International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

Blockchain Based Access Control System for Internet of Things Devices

*1Ms. Sapna S. Khapre, 2Dr. Ganeshan R.

Submitted: 29/04/2023 **Revised**: 26/06/2023 **Accepted**: 06/07/2023

Abstract*:* The dispersed Internet of Things (IoT) poses several security and privacy challenges due to its architecture and fast, massive growth. The management of access is now a top priority. Centralized solutions to this problem frequently depend on a third party, have availability and scalability limitations, and may even be a performance barrier. In this study, a unique method is proposed for coordinating the provision of decentralised, lightweight, secure access management for an IoT system, making use of a multi-agent system and a blockchain. This suggested method's principal objective is to build Blockchain Managers (BCMs) to protect IoT access management by promoting secure interoperability amongst neighbourhood IoT gadgets. The technology also allows for secure communications between cloud servers, fog nodes, and Internet of Things devices.

Keywords: *IoT (Internet of Things), Blockchain, Cloud Architecture, Multifactor Authentication*

1. Introduction

The IoT (Internet of Things) is a capability of the web that enables electronic devices to exchange data with one another. IoT refers to a system of interconnected computing nodes. These devices allow for increased communication and collaboration between individuals and organisations by providing each with a unique identify and the ability to exchange data with one another.

The advancements made possible by the IoT will surely enhance people's lives, but before the IoT can be fully adopted, a number of security considerations must be taken into account [1]. One of the most challenging aspects of the Internet of Things is ensuring user privacy and security. Security issues in the IoT may be traced back to the network's inherent heterogeneity. [2].

Designing suitable authentication and authorisation methods in resource-constrained IoT devices [3] is one of the most important parts of security and privacy challenges. This article proposes a multi-agent system architecture that takes use of a private distributed blockchain to provide decentralised, lightweight, and secure access management for the Internet of Things. Protecting the whole IoT architecture, including cloud computing, the networking of fog nodes, and the communication of IoT devices, is the major objective of the suggested solution.

This paper's main contribution is a proposal for a state-of-the-art blockchain-based architecture to secure an Internet of Things (IoT) system. This approach is built on top of a multi-agent system and utilises decentralised access control. The solution utilises a private hierarchical blockchain architecture to enhance IoT security and accommodate low-power IoT devices. The usage of mobile agent software in our suggested solution further exemplifies the system's high degree of mobility and intelligence and may significantly reduce traffic overheads. We created a system that is adaptable, scalable, and generic enough to be used in several IoT contexts.

Using a private hierarchical blockchain structure, our solution guarantees the efficient and effective protection of each layer of the IoT architecture, In addition to enabling a significant cut in traffic overheads, a lightweight consensus method based on Internet of Things needs (including the usage of mobile agent software) brings mobility, intelligence, and Mandatory Access Control to the table.

2. Related Work

This research focuses on three primary areas, two of which overlap slightly: existing methods of IoT security management, multi-agent systems for access control, and blockchain-based IoT access control.

Objectives, models, architecture, and mechanisms were employed in a comprehensive evaluation of the access control methods now in use in the Internet of Things by Ouaddah et al. [1]. (OM-AM). The study also had a taxonomy that was developed after much research. The article compared and contrasted several access control models and protocols with regards to their suitability for use with the Internet of Things. Another approach for decentralised access control of Internet of Things (IoT) devices, Fair Access [10], was shown. The framework provided a pseudonymous approach to ensure user privacy. A new kind of transaction including the issuance, reception,

*[*1]Research Scholar, School of Computing Science and Engineering, VIT Bhopal University, Bhopal, MP, India*
ORCID ID: 0000-0003-3777-5355
[2]Assistant Professor Senior Grade - II, School of Computing Science and Engineering, VIT Bhopal University, Bhopal, MP, India
ORCID ID: 0000-0003-1441-6923
** Corresponding Author Email: sapna.khapre2018@vitbhopal.ac.in*

delegation, and revocation of access tokens was established. The underlying concept is the Attribute-Based Access Control (ABAC) paradigm. Fair Access's authorization technique relies on authorization tokens, which provide the bearer the authority to utilise a resource that can be uniquely recognised by its address and whose access control regulations are specified in a smart contract. However, this framework may introduce wait times in the event of owner communication, tokenization-only authorization, token cancellation, or a request for renewed access from the owner.

In [8], Novo introduced a blockchain-based decentralised access control solution with scalability built for Internet of Things gadgets. The blockchain architecture's goal of reducing network overhead meant that IoT devices couldn't be part of the network. The system's advantages in the realm of Internet of Things access control include, among others: portability; accessibility; parallelism; a lightweight design; scalability; transparency; and a scalable architecture. This framework provides administrators with tools for registering and authenticating Internet of Things (IoT) gadgets. This system grows by distributing query rights between administrative nodes, but it might introduce security risks if the manager is malevolent.

Dorri et al. [12] argued for a lightweight infrastructure that uses private blockchain technology to secure the Internet of Things (IoT). Based on these three foundational models—smart homes, overlay networks, and cloud storage—the suggested approach leverages an access control list to assure authorization. This method eliminates the requirement for PoW (Proof of Work) consensus when confirming blocks and saves access control rules in the blockchain's policy header since the miner has control over all of the smart home layer IoT devices. They stated that the system's administrative costs are well outweighed by the advantages to security. The proposed architecture, however, is specifically designed for smart home use cases and may not be applicable in other IoT contexts. Furthermore, self-enforcing access control constraints are not supported by this method [26].

While developing a framework for access control in cloud and BYODs contexts, Almarhabi et al. [27] tackled many security and privacy problems related to BYODs, like unauthorised alteration of policy, leakage of sensitive information. They presented an architecture that would allow Mandatory Access Control rules to be executed smoothly and effectively in cloud and BYOD environments, therefore addressing security and privacy concerns.

An IoT authentication and access control approach was proposed by Liu et al. [13], and it involves using a role-based Access Control (RBAC) authorization mechanism with a security key based on the Elliptic Curve Cryptosystem (ECC). Since there would be so many users in an IoT environment and RBAC wouldn't be able to predetermine who would be granted access, the proposed approach wouldn't be scalable. The proposed protocol has a poor security rating and calls for many communications. By including mutual authentication, user anonymity maintenance, and secure session key production, Ndibanje et al. [14] increased productivity while reducing communication costs. However, this approach fails to safeguard the privacy of transmitted information.

Access control methods based on roles or credentials are not suitable for use with the IoT. However, by combining their characteristics with those of other models, these models' flaws might be corrected. The hybrid role-and-attribute-based access control architecture proposed by Kaiwen et al. [15] allows for a high number of dynamic users to be accommodated without compromising policy integrity. They also established a process for addressing policy inconsistencies and duplications. In the suggested paradigm, the administrator still has the last say over who has access to what and who does what.

Touati et al. [16] suggested a method for controlling activities based on the preferences of both users and the system (a broader version of context-aware access control). For this purpose of dynamically adapting access policies, they used a finite state machine and CP-ABE (Cipher text-Policy Attribute-Based Encryption). The key/attribute revocation problem was proposed to be addressed using the CP-ABE method [17] developed by Touati et albatch-based. Fewer processing nodes are needed by the suggested approach, lowering complexity and overhead costs.

The principle of least privilege lies at the heart of the Cap-BAC (Capability-Based Access Control) approach to managing access to services. The service provider can't provide access to the required resources without a user-issued certificate of authorization. To facilitate the development of a private and secure IoT-based ecosystem, Sicari et al. [18] created a Unified Modelling Language (UML) conceptual model to express privacy policy definitions and data quality assessment. Medical prescriptions in a mobile situation may be established and tracked with the use of Radio Frequency Identification (RFID) technology, as suggested by Goncalves et al. [19].

Due to limited computational and storage resources, the capability-based solution to IoT access control challenges developed by Gusmeroli et al. [20] requires simple safe access control rules. Lightweight access management system that takes trust into account has been introduced by Bernabe et al. [21] to provide a secure and reliable connection between IoT-connected devices. Using metrics like service quality, security, and reputation, they came up with a new trust model. Managing trust becomes very important in a distributed and decentralised IoT context when device identities are unknown.

Using the fuzzy method to trust computation using linguistic data collected from IoT devices, Mahalle et al. [22] set up a trust-based dynamic access control architecture that conserves power. In the context of Mandatory Access Control, permission to use a resource is provided by an entity having that authorization. When deciding whether to provide or deny access to a resource, government entities often employ the sensitivity label.

To prevent unwanted connections, the NTT Innovation Institute [23] created the Mandatory Access Control approach to secure an Internet of Things framework and hosting policy management point. By incorporating attribute-based control rules, they made policy administration more manageable. Seitz et al. [24] developed a distributed authorisation architecture to reduce the amount of data sent between devices. To facilitate safe interaction between embedded devices, Naedele et al. [25] presented a public-key-based protocol that provides many mechanisms for user authentication and authorization. In order to establish a safe connection, the suggested protocol calls for constant back-and-forth. The device's state and condition when it lies on the ground are ignored as well.

The access control scheme for DSNs that Zhang et al. [26] proposed is designed to safeguard users' anonymity. Users must first get a token from the network owner in order to access the sensor data, and only after the token's authenticity has been verified will the data be sent to the user. To prevent distribution tokens from being reused in a way that allows for illegal access, they use a reuse detection scheme. Their major concern was keeping information private, thus they ignored the possibility of granular end-device access controls.

3. Design Methodology

We created a blockchain-based authentication protocol as a distributed method for managing access to and exchanging data from IoT devices. The three main components of this protocol are the IoT device, the user, and the gateway connected to the blockchain. IoT devices act as nodes to exchange information and resources with other users, devices, or people who need to access the system's information and resources. A gateway that is connected to the blockchain acts as a conduit between the user and the device. In order to access the information and resources on the device in line with policies, these gateways examine a user's authorization and verification. Each user registers their public and private key pair in our system when they join the blockchain network. Through blockchain-linked gateways and device administrators, smart contracts are introduced into the blockchain network.

distributed method for managing access to and exchanging data from IoT devices. The three main components of this protocol are the IoT device, the user, and the gateway connected to the blockchain. IoT devices act as nodes to exchange information and resources with other users, devices, or people who need to access the system's information and resources. A gateway that is connected to the blockchain acts as a conduit between the user and the device. In order to access the information and resources on the device in line with policies, these gateways examine a user's authorization and verification. Each user registers their public and private key pair in our system when they join the blockchain network. Through blockchain-linked gateways and device administrators, smart contracts are introdu

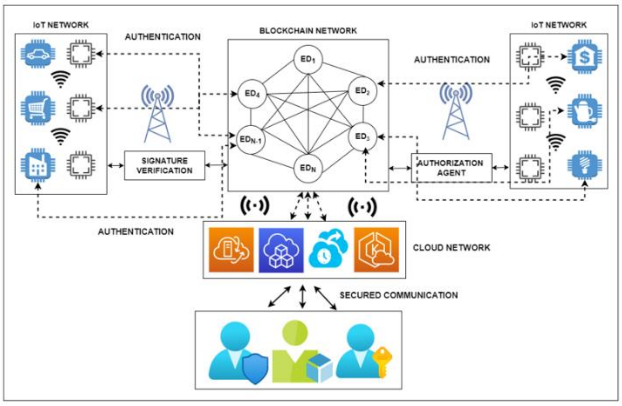

Fig. 1. Blockchain based Multifactored Authentication System on embedded Probabilistic polynomial Time Algorithm

Access rules and authentication processes are managed by smart contracts. Each device attached to a blockchain-linked gateway is maintained as a logical relationship by both the smart contracts of the device and the blockchain-linked gateway. The blockchain connected gateway is said to have access to a device's data when it establishes a connection with it. After locating the gateway smart contract address associated to the blockchain, the user may access the list of subset devices. The user must confirm that they have read and agree to the device's privacy policy in order to use any gadget. This agreement is stored on the blockchain network so that the gateway that is connected to the blockchain may be utilized when the user asks access to device data. The suggested design in Figure 1 is described in more detail as follows:

1. Preliminary Registration: When a new device enters the network and begins utilising the system, it must create a hash chain for initial registration.

2. Rebuild the hash chain Data: Devices that employ one-time passwords update their hash chains often, so in order to connect to the cloud, they must get in touch with the service provider to create a new chain.

3. Session Establishment: Communication between devices and between devices and the cloud takes place across a secure data channel.

3.1. Simplified Multi-Factored Authentication System

The HTTP (Hypertext Transfer Protocol) client authentication methods for embedded devices serve as the foundation for the cryptographic hash encryption employed in our method. In order to connect to the server using this protocol, an embedded device must first provide the server with its identification. This protocol is a client that is set up using TCP/IP (Transmission Control Protocol/Internet Protocol) and functions in a client/server relationship with three distinct stages. In order to identify the embedded device, the server will next generate a key and mix it with a random number.

We investigate the adversary model, the proposed lightweight multi-factored technique, and the multi-factor authentication architecture that unifies Single Sign-on (SSO) and Security Assertion Markup Language (SAML) in the cloud. It also describes how to build the multi-factor authentication and ePPTA (embedded Probabilistic polynomial Time Algorithm) foundations-based effective authentication approach. The decision-making process and authentication are demonstrated throughout the course of four steps. The proposed algorithm and revised strategy provide a potent set of cross-products, namely, service-based hybrid access control technology that prioritises Internet of Things devices inside a cloud architecture. The adversary model's constituent parts are discussed here as well.

This is how the suggested may be calculated:

- Device Enrollment: An embedded device (EDi) submit initial IDi

$$T_i = H(R_i \, \Phi \, H(X))$$

$$A_i' = A_j \, \chi \, G, T_i, ID_i$$

$$A_i = H(R_i \oplus H(X) \oplus P_i \oplus CK')$$

$$CK = H(R_i \,||\, X \,||\, EXP - Time \,||\, ID_i)$$

$$\text{Server Stores } A_i' = A_j \, \chi \, G, T_i, ID_i$$

$$\text{Server generates } P_i$$

$$X \rightarrow S' \text{ private\_key}$$

$$EXP - Time$$

$$S \rightarrow \text{sends } CK' \text{ to } ED_i$$

Pre-Computational Time Phase: It is critical that the verification key be used in the message calculation that has to be validated once it is received by the client/server communication device. The authentication key CK' is used to calculate the following: Given a random number N,

$$\text{Select N}$$

$$P_1 = N_j \, \chi \, G$$

$$P_2 = H(N_j \, \chi \, CK')$$

EDi sends Authentication message to (IDi, P1, P2)

- Verification Phase : For each attribute in this phase attType (att) = reset :

$$CK = H(P_r K \,||\, X \,||\, EXP - Time \,||\, ID_i)$$

$$\text{Server Stores : } A_i' = A_j \, x \, G, T_i, ID_i$$

$$\text{Server Generates : } P_U k \ \ (Public\ Key) + S_X + Hsh$$

$$x \rightarrow S' P_r K \text{ (Private Key)}, EXP\_Time$$

$$S \rightarrow \text{sends } CK' \text{ to } S_i$$

The embedded device then computes server store values, validates keys, and transmits a message to the server. When a device's mutual authentication is confirmed and both parties accept a shared session key, the server establishes a cloud. An attacker cannot attempt to discover intrusion strategies by getting unauthorized access to an embedded or IoT device; only a cloud server is open to such an attempt. With these systems, replay attacks, man in the middle assaults, listening in on conversations, cookie theft, brute force attacks, dictionary attacks, verifier attacks, mutual authentication, secrecy, and anonymity are all feasible.

3.2. Key Agreement on Multifactored Authentication

Next, we employ the hybrid Probabilistic Polynomial-Time Algorithm to facilitate end-to-end communication between users in an IoT-based environment so that they may carry out the essential agreement phases.

Step I: Verification Request: The IoT device initiates connection with the server by sending the necessary identifying characteristics.

Step II: Computation and embedded Probabilistic polynomial Time Algorithm (ePPTA) registration: Based on the following ePPTA process, the server creates a key Pi that includes a randomized number Ri and serves as a private key (Pr K).

• Device authentication uses an included Probabilistic polynomial Time Algorithm and a unique Hash for each key.

• Each participant contributes to the creation of a shared session key.

$$ePPTA \rightarrow \begin{cases} \left(\frac{1}{2} - \frac{1}{2^{n+1}} < \frac{1}{2}\right) & \text{If algorithm is not satisfied} \\ \left(\frac{1}{2} - \frac{1}{2^{n+1}}\right) X \left(1 - \frac{1}{2^n}\right) + 1 . \frac{1}{2^n} > \frac{1}{2} & \\ \text{If algorithm is satisfied} & \end{cases}$$

Step III: Phase of Verification: Data is sent from the server to ID, which may then retrieve any record.

3.3. Multifactored Authentication Based ePPTA

Every Pi produced by a device based on the key agreement will now also include a digital signature (Ds) and a hash (Hsh), as proposed by our embedded Probabilistic Polynomial-Time Algorithm (ePPTA). On this basis, consider the following formidable Pi, which your foe may not be able to foil:

$$\mathrm{T_i} = \mathrm{H}(\mathrm{R_i}\ \Phi\ \mathrm{H}(\mathrm{X}))$$

$$\mathrm{A_i'} = \mathrm{A_j}\ \chi\ \mathrm{G}, \mathrm{T_i}, \mathrm{ID_i}$$

$$\mathrm{A_i} = \mathrm{H}(\mathrm{R_i} \oplus \mathrm{H}(\mathrm{X}) \oplus \mathrm{P_i} \oplus \mathrm{CK'})$$

$$\mathrm{CK} = \mathrm{H}(\mathrm{R_i}\ ||\ \mathrm{X}\ ||\ \mathrm{EXP} - \mathrm{Time}\ ||\ \mathrm{ID_i})$$

$$\text{Server Stores } \mathrm{A_i'} = \mathrm{A_j}\ \chi\ \mathrm{G}, \mathrm{T_i}, \mathrm{ID_i}$$

$$\text{Server generates } \mathrm{P_i}$$

$$\mathrm{X} \rightarrow \mathrm{S'}\ \text{private\_key}$$

$$\mathrm{EXP} - \mathrm{Time}$$

$$\mathrm{S} \rightarrow \text{sends } \mathrm{CK'} \text{ to } \mathrm{ED_i}$$

As a result, when the embedded device determines values for A' and checks to see whether they are P4' = P4, Each time it's updated, the authentication step requires a new hash digest to ensure that the cloud server and user ID agree on the same session parameters (on Pi + IDi + Hsh). As a result of the probabilistic polynomial-time process having to go via another Hsh, the newly formed Hsh is three times stronger in a blockchain environment.

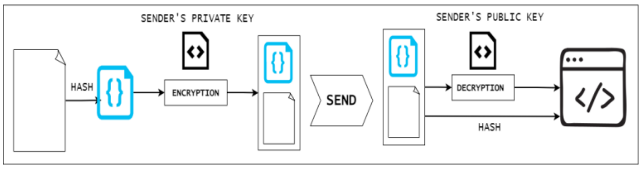

Fig. 2. Embedded Probabilistic Polynomial-Time Algorithm based Authentication

Figure 2 shows how the ePPTA is implemented with the MFA's security parameter hardened. Access control, confidentiality, and integrity are ensured by the ePPTA. This also depends on the nodes of the blockchain network coming to an agreement.

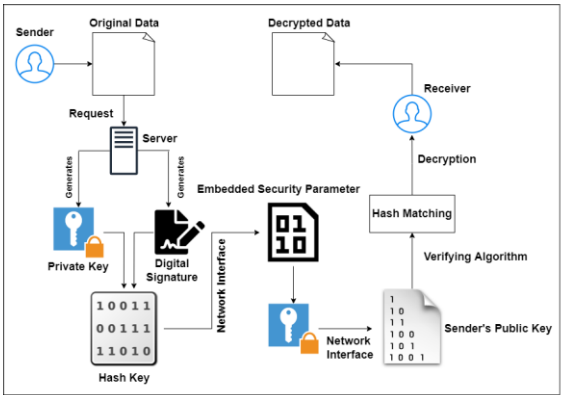

Fig. 3. Embedded Probabilistic Polynomial-Time Algorithm with Security Parameters

This helps the user save time by preventing them from having to log in again, and it also keeps a directory of the user's data in sync with the Cloud Service Provider. If a remote application is present, it can identify a user depending on their origin. The origin may relate to IP addresses or web subdomains in the context of this study report. After that, the user is routed to the IDP (Identity Provider) so they may send an AuthRq (Authentication Request). The IDP may then connect to the browser component and begin logging after that. The IDP creates an AuthRp, or authentication response, which is an Extensible Markup Language (XML) document containing the user's data. The Communications Service Providers (CSP) is then given access to these data via the Adaptive Communication Environment Single Sign-on (ACEsso). Finally, the CSP may offer Communications Service Providers Tamper - Resistant Security Module (CSPTrsm) and the putative cloud user's identity can be readily verified. The proposed approach has the potential to stop spoofing attacks and device/node takeover by leveraging this technique. There are n requests for SSO services and m responses to those requests. This suggests that several n authentication mechanisms may exist with the authenticating devices. Specific characteristics apply to each authenticating mechanism.

Our suggested framework's core consists of four layers of communication management: LBCM (Local Blockchain Manager), FBCM (Fog Blockchain Manager), CFBCM (Core Fog Blockchain Manager), and Cloud Blockchain Manager. These layers control all communications (CBCM). Access control policies must be established for each device/node in each tier by BCMs. Each block of the blockchain has a block header and a policy header. The MAC (Media Access Control) policy for each blockchain transaction is included in the block structure. The policy header in the BCMs enables them to control transaction access permissions. The most current policy header, which is found at the top of each block's header, is used by BCMs to evaluate, and modify policies even if every block in a blockchain includes one. Each layer's BCM (block chain module) is the miner in the proposed design; It is the fundamental security mechanism for verifying, authorising, and auditing financial transactions. After adding a new block to the blockchain, BCMs will duplicate the policy from the header of the preceding block into the new block and then start an attack against it [28].

4. Result and Discussion

It is crucial to note that, in accordance with the specific idea presented in this study, security approaches for an Internet of Things have been strengthened. The proposed embedded digital signature system, which makes use of asymmetric encryption, aims to increase the ePPTA's defense against intrusion. However, the proposed system integrates Security Assertion Markup Language- Single Sign-on (SAML-SSO) and makes use of a multi-factor authentication approach that enables user authentication at various stages in the cloud.

When a server connection attempt is made by an embedded device. This tactic works well since the cloud server has a reliable key generation system. This is so because immutable ledgers used in blockchain transactions include an embedded digital signature. Since the blocks in a blockchain are dispersed among nodes, it is computationally expensive to change the purpose of any one block during a transaction or ledger transfer.

This is because a blockchain's longest proof of work is more likely to be believed by its peers. This implies that the PPTA is given an additional degree of security by using our technique, making it computationally impossible to attack and ensuring a high level of trust, confidentiality, and integrity. The suggested method directly affects data privacy for IoT applications like smart cities. The achievement of the objective of smart cities and universal acceptability among practitioners depend on individual data protection and privacy. Maintaining confidentiality in high-dimensional data, protecting a network with a wide attack surface, building trustworthy applications, making the most of AI, and stopping errors from spreading across an intelligent network are all challenges that must be overcome by this vision [29].

Utilizing cutting-edge technology like blockchain and taking into account how the privacy solution will affect the system's overall efficiency are also essential. Future research opportunities based on our methodology therefore call for greater investigation of smart city deployment in pursuit of privacy and performance. The recommended method addresses important security goals that were disregarded in earlier studies. Data integrity and confidentiality are discussed [30].

Our suggested approach allows for many tiers of blockchain management to exert authority over the whole IoT infrastructure. In a connected home, the Local Block Chain Manager (LBCM) serves as a miner. It is used to manage Internet of Things devices in a smart home, for example TVs, lighting, and refrigerator accessories, and may be installed in a home hub or on a PC. Many Internet of Things gadgets in a smart home are managed by LBCM. Using LBCM, the Fog Block Chain Manager (FBCM) may regulate and connect a single smart house, a cluster of nearby smart homes, or both. To improve scalability and security, the Core Fog BlockChain Manager (CFBCM) may coordinate several FBCM clusters throughout a large area, such as a city.

Table 1. Accuracy of with different number of Hidden Nodes (HN) and hardware accelerators

HN	Accuracy	CPU	Training time (s)			Testing time (s)	
			GPU	**TPU**	**CPU**	**GPU**	**TPU**
10	96.34%	256.9	69.7	59.8	14.8	9.2	8.6
20	96.47%	451.7	79.8	66.7	23.9	12.8	11.5
30	96.78%	854.6	99.6	89.4	35.5	18.4	17.4
40	97.35%	995.2	100.9	129.8	68.4	21.9	20.6
50	97.95%	1278.4	140.3	137.5	72.3	29.1	30.9

CPU- Central Processing Unit, GPU- Graphics Processing Unit, TPU- Tensor Processing Unit

Many CFBCMs are linked to various CBCMs so that information may be stored and retrieved. Taking these kind of precautions is essential if we want smart homes to be a comfortable and secure place to live. Smart home technology is vulnerable to a variety of security threats due to the large amount of data and communication resources it uses. Tampering as well as malicious programming are two of the most typical forms of cyber assault against smart home devices. The term is used to describe malicious software that causes extensive harm to a specific device in order to steal or corrupt data or otherwise compromise the system. After doing a network scan of smart homes, an attacker's primary goal is to get and keep access to these devices with the ultimate goal of compromising the whole system.

Table 2. Accuracy of with different number of hidden nodes and hardware accelerators

HN	Accuracy	CPU	Training time (s)			Testing time (s)	
			GPU	**TPU**	**CPU**	**GPU**	**TPU**

10	95.73%	120.2	15.3	14.8	3.6	2.4	2.5
20	96.85%	290.7	27.5	26.4	7.5	3.5	3.7
30	96.67%	810.6	50.7	49.6	17.5	8.3	8.6
40	97.78%	989.5	80.9	65.4	32.7	16.8	16.5
50	97.56%	989.8	92.8	72.7	41.9	32.9	29.7

When hackers tamper with a smart home system by installing a code or function on Internet of Things devices, the integrity of the system is weakened since the hackers now have access to and control of the house's private data. Our study effort will be severely hindered in many framework-related areas if we choose to focus on these topics. A first step in the suggested method is for an authentication agent to determine who is permitted to access a system and who is not. To implement the MAC policy's access restrictions and label authenticity checks, an authorization agent is utilised. We also use the compartmentalization approach. To further ensure the system's safety and integrity, the signature verification agent maintains data consistency.

5. Conclusion

The use of cloud computing and cloud-enabled IoT has skyrocketed. This integration aimed to increase the use of intelligent transportation systems. However, this growth necessitates security measures that guarantee data integrity, privacy, and resource availability. This study looked into the potential of an MFA system based on blockchain technology to protect the integrity and privacy of connected IoT devices. The proposed approach for a cloud-connected ecosystem combines SSO and SAML features. The evaluation's findings indicate that the suggested method offers a solid method for strengthening the security of IoT-to-Cloud linked devices. This study also emphasizes the agenda for future research as well as the need for effective access control in networked systems and its vision. The results of this study should aid in the creation of formal IoT access control models as well as practical Cloud-Enabled IoT Platforms. To emphasize the degree of trustworthiness of the suggested approach, more research on factors like trust and evil intent will be done as part of an ongoing inquiry. Another area for potential future study on an IoT platform is device and user attribution. Future research will concentrate on developing a number of use-cases for evil intent where behavioral intents may be modeled. On the other side, a behavioral model may make advantage of the attribution process. The study of use cases that use behavioral models and attribution procedures will thus be a significant component of future attempts to create a trustworthy IoT authentication method.

List of Abbreviations

Sr. No.	Acronym	Full Form
1	BCMs	Blockchain Managers
2	OM-AM	Objectives, Models, Architecture, and Mechanisms
3	PoW	Proof of Work
4	BYOD	Bring Your Own Device
5	ECC	Elliptic Curve Cryptosystem
6	RBAC	Role Based Access Control
7	CP-ABE	Cipher Text Policy Attribute Based Encryption
8	UMP	Unified Modelling Language
9	IoT	Internet of Things
10	Cap-BAC	Capability-Based Access Control
11	HTTP	Hypertext Transfer Protocol
12	SSO	Single Sign-on
13	SAML	Security Assertion Markup Language
14	ePPTA	embedded Probabilistic polynomial Time Algorithm
15	IDP	Identity Provider
16	AuthRq	Authentication Request
17	XML	Extensible Markup Language
18	CSP	Communications Service Providers
19	CSPTrsm	Communications Service Providers Tamper - Resistant Security Module
20	ACEsso	Adaptive Communication Environment Single Sign-on
21	LBCN	Local Blockchain Manager
22	FBCM	Fog Blockchain Manager
23	CFBCM	Core Fog Blockchain Manager
24	CBM	Cloud Blockchain Manager
25	MAC	Media Access Control
26	SAML-SSO	Security Assertion Markup Language-Single Sign-on
27	HN	Hidden Node
28	CPU	Central Processing Unit
29	GPU	Graphics Processing Unit
30	TPU	Tensor Processing Unit

Author contributions

Sapna Khapre: Conceptualization, Methodology, Software, Writing-Original draft preparation

Dr Ganeshan R: Validation, Visualization, Investigation, Writing-Reviewing and Editing.

Conflicts of interest

The authors declare no conflicts of interest.

References

[1] Li, Y. Emerging blockchain-based applications and techniques. Serv. Oriented Comput. Appl. 2019, 13, 279–285.

[2] Kebande, V.R.; Karie, N.M.; Venter, H. A generic Digital Forensic Readiness model for BYOD using honeypot technology. In Proceedings of the 2016 IST-Africa Week Conference, Durban, South Africa, 11–13 May 2016; pp. 1–12.

[3] Alshehri, M.D.; Hussain, F.K. A centralized trust management mechanism for the internet of things (CTM-IoT). In Proceedings of the International Conference on Broadband and Wireless Computing, Communication and Applications, Barcelona, Spain, 8–10 November 2017; pp. 533–543.

[4] Alshehri, M.D.; Hussain, F.; Elkhodr, M.; Alsinglawi, B.S. A Distributed Trust Management Model for the Internet of Things (DTM-IoT). In Recent Trends and Advances in Wireless and IoT-enabled Networks; Springer: Cham, Switzerland, 2019; pp. 1–9.

[5] Ouaddah, A.; Abou Elkalam, A.; Ait Ouahman, A. FairAccess: A new Blockchain-based access control framework for the Internet of Things. Secur. Commun. Netw. 2016, 9, 5943–5964.

[6] Huang, J.; Kong, L.; Chen, G.; Cheng, L.; Wu, K.; Liu, X. B-IoT: Blockchain driven Internet of Things with credit-based consensus mechanism. In Proceedings of the 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS), Richardson, TX, USA, 7–9 July 2019; pp. 1348–1357.

[7] Gupta, M.; Awaysheh, F.M.; Benson, J.; Alazab, M.; Patwa, F.; Sandhu, R. An Attribute-Based Access Control for Cloud Enabled Industrial Smart Vehicles. IEEE Trans. Ind. Inform. 2020, 17, 4288–4297.

[8] Awaysheh, F.; Cabaleiro, J.C.; Pena, T.F.; Alazab, M. Big data security frameworks meet the intelligent transportation systems trust challenges. In Proceedings of the 2019 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/13th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), Rotorua, New Zealand, 5–8 August 2019; pp. 807–813.

[9] Aladwan, M.; Awaysheh, F.; Cabaleiro, J.; Pena, T.; Alabool, H.; Alazab, M. Common security criteria for vehicular clouds and internet of vehicles evaluation and selection. In Proceedings of the 2019 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/13th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), Rotorua, New Zealand, 5–8 August 2019; pp. 814–820.

[10] Aladwan, M.N.; Awaysheh, F.M.; Alawadi, S.; Alazab, M.; Pena, T.F.; Cabaleiro, J.C. TrustE-VC: Trustworthy evaluation framework for industrial connected vehicles in the cloud. IEEE Trans. Ind. Inform. 2020, 16, 6203–6213.

[11] Elkhodr, M.; Alsinglawi, B.; Alshehri, M. A privacy risk assessment for the Internet of Things in healthcare. In Applications of Intelligent Technologies in Healthcare; Springer: Cham, Switzerland, 2019; pp. 47–54.

[12] Alshehri, M.D.; Hussain, F.K. A comparative analysis of scalable and context-aware trust management approaches for internet of things. In Proceedings of the International Conference on Neural Information Processing, Istanbul, Turkey, 9–12 November 2015; pp. 596–605.

[13] Kebande, V.R.; Alawadi, S.; Awaysheh, F.M.; Persson, J.A. Active Machine Learning Adversarial Attack Detection in the User Feedback Process. IEEE Access 2021, 9, 36908–36923.

[14] Awaysheh, F.M.; Aladwan, M.N.; Alazab, M.; Alawadi, S.; Cabaleiro, J.C.; Pena, T.F. Security by Design for Big Data Frameworks Over Cloud Computing. IEEE Trans. Eng. Manag. 2021, 1–18.

[15] Chaturvedi, K.; Matheus, A.; Nguyen, S.H.; Kolbe, T.H. Securing spatial data infrastructures for distributed smart city applications and services. Future Gener. Comput. Syst. 2019, 101, 723–736

[16] Karie, N.M.; Kebande, V.R.; Ikuesan, R.A.; Sookhak, M.; Venter, H. Hardening SAML by Integrating SSO and Multi-Factor Authentication (MFA) in the Cloud. In Proceedings of the 3rd International Conference on Networking, Information Systems & Security, Marrakech, Morocco, 31 March–2 April 2020; pp. 1–6

[17] Ramatsakane, K.I.; Leung, W.S. Pick location security: Seamless integrated multi-factor authentication. In Proceedings of the 2017 IST-Africa

Week Conference (IST-Africa), Windhoek, Namibia, 31 May–2 June 2017; pp. 1–10.

[18] Rehman, F.; Akram, S.; Shah, M.A. The framework for efficient passphrase-based multifactor authentication in cloud computing. In Proceedings of the 2016 22nd International Conference on Automation and Computing (ICAC), Colchester, UK, 7–8 September 2016; pp. 37–41.

[19] Furnell, S. The usability of security–revisited. Comput. Fraud Secur. 2016, 2016, 5–11.

[20] Zhu, H.H.; He, Q.H.; Tang, H.; Cao, W.H. Voiceprint-biometric template design and authentication based on cloud computing security. In Proceedings of the 2011 International Conference on Cloud and Service Computing, Hong Kong, China, 12–14 December 2011; pp. 302–308.

[21] An, Y.; Zaaba, Z.; Samsudin, N. Reviews on security issues and challenges in cloud computing. IOP Conf. Ser. Mater. Sci. Eng. 2016, 160, 012106.

[22] Radha, V.; Reddy, D.H. A survey on single sign-on techniques. Procedia Technol. 2012, 4, 134–139.

[23] Awaysheh, F.M.; Cabaleiro, J.C.; Pena, T.F.; Alazab, M. Poster: A pluggable authentication module for big data federation architecture. In Proceedings of the 24th ACM Symposium on Access Control Models and Technologies, Toronto, ON, Canada, 4–6 June 2019; pp. 223–225.

[24] Awaysheh, F.M.; Alazab, M.; Gupta, M.; Pena, T.F.; Cabaleiro, J.C. Next,-generation big data federation access control: A reference model. Future Gener. Comput. Syst. 2020, 108, 726–741.

[25] Awaysheh, F.M.; Alazab, M.; Garg, S.; Niyato, D.; Verikoukis, C. Big Data Resource Management & Networks: Taxonomy, Survey, and Future Directions. IEEE Commun. Surv. Tutor. 2021, 1.

[26] Asim, J.; Khan, A.S.; Saqib, R.M.; Abdullah, J.; Ahmad, Z.; Honey, S.; Afzal, S.; Alqahtani, M.S.; Abbas, M. Blockchain-based Multifactor Authentication for Future 6G Cellular Networks: A Systematic Review. Appl. Sci. 2022, 12, 3551. https:// doi.org/10.3390/app12073551

[27] Bagga, P., Das, A.K., Chamola, V. et al. Blockchain-envisioned access control for internet of things applications: a comprehensive survey and future directions. Telecommun Syst 81, 125–173 (2022). https://doi.org/10.1007/s11235-022-00938-7

[28] Attkan, A., Ranga, V. Cyber-physical security for IoT networks: a comprehensive review on traditional, blockchain and artificial intelligence based key-security. Complex Intell. Syst. 8, 3559–3591 (2022). https://doi.org/10.1007/s40747-022-00667-z

[29] Youcef Ould-Yahia, Samia Bouzefrane, Hanifa Boucheneb, Soumya Banerjee. A data-owner centric privacy model with blockchain and adapted attribute-based encryption for internet-of-things and cloud environment. International Journal of Information and Computer Security, Inderscience, 2022, 17 (3/4), pp.261. ff10.1504/IJICS.2022.122374ff. ffhal-03688529

[30] Li Z, Miao Q, Chaudhry SA, Chen C-M. A provably secure and lightweight mutual authentication protocol in fog-enabled social Internet of vehicles. International Journal of Distributed Sensor Networks. 2022;18(6). doi:10.1177/15501329221104332

[31] Meneses-Claudio, B. ., Perez-Siguas, R. ., Matta-Solis, H. ., Matta-Solis, E. ., Matta-Perez, H. ., Cruzata-Martinez, A. ., Saberbein-Muñoz, J. ., & Salinas-Cruz, M. . (2023). Automatic System for Detecting Pathologies in the Respiratory System for the Care of Patients with Bronchial Asthma Visualized by Computerized Radiography. International Journal on Recent and Innovation Trends in Computing and Communication, 11(2), 27–34. https://doi.org/10.17762/ijritcc.v11i2.6107

[32] Rodriguez, L., Rodríguez, D., Martinez, J., Perez, A., & Ólafur, J. Leveraging Machine Learning for Adaptive Learning Systems in Engineering Education. Kuwait Journal of Machine Learning, 1(1). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view /103

[33] Dhabliya, D. (2019). Security analysis of password schemes using virtual environment. International Journal of Advanced Science and Technology, 28(20), 1334-1339. Retrieved from www.scopus.com