoT), blockchain technology—a distributed ledger used in cryptocurrencies—has gotten a lot of attention. However, owing to the overheads and delays generated by BC operations, transitioning BC to the IoT is typically not an easy process. We implement Hyperledgder Fabric, a BC technology, into an IoT network in this article. To improve performance, this approach isolates consensus from transaction execution using an execute-order technique. When it comes to the three most important security objectives—availability, confidentiality, and integrity—we show that our suggested IoT-BC architecture is rock solid. Last but not least, we discuss the simulation findings that demonstrate our method has performance overheads that are low when compared to the Hyperledger Fabric architecture and much smaller when considering privacy and security.

Christidis, Konstantinos & Devetsikiotis, Michael. (2016) In light of blockchains' meteoric rise in popularity, we investigate if they are well-suited to the IoT industry. With blockchain technology, we can create a decentralised, peer-to-peer network where users may verify each other's identities and conduct transactions directly with one another, even if they don't trust each other. We go into the inner workings of this system and also explore smart contracts, which are scripts stored on the blockchain that enable the automation of multi-step procedures. We next go into the Internet of Things (IoT) space and explain how a blockchain-IoT hybrid does two things: 1) makes it easier for devices to share resources and services, which creates a marketplace for such offerings, and 2) automates multiple tedious processes in a way that is cryptographically verifiable. From the anticipated value of the digital assets exchanged on the network to concerns about transactional privacy, we highlight a number of aspects that should be thought about prior to deploying a blockchain network in an IoT environment. Whenever possible, we find ways to fix things or find alternatives. We conclude that the marriage of blockchain technology with the Internet of Things is formidable, and has the potential to usher in new distributed applications and business models across a number of sectors.

III. PROPOSED METHODOLOGY

Our proposed solution is an approach to controlling access to Internet of Things devices that is based on attributes. We reduce the possibility of data tampering and single point failure by combining Blockchain technology with cipher-text-policy-based attribute-based encryption (CP-ABE). We optimise the access control process by establishing smart contracts for lightweight authentication and to fulfil the high efficiency requirements of the Internet of Things. One type of blockchain network is used for user-defined policy storage; the other is a public blockchain for Internet of Things (IoT) device authentication and attribute servers. In contrast, after users and devices have been validated, the consortium blockchain stores the transaction hashes.

Figure 1 shows a common Internet of Things situation. Internet of Things (IoT) devices, attribute servers, and gateways are the three evolving entities in an IoT system. Wireless or direct wire connections are conveniently accessible by devices like laptops, smartwatches, and mobile phones. Some lightweight gadgets, on the other hand, need the specialised gateway. The registration server is in charge of gathering and authorising users and IoT devices. Once the server authentication is complete, these organisations are free to share and request data access in a multitude of ways.

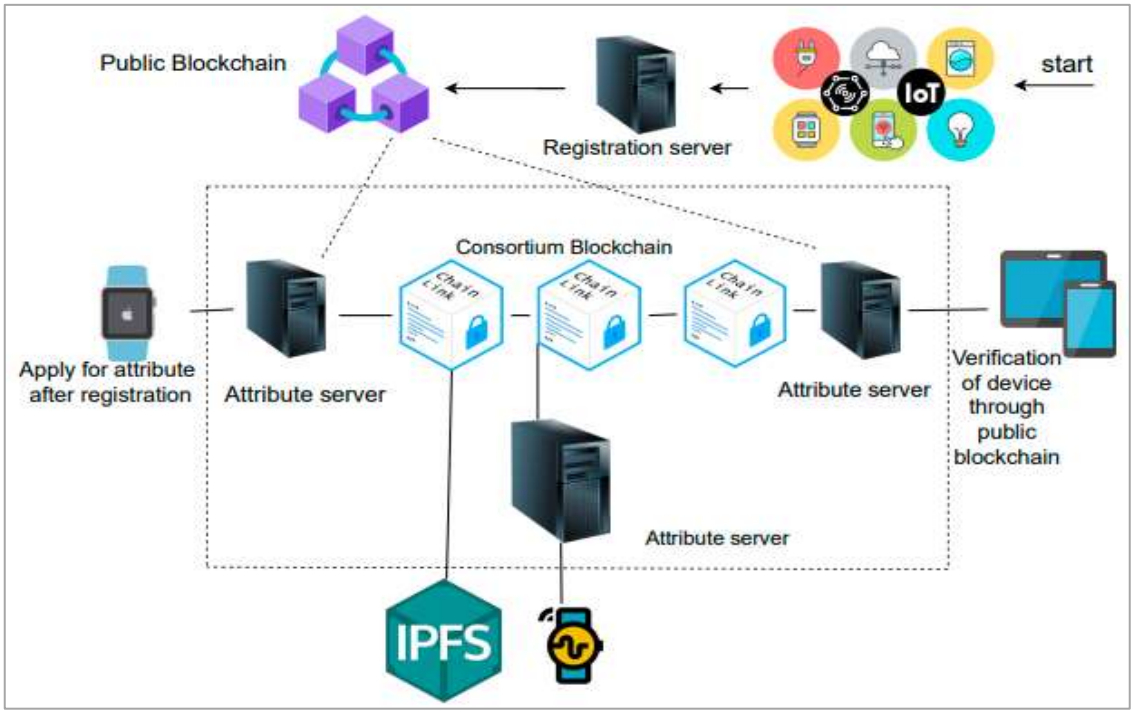

Figure 1: The System Model of Our Proposed Architecture

All of the financial dealings in our blockchain network take place in individual accounts held by each node. To ensure that no third party may change a user's verified identity, the registration server issues a set of keys—public and private—that can be used to sign and address transactions. On the distributed blockchain, each smart contract and transaction is recorded using a unique address. Thus, the blockchain will record each user interaction as a transaction, allowing for transparent access and traceability. In order to address concerns about scalability, smart contracts and transaction creation are executed over numerous blockchains.

Smart contracts are used to provide authorisation and manage access control. A user may possess many Internet of Things (IoT) devices, each of which needs its own set of credentials. That is why the user would have to verify each device separately. A public Ethereum blockchain could register users and their devices, but this would add an authentication burden. Smart contracts might solve this problem. The user and their devices may be authenticated by attribute authority using a wallet address, and then transactions can be executed. A distributed authorisation server can replace a single server with access control smart contracts.

Smart Contract System

The four smart contracts depicted in Figure 2 form the mechanism and are executed on the Ethereum blockchain. A policy management contract (PMC) stores the policies of each subject and object together with their stated actions, while the object attribute management contract (OAMC) and the subject attribute management contract (SAMC) make up the access control contract (ACC). Both the ACC and the PMC are responsible for managing the insertion and deletion of characteristics.

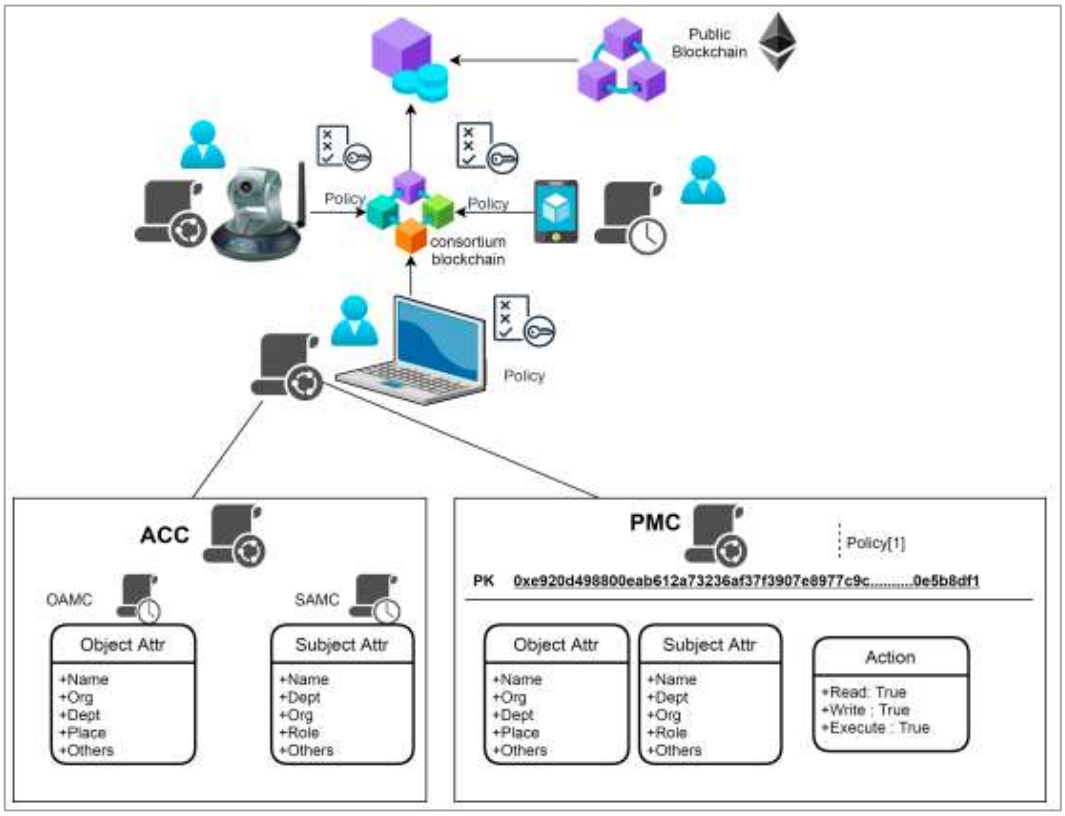

Figure 2: Building Blocks of The Access Control Mechanism

Performance Evaluation

The prototype was implemented on an Ubuntu 16.04 system with 4GB RAM and an Intel core i3 processor in order to evaluate the model's performance and viability. C++ and the Solidity language have been utilised for smart contracts. Remix IDE is used to simulate smart contracts. The Chrome browser plugin Metamask allows users to connect to Ganache and Remix, while Ganache is utilised for the provision of virtual accounts and the

execution of smart contracts. Paring computations make use of the PBC library. During development, we put smart contracts through their paces using Truffle, and for free smart contract deployment, we use Testnets like Ganache (local blockchain) and Ropsten (internet). We employ the cypher text policy in attribute-based encryption through the use of a cpabe toolbox to verify the ABE program's analysis. The PBC library is used to perform the algebraic operations. Cpabe is utilised for user interface and high-level functions, whereas libbswabe is utilised for the implementation of crypto operations.

IV. RESULTS AND DISCUSSION

The process of registering users and devices, storing data on distributed file systems like IPFS, and managing data according to policies are all illustrated in Figure 3.

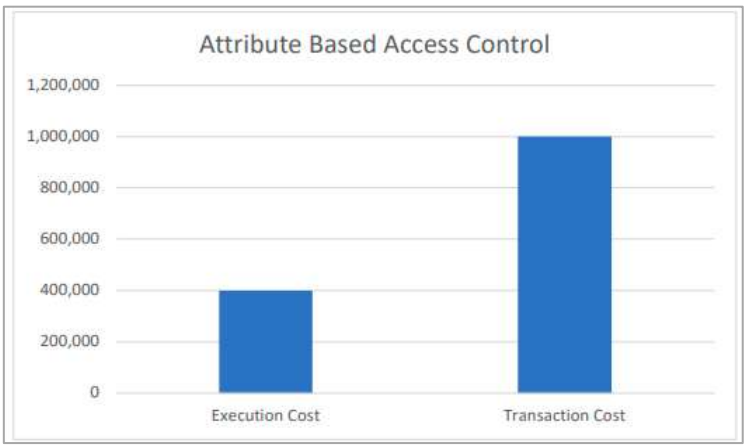

Figure 3: Attribute-Based Access Control Model Details

Gas is a very minor cryptocurrency unit on the Ethereum network. When users make a transaction in Ethereum, their accounts are debited with the unit. The energy required to run a smart contract is seen in Figure 4. A grant, an init, a policy, and a request are the four distinct smart contract functionalities utilised in the suggested work. Gas use is proportional to smart contract complexity. A costly activity in Ethereum is the deployment of the smart contract.

But transmitting the smart contract to Ethereum incurs the transaction fee. A transaction's execution cost is proportional to the number of activities carried out by the transaction. Consequently, the transaction cost already includes the execution cost.

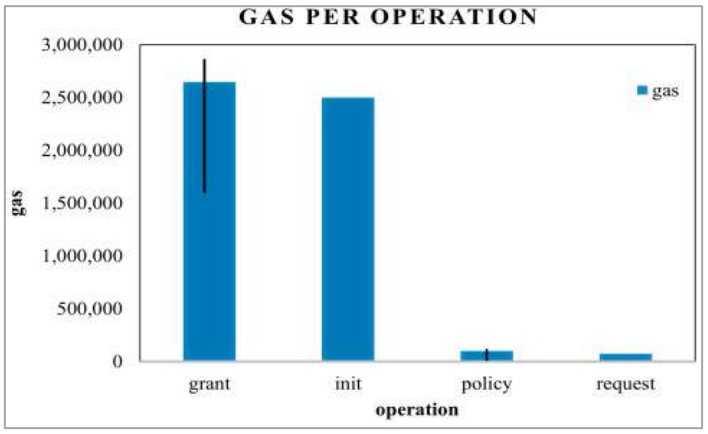

Figure 4: Gas Per Operation

Figure 5 displays the time required to execute our scheme's encryption and decryption procedures. A set of characteristics representing a user's capabilities is linked to their private key in our scheme. Because decryption can only be performed once a certain policy criterion has been met, it was quicker than encryption. It takes more time to process data when there are more characteristics.

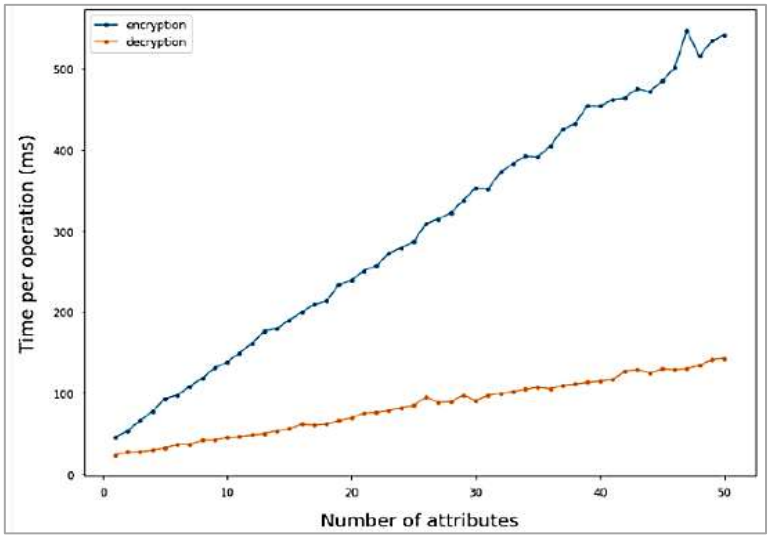

Figure 5: Operation Time with The Number of Attributes

In the simulation, we ensured each of the three qualities using the AND-gate-based access structure. Figure 6 shows the specifics of our system's operation, and it also provides information about how to share data with the owner. Access control in the registration setup has been implemented using the web3j package. The receiver can access the data if the port combination that included the device name and service name successfully confirmed the transaction according to specific regulations.

```
> Executing task: dlv debug --headless --listen=:2345 --log --api-version=2 -- g
rant access --for="0x1e52b030261C4890A6aCe85Ed48CaE5f459525A0" --contract="0xC69
5C023d4A2FfB1C98e0d609A7Ff02e858AF09e" --owner="0x20683Db6E6d7ff53b62BCD6F723f74
eC94dC410e" --attributes="admin,ceo,it_staff" <
```

Figure 6: Access Verification

In Figure 7, we can see the correlation between the amount of policy characteristics and the verification costs of access control. For this evaluation, we evaluated three different architectures: one for centralised access control verification with timely cpabe; one for decentralised access control with timely cpabe and blockchain; and finally, one for a timely access control list utilising blockchain technology. The outcomes demonstrate that the decentralised architecture has embraced an extra expense. While timely cpabe is more efficient, the verification cost is increased by using the timely access control list. Cpabe offers decentralised access management more efficiently than alternatives that do not use the access control list for verification of user access.

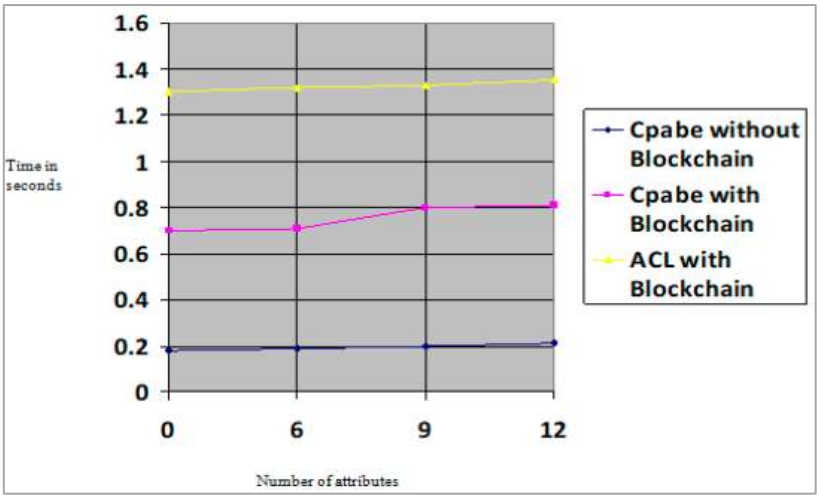

Figure 7: Cpabe Performance Comparison

V. CONCLUSION

This research proposes that the integration of blockchain with smart contracts can strengthen the security, privacy, and trust of Internet of Things (IoT) ecosystems. The new paradigm proposed addresses the drawbacks of traditional centralized access control systems, including single point of failures, transparency and scalability shortcomings, by incorporating a decentralized model using Ciphertext-Policy Attribute-Based Encryption (CP-ABE). A hybrid blockchain with IPFS (InterPlanetary File System) for distributed storage enables data to be securely and consistently shared, viewed, and modified across IoT networks. The model incurs higher computing and transactional costs, but increased trust, automation, and total access control offsets the costs.

REFERENCES

1. C. Bhattacharjee, "Enhanced Security for IoT Devices Using Blockchain Smart Contract," *International Research Journal of Management Science*, vol. 15, no. 4, pp. 7–12, 2024.
2. M. Rouached *et al*., "Policy-Based Smart Contracts Management for IoT Privacy Preservation," *Future Internet*, vol. 16, no. 12, pp. 1–24, 2024.
3. S. Gopalan *et al*., "Enhancing IoT Security: A Blockchain-Based Mitigation Framework for Deauthentication Attacks," *International Journal of Networked and Distributed Computing*, vol. 12, no. 10, pp. 1–13, 2024.
4. Zainuddin, A. Mortadza, and F. Musa, "Integrating IoT and Blockchain for Enhanced Security: Challenges and Solutions," *Data Science Insights*, vol. 2, no. 1, pp. 53–71, 2024.
5. Senturk and S. Terazi, "IoT security with blockchain: A review," *The European Journal of Research and Development*, vol. 3, no. 4, pp. 117–132, 2023.
6. Barazanchi and W. Hashim, "Enhancing IoT Device Security through Blockchain Technology: A Decentralized Approach," *SHIFRA*, no. 1, pp. 1–8, 2023.
7. P. Setia and S. Sandosh, "Enhancing Cybersecurity Defense of IoT Ecosystem Using Blockchain," *Suranaree Journal of Science and Technology*, vol. 30, no. 4, pp. 1–14, 2023.
8. M. Hasan *et al*., "Smart Contract-Based Access Control Framework for Internet of Things Devices," *Computers*, vol. 12, no. 11, pp. 1–22, 2023.
9. Fadele *et al*., "Smart Contracts Security Application and Challenges: A Review," *Cloud Computing and Data Science*, vol. 5, no. 1, pp. 15–41, 2023.
10. S. Rosaire and J. Degila, "Smart Contracts Security Threats and Solutions," *International Journal of Information Technology and Web Engineering*, vol. 17, no. 1, pp. 1–30, 2022.
11. S. Algarni *et al*., "Blockchain-Based Secured Access Control in an IoT System," *Applied Sciences*, vol. 11, no. 1, pp. 1–16, 2021.
12. Samanta, B. Sarkar, and N. Chaki, "A Blockchain-Based Smart Contract Towards Developing Secured University Examination System," *Journal of Data, Information and Management*, vol. 3, no. 4, pp. 237–249, 2021.
13. M. Muneeb, Z. Raza, I. Haq, and O. Shafiq, "SmartCon: A Blockchain-Based Framework for Smart Contracts and Transaction Management," *IEEE Access*, vol. 4, no. 1, pp. 1–14, 2021.
14. L. Alotaibi and S. Alshamrani, "Smart Contract: Security and Privacy," *Computer Systems Science and Engineering*, vol. 38, no. 1, pp. 93–101, 2021.
15. S. Kumar, A. Murugan, B. Muruganantham, and B. Sriman, "IoT–smart contracts in data trusted exchange supply chain based on blockchain," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 1, pp. 438–446, 2020.
16. Ali, T. Syed, S. Musa, and A. Alzahrani, "Towards Secure IoT Communication with Smart Contracts in a Blockchain Infrastructure," *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 10, pp. 584–591, 2018.
17. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*, vol. 4, no. 1, pp. 2292–2303, 2016.