Blockchain based Access Control and Data Sharing Systems for Smart Devices

P Chinnasamy¹, B Vinodhini², V Praveena³, C Vinothini⁴, B Ben Sujitha⁵

¹Assistant Professor, Department of Information Technology, Sri Shakthi Institute of Engineering and Technology, Coimbatore,
²Assistant Professor, Department of CSE, SNS College of Technology, Coimbatore,
³Assistant Professor, Department of CSE, Dr.N.G.P Institute of Technology, Coimbatore,
⁴Assistant Professor, Department of CSE, Dr.N.G.P Institute of Technology, Coimbatore
⁵Professor, Department of Information Technology, Jeppiar Institute of Technology, Chennai,

chinnasamyponnusamy@gmail.com

Abstract. Internet-of-Things and Blockchain technology are evolving all around today's modern world to solve many problems such as security, communications, data collection and analysis, etc. However, we also have some issues, such as efficient data sharing, restriction of access, reliable authentication, etc. The proposed framework is designed to solve the problems related to security and authorization in IoT network access control. In addition, the system's aim is to accomplish security, authorizing, and encryption for information exchange through IoT networks. In this article, a novel system is introducing to provide the data sharing system that integrates blockchain based access control system for IoT devices. Here, we are creating three different smart contracts to offers an efficient access control management like contract to provide access control, contract to provide authentication, and contract to provide a judgment. Finally, the effectiveness of the proposed approach is measured against the cost consumption of smart contracts and cryptographic functions. The cost utilization comparison is carried out against certain current approaches as well as the findings clearly demonstrate that the proposed approach is cost-effective.

1. Introduction

Growth of the internet is leading to a rising popularity of smartphones. Owing to the emergence of telecommunications and connectivity technology, systems are much more willing to communicate among each other. The creation of the Internet of Things (IoT) systems has been fostered by the link of sensors. IoT is a revolutionary system that enables the Network with real world. The IoT system is described as "the devices share the data, and resources thru internet". Without even any human involvement, the link between IoT systems is set up. Sharing of data, and services between devices is among the main characteristics of IoT. Device link expands the implementations of IoT systems in various domains including vehicular networks, smart home, smart healthcare, security systems, etc.
IoT devices are geographically linked due to the extreme applications especially, and the networking proportion is rising year-by-day.

In the networks, the link of sensors poses many challenges. A few of the problems are: ineffective data processing, unauthorized access, malicious programs, centralized point of failure and a few others. IoT devices comprise of confidential information, hence successful network management is extremely important. Because the data of an IoT systems is massive, centralized storages are used it to secure the information, i.e. cloud and fog. The cloud is capable of processing a massive volumes of information in a short way. Furthermore, for information processing, it enhances precision, performance, and speed. In addition to networks’ storage systems benefits, clouds and fog often create problems with bandwidth, security, and confidentiality. The big concern, indeed, is unauthorized access to services.

In the research, several methods are proposed to solve IoT technical difficulties. Effective sharing of information and licensed access control are now the demanding aspects of IoT systems. Data exchange and licensed access control over data are handled through many techniques including Mandatory Access Control, Role based Access Control, and Attribute based Access Control [1,2] etc. To minimize the problems in conventional systems, blockchain technology is however combined with access control and data sharing mechanisms. In order to ensure data integrity, accountability, legitimacy, security, and redistribution, blockchain offers a solution to several issues that are much more effective [3].

1.1. Background of Blockchain and its Applications

Nakamoto introduce the theory of the cryptocurrency in a journal article in 2008. It's often applied as just a technology involved for the cryptocurrencies of bitcoins. Bitcoin is often recognized as a first blockchain programme. Blockchains would be used to protect digital currencies money transfers through the removal of a central authority. Blockchain is a communication network whereby networks are linked in a Peer-to-Peer (P2P) way actually to one another. The principle of centralized control by consensus processes has been abolished. Network decisions will be made after a consensus amongst all the participants.

![Figure 1. Skeleton of Block Header](image)

**Figure 1. Skeleton of Block Header**

a) **Hash:** It takes variable length as input and generate a fixed length as a hash code. If small changes in the input message then we will get as a different hash values. In this, every operations or resources are carried out based on this cash value [3].

b) **Merkle Tree:** This Merkle tree enables the system to handle the large unstructured data securely and efficiently. [3].
c) **Timestamp:** Using this, we could monitor any document's creation or alteration time in a secured manner [3].

d) **Nonce:** A nonce attribute is almost a 32 bit number that stared longingly at 0 and increases every moment hash processing is performed [3].

e) **Previous Block:** A sha-256 hash which points to the previous block header [3].

1.2. **Contributions**
The major contributions to this research includes:

1. For effective sharing information, trusted and licensed access control amongst IoT connected devices, a blockchain-based framework is proposed.
2. For effective, safe, approved, and trust-based access control of users on a network, multiple smart contracts are used.
3. Safe and efficient sharing of data is also accomplished by intelligent contracts.
4. Control to supply access control to overall users and data sharing as well as it increase the cost effectiveness of the system.
5. Authentication of the system is provided by Registration Contract (RC) via user registration.
6. User abuse is reviewed by contract provide by judgement; the resulting punishment is decided after that.
7. A user's misconduct is documented in the system by introducing a recording tables of subjects abuse.
8. Various kinds of authorization are set continue providing users with authorized access rights and also to ensure trustworthy and secure sharing.
9. In addition, all smart contract transaction and operation costs and its responsibilities are measured.

The remainder of the article is structured as follows. A comprehensive review is provided in Section 2. The goals of the framework are explained in section 3. In addition, the proposed framework including its functionality is addressed in detail in Section 4. Afterwards the, in Section 5, the simulated results are mentioned. A summary of the actual and suggested systems is addressed in section 6. Finally, the complete paper is concluded in Section 7.

2. **Related Works**
Blockchain framework is believed to provide IoT systems with efficient analysis of large data exchange and access control. A few frameworks that combine blockchain with IoT system are documented in the literature.

In [1,2], the authors proposed a smart access control mechanism relying on contracts to have users with confidence and authentication. This framework, indeed, did not allow for direct contact among IoT devices and was also undermined in addition to high costs. In [3], the authors proposed a distributed access control framework for IoT devices blockchain - based to obtain optimum flexibility, competition, efficiency and resilience to attackers. The architecture introduced doesn't really, indeed, provide allowed and verified connections. In [4], the researchers reported an ABAC framework for IoT systems in terms of achieving less overhead communication and computing and improved versatility and efficient operational monitoring. The consensus protocol, i.e. the PoC used throughout the framework, thus worked successfully for certain components of the process. A blockchain consensus-based access control framework was proposed by the authors in [5] to authenticate a user via the given Channel State Information (CSI). A numerous blockchain-based inter-chain mechanism for physical access control in IoT systems was conceived by the researchers in [6]. The system's
primary goal is to achieve the protection of IoT nodes. Nevertheless, the protection and trustworthiness of users’ data is not effectively assured. The researchers in [7] suggested a new Decentralized Key Management Framework (BDKMA) blockchain based to solve the problem of system failure. Interoperability is accomplished by the scheme; the block chain, still, also isn't completely utilized. In [8], the authors addressed a little off-chain-based constitutional blockchain to guarantee access control security and efficiency. Consequently, once incorporated with industrialized use cases, the device will not provide trustworthy transactions.

A new blockchain-based resource allocation framework for Lw users was developed by the researchers in [10]. Smart contracts are used to preserve the integrity including on-chain and the off-chain operations. The framework thereby lost all ability provide the allowed data access and efficient distribution. In [11], the author implemented an AI-based trustworthy wireless communications sharing network via distributed consensus implementation. Using smart agreements and fine-grained access control, the system achieves trustworthy distribution. Even so, throughout all distribution settings, the system doesn't really work more efficiently. The authors in [12, 13] suggested a data sharing system based on legitimacy. The aim is to strengthen the accuracy of data sharing between network devices as well as to guarantee computer storage privacy. Anyhow, this system applicable only for small networks.

2.1. Objectives of the Proposed System
The goals of a proposed system for access control and data sharing amongst consumers of IoT systems are explained in this section. These goals are presented herein.

[1]. **Trustfulness**: The trust of consumers of sensor nodes is preserved by a system of misbehavior-judging that is enforced by JC. Users that misbehave are identified and fined as untrusted users. Even authorized users are allowed to view the resources they need.

[2]. **Authentication**: In this method, RC is used to authenticate users. RC registers every client who will become a member of the framework. Besides this, a record must be kept in the user registration table.

[3]. **Authorized access**: Only authorized users are permitted to view their necessary resources throughout this scheme. Authorization of the clients is retained by access rules.

[4]. **Effective data exchange**: The exchange of information amongst consumers of sensor nodes is preserved thru the ACC. That preserves the exchanging between service providers. In addition, permission-based exchanging is often done across the stages of authority.

3. Proposed Method
The clear picture of proposed method is shown in Figure 2. Since finding inspiration from research, this framework is built in [1,2,11, 13]. Sharing of information among two user groups or peers, named subject and object, is carried out in this framework. A consumer who really wants the service providers is the focus. Namely that, the object includes the resources that the subject needs. Resources provide details, files, programmers, etc. In addition, to monitor data exchange and access control between subjects and objects, triple contracts are being used.
3.1. **Smart Contracts**

The conceptual method comprises three distinct contracts (i.e., ACC, RC, and JC) to control and provide network users with different security services. ACC is responsible for controlling all access control of the whole framework. Authentication and authorization of the subject / object are issued by the registry contract along with maintaining all of the records in the data stores. Subject / object negligence is tracked by the Judgments Contract (JC). If any negligence occurs, the JC imposes obligations on the individual.

3.2. **Access Control Contract**

It is the key intelligent contract which really maintains the privileged access among IoT nodes. It processes the request to a process because when subject needs any facility again from object. Afterwards, the ACC retains the recipient's data access. This also improves the service's efficiency effectiveness. As a consequence, the technology is changing in expense and time. In addition, device computation time is often carried out. Hence, the ACC is implemented whenever a subject passes customer inquiries in to device.

3.3. **Register Contract**

It ought to be legal for consumers who really are supposed to be using the resources. For this reason, user verification is done thru RC, by adding everyone upon its database. For verification, as in [3], RC
preserves the authorization table. Throughout the table, all consumer data will be stored that is will be look like in Table 1.

| Subject | Object | Service | Time       |
|---------|--------|---------|------------|
| User A  | User X | File    | 2020/10/10 |
|         |        | Access  |            |
| User B  | User Y | Gmail   | 2020/10/10 |
| User C  | User Z | Data    | 2020/10/10 |

3.4. Judgement Contract
The JC, who evaluates the actions of components in the network, is introducing a judgment process. Whenever a participant submits service requests to the network, the JC verifies its actions. The wrongdoing is often handled by the participant. Whether regular and far too many applications are submitted by the recipient for just a resources, is known to be acting inappropriately as a service.

4. Simulation Settings
The experiment settings was implemented on windows 10 with 8 GB RAM and Intel core i5 processor. The code for the proposed method was written using solidity language, which is used to construct the ethereum blockchain network. Simulation outcomes for cost utilization are discussed in detail. In this method, Ethereum platform is often used; for all this, smart contract costs and its operations are discussed in terms of gas consumption. In addition, with each gas unit, the ether quantity is verified. The simulation setting and cost utilization of the each shared ledger and its parameters are discussed in upcoming section.

5. Performance Evaluation
Figure 3 shows the transaction and implementation costs for consensus mechanism like: ACC, RC, JC. The gas products utilized by ACC are greater than most other smart contacts, i.e., RC and JC, as shown in the above figure. It is clear that ACC is the primary intelligent contract between two connected systems that handles the ultimate network access and expenditures and executes additional complex computations.

Figure 3. Cost of Smart Contracts
5.1. **ACC Functions**

Figure 4 shows the transaction cost and the computation time between each ACC operation. Compared to two smart contracts, it requires several system call, since ACC controls the entire service's access control. Nevertheless, for the main responsibilities of the smart contract, gas value is measured. ACC’s responsibilities that manage numerous activities entail registration process, the generation of subject access rules, as well as the access control mechanism.

![Figure 4. Function Cost of Access Control Contact](image)

5.2. **Cost of Registration Contract**

In Figure 5, the transaction and implementation costs of RC operations are being shown. The aim of RC would be to control the registering of user accounts and also to create a registration table to record the details of the users. The operations of RC are managing the registration table and user registration process.

![Figure 5. The Function Cost of Registration Contract](image)

6. **Conclusion**

In IoT networks, the significant obstacles are also the delivery of authorized, trustworthy sharing information and allowed access control between connected systems. Consequently, blockchains is
combined with both the structure of data exchange and access control throughout this article. Achieving authentication, authorization, and trust are the key objectives of this method. Numerous advantages are introduced into systems with both the incorporation of blockchains. Numerous different contracts have been used in these methods to accomplish the above goals. ACC, RC, and JC are indeed the smart contracts. Where even the access rights amongst IoT systems is maintained by ACC and information sharing with them is controlled. In addition, RC is named to handle authentication process in the process by authorizing everyone. The info about the users is reported in the user registration table. The results show that the performance is cost-effective, because ACC controls the user access. For physical access management between IoT systems, the proposed approach becomes less intuitive.

References
[1] P. Chinnasamy, P. Deepalakshmi, K. Shankar (2020), “An analysis of security access control on healthcare records in the cloud”, Intelligent Data Security Solutions for e-Health Applications, Academic Press – Elsevier, ISBN: 9780128195116, Page(s): 113–130, 2020.
[2] Chinnasamy P and Deepalakshmi P, “A scalable multilabel-based access control as a service for the cloud (SMBACaaS)”. Transactions on Emerging Telecommunications Technologies, 29 (8), e3458. doi:10.1002/ett.3458,2018
[3] P.Chinnasamy, P.Deepalakshmi, V. Praveena, K.Rajakumari, P.Hamsagayathi, (2019) “Blockchain Technology: A Step Towards Sustainable Development” International Journal of Innovative Technology and Exploring Engineering (IJITEE), Volume-9 Issue-2S2.
[4] Zhang, Y.; Kasahara, S.; Shen, Y.; Jiang, X.; Wan, J (2018). Smart Contract-Based Access Control for the Internet of Things. IEEE Internet Things Journal, 6, 1594–1605
[5] Ding, S.; Cao, J.; Li, C.; Fan, K.; Li, H. (2019). A Novel Attribute-Based Access Control Scheme Using Blockchain for IoT. IEEE Access, 7, 38431–38441.
[6] Lin, D.; Tang, Y (2018). Blockchain Consensus Based User Access Strategies in D2D Networks for Data-Intensive Applications. IEEE Access , 6, 72683–72690.
[7] Ma, M.; Shi, G.; Li, F (2019). Privacy-Oriented Blockchain-Based Distributed Key Management Architecture for Hierarchical Access Control in the IoT Scenario. IEEE Access, 7, 34045–34059.
[8] Liu, H.C.; Lin, Q. (2018); Wen, S. Blockchain-enabled Data Collection and Sharing for Industrial IoT with Deep Reinforcement Learning. IEEE Trans. Ind. Inform., 15, 3516–3526.
[9] Zhang, G.; Li, T.; Li, Y.; Hui, P.; Jin, D (2018). Blockchain-Based Data Sharing System for AI-Powered Network Operations. J. Commun. Inf. Netw., 3, 1–8.
[10] Kang, J.; Yu, R.; Huang, X.; Wu, M.; Maharjan, S.; Xie, S.; Zhang, Y (2019). Blockchain for secure and efficient data sharing in vehicular edge computing and networks. IEEE Internet Things Journal, 6, 4660–4670
[11] Chethana Dukkipati, Yunpeng Zhang, and Liang Chieh Cheng. (2018). Decentralized, BlockChain Based Access Control Framework for the Heterogeneous Internet of Things. In Proceedings of the Third ACM Workshop on Attribute-Based Access Control (ABAC’18). Association for Computing Machinery, New York, NY, USA, 61–69. DOI:https://doi.org/10.1145/3180457.3180458.
[12] Quyun Lyu, Qi, Xiaochen Zhang, Huaping Liu, Qihua Wang, Ning Zheng, SBAC: A secure blockchain-based access control framework for information-centric networking, Journal of Network and Computer Applications, Volume 149, 2020, 102444, doi.org/10.1016/j.jnca.2019.102444.
[13] Basudeb Bera, Durbadal Chattaraj, Ashok Kumar Das, Designing secure blockchain-based access control scheme in IoT-enabled Internet of Drones deployment, Computer Communications, Volume 153, 2020, Pages 229-249, doi.org/10.1016/j.comcom.2020.02.011.