EasyChair Preprint

№ 10317

An Identity Management System Utilizing Voice Authentication and Blockchain in Conjunction with Reputation and Trust-Based Access Control

Prashnatita Pal, Bikash Chandra Sahana, Jayanta Poray and Rituparna Bhattacharya

June 1, 2023

An Identity Management System Utilizing Voice Authentication and Blockchain in Conjunction with Reputation and Trust-based Access Control

Prashnatita Pal[1]*, Bikash Chandra Sahana[2], Jayanta Poray[3], Rituparna Bhattacharya[4]

[1],[2]Department of Electronics & Communication Engineering, National Institute of Technology, Patna, India
[3],[4]Department of Computer Science & Engineering, Techno India University, West Bengal, India

ARTICLE INFO

Keywords:
Blockchain, Internet of Things, Reputation–Trust Management, Voice authentication.

ABSTRACT

Access control or Authorization is an important aspect of increasing the privacy and security of Internet of Things networks. An association of private and public companies or two more organizations have collaborated for greater common achievement or to enable sharing resource pools due to the economic aspect. However, the most common traditional access control mechanism based on a centralized system is suffering from data bulkage and solitary-point failure. Recently, many researchers are investigating the prospects of tackling the issue of conventional access control with the help of modern technology like Blockchain. But such solution overlooks the scalability challenges and considers the importance of flexibility/dynamic mechanism. To fill these gaps, we design a decentralized reputation and trust-based access control technique. We name our proposed system as IoT Consortium reputation and trust-based Access Control Model (IoT-RTS). Not only blockchain- is used in our proposed solution to improve performance but also both conventional and blockchain database exhibits advances features. We design a voice authentication system to improve the scores of reputations and trust in the Internet of Thing (IoT) network. Our proposed model achieves secured, dynamic and smart access control. The secure, smart IoT-RTS meets the effective solution for business and enterprise purposes and is applicable for many applications leveraging IoT.

1. Introduction

The use of Internet of Things (IoT) related devices has increased at an unprecedented rate as we enter the era of connected and omnipresent items [1]. We have benefited greatly from the growth of the IoT, which has accelerated the development of several technologies like the smart home [8] and smart city [9]. However, security and privacy issues with both existing and future IoT devices are also a cause for concern as explained in [2,3,23]. In particular, malevolent people may access non-owned devices, combating which is essential for IoT security and privacy as described in [6,20,21]. Context access-based control (CBAC) is lighter than the Attribute-based access control (ABAC) and Role-based Access Control (RBAC) because it ties an object with the proper access permissions using an unforgeable and communicable token of authority. However, the original CBAC has a flaw - only one subject can get a token; this might lead to inefficiency and need the development of a suitable fix. The first issue is that central management ends up with single-point failures since many more systems have security problems. Secondly, when a centralized server is used or another party authorizes to access, checks on the data and it is being saved, it might result in privacy leaks. Thirdly, since transparency is not included, centralized systems are not a better choice in comparison to a group of private blockchain **(**consortium) applications.

Blockchain maintains a distributed ledger that includes all transactions via an associate network [5]. In essence, it is a growing collection of data in the form or type of blocks that are cryptographically connected. Blockchain is a reliable alternative architecture for access control systems thanks to certain characteristics (such as decentralization, tamper-proofing, and security) [4].

The following are the primary contributions of this paper:

- In response to the problem with the bulk of current IoT access control systems discussed above as well as the limitation of current blockchain-based solutions, we offer the IoT-RTS, a better-decentralized reputation, and trust-based access control technique for modern consortium applications. The capability of group type token notation has introduced a way to improve more reputation and trust with the current works and solutions.
- We delineate the need for IoT authorization control data registries and then show the architecture for blockchain-based database systems. A proof-of-concept prototype is used to implement and assess the suggested strategy. The findings demonstrate that IoT-RTS is quick, secure, scalable, and capable of supporting IoT municipal and corporate applications.

The rest of this essay is structured as follows.

Related blockchain IoT access control systems are included in Section 2. Sections 3-5 describe the components, authorization mechanism, and token generation protocol of the IoT-RTS architecture. Section 6 describes the requirements for an IoT access control data registration and the integration of a blockchain database. In Section 7 and 8, we explore the prototype model of our suggested technique in addition to a description of its security and performance while implementing and evaluating it. A conclusion, a prognosis for the future, and recommendations for further effort in Section 9 round out our work.

2. ASSOCIATED WORKS

The research on the use of Reputation and Trust based access control (RTAC) and blockchain for IoT is mostly summarised in this section. In particular, RTAC was selected because of its advantages over RBAC and ABAC. The concept of least privilege, for instance, allows a subject to utilize the CBAC to carry out its objective while granting as few access rights as feasible [18]. In terms of their lightweight nature, scalability, dynamicity, heterogeneity, flexibility, and granularity, the three access control systems are carefully contrasted.

*Corresponding author.-Department of Electronics & Communication Engineering, National Institute of Technology, Patna, India
E-mail address: prashnatitap@gmail.com

Table 1
Overview *of Access Control Models in Compared* of some Recent Publication

Reference	Model [Year]	Core concepts	Advantage	Disadvantage
10	Trust Based Access Control (TBAC) [2021]	The key concept is Trust level	Access requests may be reviewed promptly which is fair and acceptable.	Suitable for the cloud and not IoT-focused
12	Pervasive Based Access Control (PBAC) [2019]	Multiple sections, characteristics, and the matching function	Dynamic and proactive broad adaptability	Decentralized architecture's working paradigm has not yet been implemented.
[13,14]	Transaction Based Access Control (TBAC) [2019]	Transactions are used to handle access tokens.	-Management of protected, decentralized access tokens. Support the delegation of access. Accessibility with ease.	The decision about access made centrally: Time response is severely impacted.
[15,16,17]	Smart Contract Based Access Control (SCBAC) [2018,2018, 2021]	Contracts are essential to the creation of distributed servers.	-Accessibility with ease. - Dynamic access management. - Scalable and Flexible	Collaboration amongst access contracts to pinpoint subject behavior's might be quite time-consuming.

First of all, since a large amount of data cannot be stored on a blockchain, on-chain and off-chain databases must be correctly integrated to carry out some tasks. Second, the public blockchain does not satisfy the requirement for a consortia enterprise network's transaction to be private and only visible to participants, as every one may see them. A blockchain database can accomplish the same duty with even better performance, even though private blockchains have been developed to address this issue as indicated by Tseng et al., [26]. Third, scalability and performance have consistently been the main problems with the blockchain technology. Despite recent improvements in transaction authentication, validation, and execution performance brought about by the introduction of consensus-type mechanisms by Biswas et al. [6], more effective transaction processes like the Hyperledger Fabric blockchain are discussed here.

The execution and scalability of access control solutions still fall short of the current centralized solutions as portrayed by Androulaki et al. [21]. We offer an upgraded IoT Consortium reputation and trust-based Access Control (IoT-RTS) architecture for trust-based access control on the blockchain Regulatory Model due to the precedent shortcomings of current blockchain technology-based access control tactics. We divided the access control data into services, statement, assets, and profiles to make the conclusion adaptable while taking into account the IoT's rapid expansion and scalability. Data interchange and interoperability are the main goals of this strategy.

Our strategy is designed for bulk networks rather than the individual platform, in contrast to previous IoT-RTS solutions. We examine a database that uses a blockchain and combines its security characteristics in the context of the shortcomings of the blockchain as mentioned above. It is giving the performance improvement of the database and using it as the basis for the suggested access control. Access control can therefore result in the following shown in table1 when used in conjunction with blockchain technology. There are several restrictions associated with using blockchain for IoT access control, though. A few of the urgent issues facing the IoT ecosystem were identified in this report from the thorough investigation. The following constraints, which will need to be addressed by future access control models:

- Scalability: Problems with widespread application
- Limited environment: IoT environments are too complex to implement.
- Lightweight: Mobile device usability.
- Mobility: An administrative system that operates in isolation.
- Accessibility: The rule for access control is always available.
- Interoperability: The capacity to converse with equipment with disparate standards.
- Time: reaction in real-time
- Dynamic Configuration: The access policy must be altered on the fly.
- Distributed and limited devices: IoT environment specifications are not taken into consideration.

Solutions for the aforementioned issue:

1. A Blockchain Supported Trust Based Secure Wireless Communication Framework for IoT Networks
2. It is necessary to create a decentralized access control system with an attribute base and an additional Reputation and Trust System (RTS) for IoT procedures.
3. To create a database with a blockchain technology system that combines the best aspects of both traditional and blockchain databases for improved performance of the blockchain and secure IoT communication.

3. MODEL FOR ACCESS CONTROL BASED ON IOT REPUTATION AND TRUST (IOT-RTS)

We develop and summarise the key elements used in this study for a voice authentication-based IoT reputation and trust-based authorization control model in this part. We also provide a thorough explanation of the connections between each of the elements that make up our proposal.

RTS description for IoT

IoT authorization control is a paradigm that includes the creation of rules, the assignment of those network resources, groups of users, and rules to persons such as sensors and devices, the definition of those resources' rights, and the protection of the network from harmful and illegal access. For example, the IoT is a complicated network that consists of interconnected domains. Each linked domain has its sub-network and is responsible for maintaining its resources. When it comes to establishing laws for a complicated network, it is important to take into account the ecosystem's flexibility, granularity, and privacy as well as its cross-organizational interoperability, and information sharing.

IoT-RTS makes it possible for any domain to administer, and it can share resources. This is done to facilitate interoperation in service provisioning with other organizations and to provide the owners of the different networks and subnetworks with ownership of the resources provided by the network and the subnetworks. To further exemplify the recommended strategy, we identify significant components of both the IoT network and the IoT-RTS.

Voice authentication system.

Users can enter the management system and blockchain after passing the voice authentication system.

We already work voice authentication process using high frequency innovative technique [36]. In this study, the main aim is to achieve secured communication using voice authentication technique. After voice authentication, secured communication has been done successfully. Using this technique, we have designed Voice identity management.

Voice identity management (VIDM) is an innovative and important feature of any digital environment. VIDM mainly used IoT ecosystem access control. Each IoT entity must contain a unique identifier (VID) to representing its identity. VIDM has mainly three functions. In our system's design, all the aspects have the relation to the authentication process for this work. Voice registration, Voice authentication and Cancellation of identity are the three main parts at VIDM system. The function voice registration is uploading a voice identity to the system and assigns unique voice identifier. To inspect voice identity with ecosystem at each time is the function of voice authentication. Finally, the system has a feature to withdraw the Voice identity, if required. Identity management components outside
any digital environment must include voice identity management (VIDM), for access control in the IoT ecosystem. In IoT-RTS authorization process, unique identification for each IoT entity will be an important feature.

The flowchart for the authorization process is shown in Figure 1, VIDM and the access control module are the elements taking part in the authorization choice. VIDM is in charge of determining if the individual seeking access is legitimate. The IoT-RTS authorization entails the following functionalities:

Verify the token's validity: This is the first stage in the authorization process. The subject ID will be submitted to identity management for verification of whether the token is legitimate, at which point it will be decoded. The request is denied if the token is corrupt or the subject has not been verified as legitimate. For the access to be allowed, the manner of access that is being requested has to coincide with the access right that is permitted in the statement credentials. If this is not the case, the request will be denied.

Check the asset's availability: Using the profile ID, we confirm the profile's existence, the services it offers, and the asset's accessibility. The request will be turned down if the requested material is not accessible.

Verify the fulfilment of requirements: The last step is to verify that the statement metadata's criteria have been satisfied and correspond to the entries in the database. The request is granted if the prerequisite is satisfied.

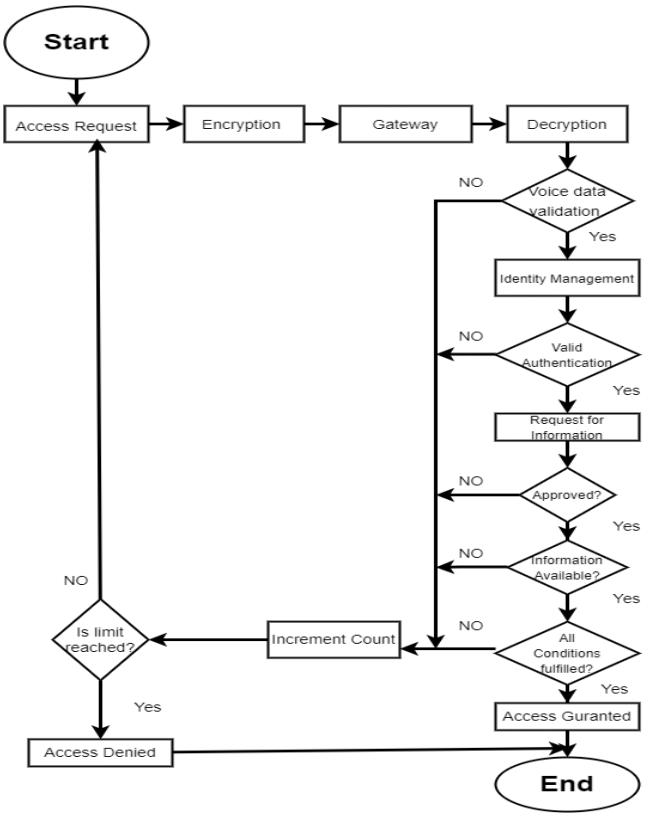

Figure1. The flowchart for the voice authorization process

4. SYSTEM ARCHITECTURE FOR IOT-RTS

Register administration, Service Provider administration, profile management, Summary Contract, and user Information control make up the bulk of the IoT-RTS system. As indicated in Figure 2, the system also includes a module for the token generation with verification and a module for generating unique identifiers (UIDs).

Registrar administration

Each domain is given the ability to store and register its physical resources as assets, and only the owner is permitted to change or remove its information. The physical resources that are accessible and the services which can be utilized and interacted with make up the system assets.

Asset context information is a representation of data such as the issuer ID, the creation time, and the unique identifier (UID). Asset credentials provide information about constant resources, such as the resource ID, domain ID, resource kind, and resource function. Asset metadata includes information about resources that may be changed, including their URI and location.

Service Provider administration

Due to the possibility of a consortium having several collaborative service providers, each provider is seen as a service inside the network. The task of developing, updating, and changing service-related activities falls within purview of the service management module. The network's flexibility and granularity will increase with the introduction of the concept of service, and the requesters and requests for the collaborative project will be governed.

The following notations may be used to represent properties required for service creation:

The system's representation of a service's context includes the service's unique identity (UID), its issuer ID, and the time at which it was issued.

Summary Contract

A profile is a conceptual description of the data in a particular context that a resource has for a certain service. Even though a resource may have several profiles, each profile can only be created for a single resource inside a specific service.

A profile serves as the resource identification and may be applied to one or more assertions. The task of establishing, amending, and changing profiles fall within the purview of the profile administration module. The related asset ID, service ID, and profile context, which include system-associated data, are used to identify the proxy profiles using a profile authorization

Management of context

A key component of controlling access rights is context management, which involves establishing the environmental conditions that need to be met to provide access in certain cases and deny it in others. Protocol, location, time, authentication status, and security level are examples of conditions. To guarantee the accuracy of the condition values, the values of context information are routinely acquired from the surrounding area and the network resources. Profiles, assets, and service information may all have context conditions attached to them to provide or prohibit access based on the fulfilments of the criteria. These notations are used to present context management:

The information in the system is represented by the conditioned context, and the many conditions to be checked before allowing access are covered by the condition metadata.

User Information control

A new statement is a record that specifies the authorization right and permission for a certain resource inside a particular type of service. This document is known as a statement. Registering new statements, keeping existing ones up-to-date, and making changes to them are the responsibilities of the statement management module. Each time an update or registration is performed, it also verifies the validity of other system data, including profiles and services.

The following notations may be used to represent the whole statement specification in IoT-RTS:

Information = {information Context, information Credential, information Metadata}

information Context = {IID, Service Admin $_{ID}$, Service Admin $_{time}$, and Primary}

Information Credential= {Portrait $_{ID}$, Step, and Reference $_{URL}$}

Information Metadata = {Condition$_{1,}$ Condition$_{2,}$ ....., and Condition $_{n\,ID}$}

The following is a succinct summary of statement components:

IID: A special identification number assigned to the individual states in the system.

Service admin: Issuer provide the appropriate information.

Service time: Indicate the moment the statement was created or last updated.

Primary: Each time a statement is changed, a new statement is produced with the old IID value in the principal field. The primary domain will have the identical IID field value at first construction. It is primarily used due to the attributable issues.

Portrait: This word denotes the resource profile for a certain service.

Steps: Display the set of access privileges that the statement grants. It's worth may be described as follows:

1. The Steps belong to read, write, and NULL.
2. If the Permission is not granted then if Steps is equal to NULL.
3. The Internationalized Resource Identifier (IRI) is a particular format used to specify a specific entity's access route.

Reference $_{URL}$ = Service $_{ID}$: Domain $_{ID}$ Resource $_{ID}$: Region $_{ID}$

The domain $_{ID}$ stands for the company that owns the entity, the service $_{ID}$ for the program in which the entity participates, the location $_{ID}$ for the entity's location, and the assets $_{ID}$ for the authorization process.

Membership service for IoT-RTS

To communicate with its administration module, the IoT-RTS Membership Service (MS) supports accounts. There are two types of accounts, each of which consists of a set of permissions, and each account belongs to a single domain. Administrators fall under the first category and have complete access to assets and service-related data, allowing them to create and modify it as well as assign members to services. The second group consists of service members who have the authority to carry out different network-related tasks, including making and changing statements, giving subjects access tokens, and auditing or examining reports. After acquiring a legitimate authentication token from the VIDM, subjects (requesters) may communicate with the access control system by using client-server abstractions. Device-to-device communication is made possible by IoT-RTS token operations.

In this part, we go over how to use capability tokens, beginning with turning a statement into a token, then creating a group token, and finally going through the revocation procedure.

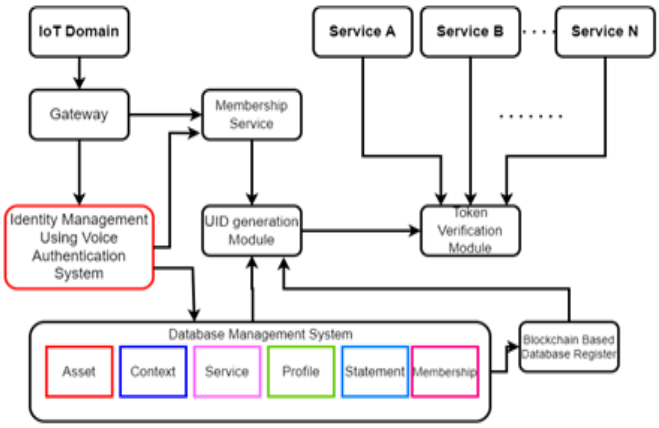

Figure 2. Proposed Model for Voice authentication-based identity management supported by Blockchain for IoT Network

Issuing a symbol of capability

Figure 3 depicts the system interactions that take place to generate capability tokens. These interactions take place between the subject, the VIDM, and the access control. Before moving on to the later stages of establishing the various components of the blockchain access control and integrating the services and resources, all subjects that desire access must initially register to the network through the VIDM for legitimate identification purposes. Only then can the process move forward. After the subject has correctly registered, they can ask for a token that grants them access permission to the resource with in network. In addition to this, the member of the service verifies that the subject being discussed is legitimate and checks to see whether there is already a statement with the same authentication.

If it does not already exist, it makes a statement with the information listed above, together with the access rights and constraints that were provided.

After the formulation of the statement, the system produces a capability token by applying an algorithm for token generation, and then it sends the capability token to the requester in the following format:

Token for group capabilities

When a group is formed and has a small number of subjects it will aid in categorizing and consolidating the access forms. Since we don't internally store capabilities, our architecture supports a group capability token. By design, if the subjects are from the same service and ask for the same access privileges, the statements may be shared among them. The system will also create a token immediately after the notation.

Cancellation of the capability token

A capability token may be revoked simply by storing it in a database, carrying out a quick-erase operation, and checking all tokens for each authorization request. Alternatively, you may revoke a token by including it in an exception list and whenever a user requests access, run a check job for that list. We decided to revoke the tokens using an exception list in our design. For instance, our modular architecture enables varying degrees of access denial to resources. Consider deleting a profile, archiving a service, or changing a statement document. When making an authorization judgment in such a situation, the assertions containing obsolete data will not be legitimate, and the request will be denied.

Process for IoT-RTS authorization

The flowchart for the authorization determination process is shown in Figure 3. VIDM and the access control module are the elements taking part in the authorization choice. VIDM is in charge of determining if the individual seeking access is legitimate. The IoT-RTS authorization entails examining the token's validity, the activity permitted, the asset's accessibility, and the fulfilment of requirements:

a. Verify the token's validity: Verifying the token's validity is the first stage in the authorization process. The subject ID will be submitted to identity management for verification of whether the token is legitimate, at which point it will be decoded. The access method sought must match the access permission authorized in the statement for the access right to be approved. Otherwise, the request is turned down.
b. Check the resource availability: Using the profile ID, we confirm the profile's existence, the services it offers, and the asset's accessibility. The request will be turned down if the requested material is not accessible.
c. Verify the fulfilment of requirements: The last step is to verify that the information metadata's criteria have been satisfied and correspond to the entries in the database. The request is granted if the prerequisite is satisfied.

5. INTEGRATION OF IOT-RTS AND BLOCKCHAIN

The most susceptible part of access control is the data layer since it permanently retains the information that is required. The system uses the data it has already saved to determine if the actions were done correctly. To sustain such a network, great dependability and availability would be necessary. Additionally, interoperability and data interchange across the sub-networks are essential for maximizing the value of IoT; as a result, transparency, confidentiality, and integrity are essential to attaining the goal. Blockchains are immutable digital ledgers made up of blocks that record data using cryptographic techniques.

In the end, blockchain can fulfil the security requirements for access control, while the database can reap the advantages of performance. Since databases have a history of use in the development of computers, so blockchain technology is developed to promote the concept of decentralized payment systems.

To fulfil the demands of IoT domains and maximize the use of IoT by facilitating, the ability of a system and data sharing, our goal is to create a new secure, reliable access-based solution. We use blockchain-control database technology as a result to increase the security of IoT-RTS.

Integration of blockchain

A reputation and trust network-based access control model, and blockchain-induced register of database make up the IoT-RTS-based blockchain, which is shown in Figure 2. The consortium is created by the network participants to work together on a specific project or to accomplish a commercial objective. Each member must contribute to one or more nodes to take part in network activities and maintain a copy of the data. The preceding section explained the IoT-RTS module. Each module communicates with and connects to its registry. The off-line/chain saves environmental data obtained from networked devices and sensors.

6. EVALUATION AND IMPLEMENTATION

The phases of implementation and the findings of the assessment will be covered in this section. We first talk about the system design, then we show the testing environment and the technologies we used, and then we talk about the outcomes.

Discourse on system design

The consortium's commercial strategies and objectives will be impacted by any compromised data, making confidentiality and integrity of data even more crucial. Since end users are not likely to interact with the system in these apps (end-user privacy includes the personal network), it is not particularly necessary to protect their privacy. The physical resources that are recorded as assets and the environmental data that will be used in the condition fulfilment process make up our system's input data. The payload object in the output, on the other hand, includes a permission decision.

Environment for experiments

we tested our solution. As an example, in our simulation of three firms working together on various services, each company was able to register actual equipment as assets and produce JSON Tokens that matched the access control requirements. The outcomes of our experiment are based on two different kinds of data stores; for the first, Docker technology is used locally (offline), and for the second, we utilize the BigchainDB for the online test node. To share data, several parts of the experiment employ RESTful APIs.

A machine with Ubuntu, 8 GB of RAM and a single Intel Core i5-5510Z 2.00 GHz processor serves as the execution environment. Additionally, Apache JMeter was utilized to model concurrent registration and authentication queries.

Security evaluation

We outline various typical assaults on the decentralized system and detail defences against them to assess the security of our solution. Forgery attacks are often used to gain sensitive information or to contaminate the system with random data by altering IDs and transaction data. Attackers may modify the authorization process, change a database record, or perform an undesirable operation by injecting a script. A man-in-the-middle assault occurs when the assailant silently intervenes between two communicative entities to intercept their data.

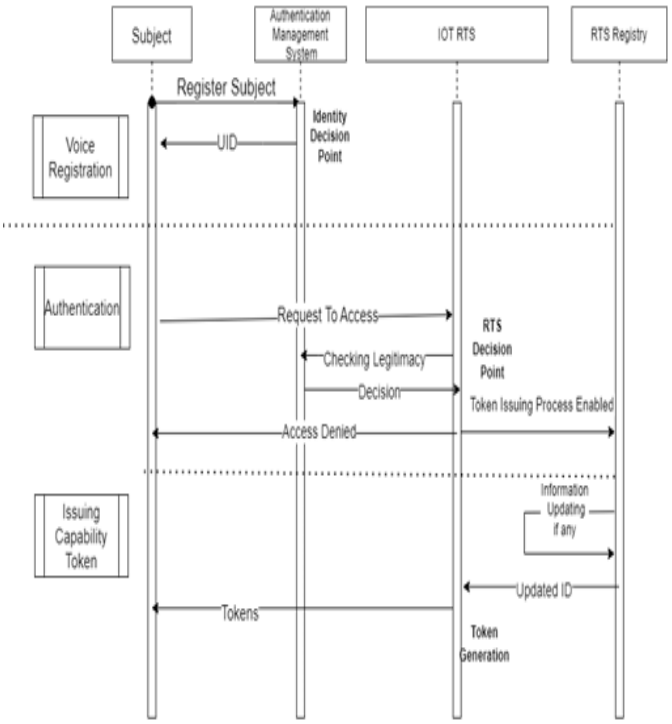

Figure 3. Token Generation Sequence Diagram

We stop these assaults by setting up the following conditions:

- Attackers and other participating organizations are unaware of the identities of the assets.
- The exchanged messages and tokens are securely signed using the SHA256 method, making them difficult to counterfeit or modify.
- Before gaining access to the data storage, we perform several checks on each system input to verify the accuracy of the data.

7. RESULT AND DISCUSSION OF THE EXPERIMENT

We first calculated the costs for producing assets, services, profiles, and transaction statements to assess the efficacy of IoT-RTS. The results are shown in Table 2. Before a transaction is committed for long-term storage, it goes through two steps in BigchainDB. Construction of the transaction and first input checks to guarantee its legitimacy constitute the preparation step. The transaction is signed with the creator's private key during the fulfilment stage, and its body information is hashed to provide the transaction ID.

The second experiment involves sending large numbers of transactions to the server to evaluate the data store's scalability and performance while processing many concurrent transactions. We tested 4 groups of 20, 100, 200, and 400. concurrent transactions using Apache JMeter to create and authenticate activities. The execution times for the creation operation are shown in Figure. 4, and the execution times for the authentication process are shown in Figure 5. The execution time (ms) is the plot on the y-axis, the four bulk transactions are shown on the x-axis, and the series shows the average commit time, the latency of the transaction, and the server connection time.

The creation process seems to take longer at first glance since a transaction must go through two verification procedures before being written within a block. For example, this ensures that the transaction is genuine. If both of these tests result positive and the transaction does not already exist in the system, then the transaction will be added to the database that the blockchain uses. Because we use databases, the authentication process is comparatively quicker.

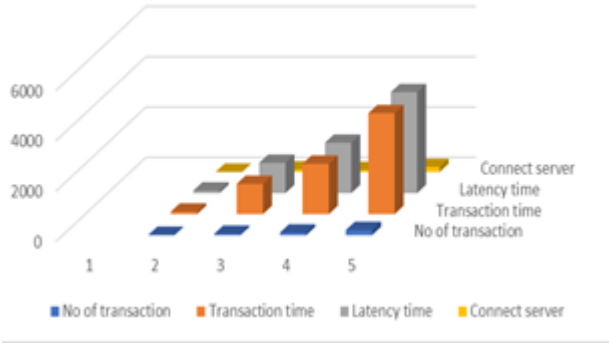

Figure 4. Execution time of Creating transactions

Figure 5. Execution time of authentication transactions

Table 2

The costs for producing assets, services, profiles, and transaction statements to assess the efficacy of IoT-RTS

Type of Transaction	Consciousness Time(ms)	Realization Time(ms)	Offline Conclude Time (ms)	Online Conclude Time (ms)
Asset	1.6	2.1	210	1,510
Service	1.9	2.5	210	1,870
Profile	1.6	3.3	210	780
Statement	1.7	2.7	210	970

We just validate the requester's signature and quickly get the various transactions by utilizing their IDs. The total delay time for 50 simultaneous authentication requests is shown in Figure 6. The latency time increases as more requests come through to the server. A vertical or horizontal resource scale may be used to minimize latency and achieve the desired performance. We made use of a database technology that was based on the blockchain so that we could benefit from the many safeguards offered by the blockchain as well as the excellent operational speed of the database. Our solution demonstrated higher performance outcomes when compared to comparable work. The experiment's findings show that our approach is capable of delivering the performance required for IoT city-level access management. IoT-RTS is also adaptable for a variety of use cases and IoT applications due to its flexibility and compatibility.

We compare and contrast the RTSAC model provided in this work due to its ability to grow activity published in the literature [32,33,34] to demonstrate the superiority of the suggested method in this study. The comparative analysis results of the are shown in Table 3. Considering how scalable the storage is in the table indicates that side chaining is appropriate than the replicated block scaling strategy. The access control model may be more effective than the current solutions in terms of throughput, efficiency, and security by improving the scalability of the storage of the blockchain model

using the sidechain scaling technique. Consequently, the scaling strategy utilizing numerous sidechains is more successful.

We contrast the IoT RTS model described in this study with the models provided in the published work [28,29,30,31,35] in terms of the protection of data privacy.

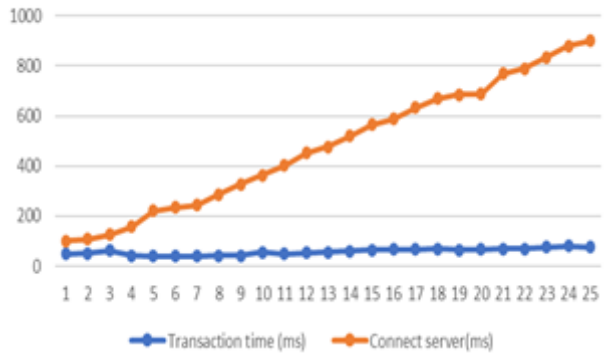

Figure 6. Latency time of 100 simulations authentication transaction

8. Prototype Evaluation

Table 4 displays the comparison's findings in four categories, including whether the system is based on blockchain, control of access, storage mechanism, and privacy protection. Table 3 shows that the majority of currently used data privacy protection strategies solely use access control or blockchain technology, with comparatively little research combining the two. The majority of conventional blockchain storage techniques use single-chain type storage, which does not ensure that the more data are entirely isolated. Also, if the data is stored in a repository of the system as well as transferred to the blockchain via the system's mapping type relationship, the possibility of unintentional information disclosure still exists.

The approach is simple to administer, but if the server hosting the data is hacked, the volume of data causes a significant quantity of information to leak.

In this work, four sidechains are utilized for block, data storage, and nodes on the primary chain only hold relevant information that may be released. The side type chains, which follow the incorporate-chain isolated type storage concept, can reasonably store additional data resources. The incorporate-chain isolated storage concept may address the drawbacks of the separate-chain storage paradigm by isolating various services onto distinct blockchains and storing data under segregated encryption.

The suggested model also limits the access of the seeking visitors, who are required to gain authorization and authentication before they can enter the system and view the side chain data. In addition, the Roll-up smart contract that has been installed on the side chain monitors visitors' access patterns, identifies users who access the data on the sidechain with malicious intent, and blocks such users from accessing the sidechain's data.

As a result, the decentralized access control architecture suggested in this work significantly decreases data privacy leakage and offers strong data privacy security protection. The parties to the transaction, the asset value, the prior hash, the nonce number, the time stamps, and the way the blocks are connected to the previous and subsequent blocks constituting a sequence of transactions are highlighted as shown in Figure. 7.The database that is located, stored, and maintained in a single location. In Figure 8 and figure 9 shown, Comparative Analysis of throughput and Execution Time on different Model. We are performing our experiment with the help of 100, 200, and 300 nodes. After a comparative analysis, we conclude that our system is better than the other three methods.

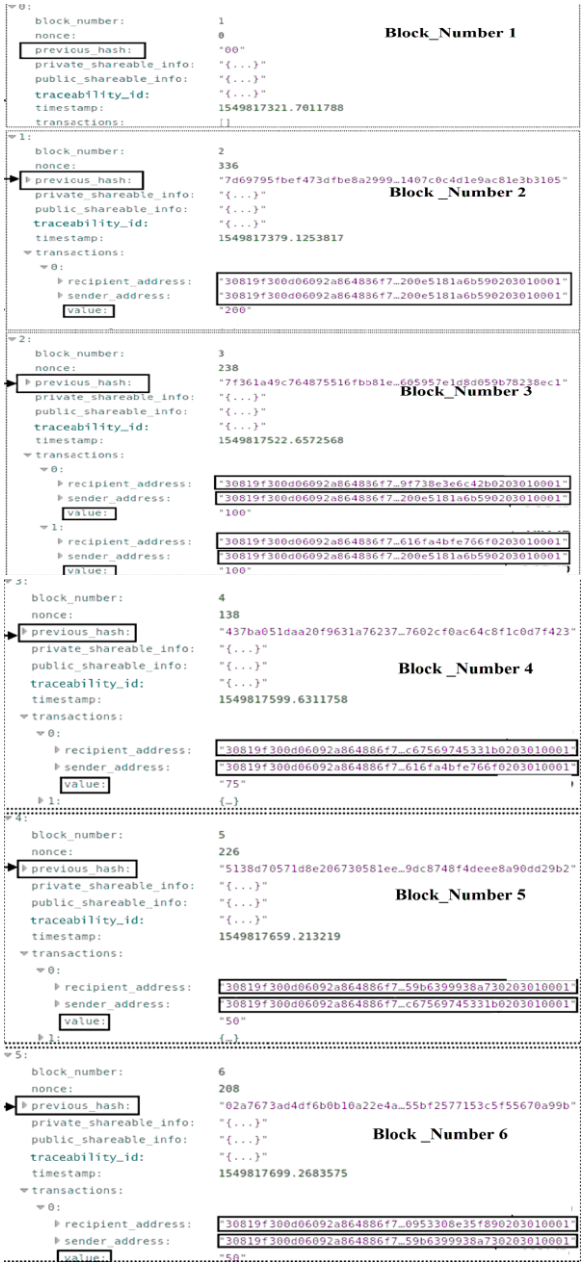

Figure 7. An instantaneous view of the entirety of the blockchain that shows transactions plus block information as they happen.

Table 3
Analysis of scaling correlations

Scalability Parameter	Store of BFT [29] [2020]	File coin [28] [2018]	Chain of Light [27] [2021]	IoT-RTS (Ours System)
Level of extensibility	Low	High	Low	**High**
Degree of decentralization	Full	Semi-Type	Semi-Type	**Full**
Cost of communication Value	High	High	Low	**Low**
Consensus protocol	Proof-of-validation	Proof-of-stake	Proof-of-Replication	**Concept-proof prototype**
Authentication	-	-	Yes	**Yes**
Privacy level Value	Low	Low	High	**High**
Complexity of computation	High	High	Low	**Low**
Expansion strategy	Block type copy	Block type copy	Hybrid type copy	**Multiple side type chains**

Table 4:
Model contrast

Model	Year of Publication	Blockchain	Access control	Storage method	Privacy protection
UPHFPR [23]	2022	X	Support	Centralized	Support
FTAC [24]	2020	X	Support	Centralized	Support
FLP-RA [25]	2021	Support	X	Single Chain	X
BAEAC [26]	2021	Support	Support	Single Chain	X
BBMD [30]	2019	Support	X	Single Chain	Support
IoT RTS (Our System)	**2023**	**Support**	**Support**	**Multi-chain isolation**	**Support**

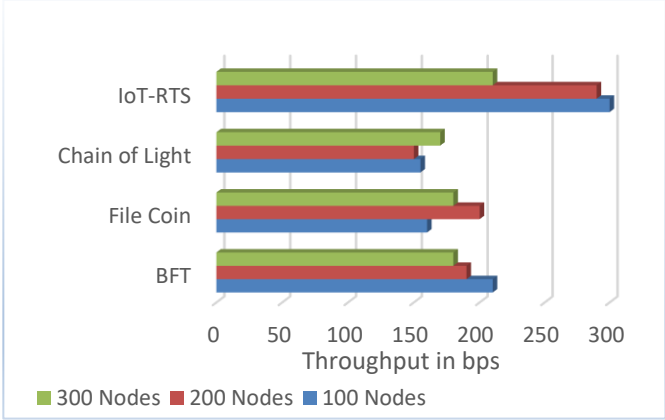

Figure 8. Throughput Comparison different Model

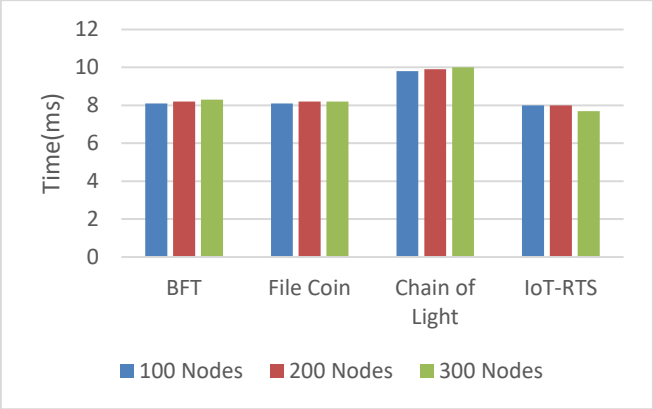

Figure 9. Comparative Analysis of Execution Time on different Models

9. CONCLUSION

As part of our investigation, we developed a system for controlling reputation and trust that is based on blockchain and is intended for use in large-scale Internet of Things applications. We began by comparing the role & attribute-based access control, also known as RBAC and ABAC, to the Reputation & Trust based access control model, also known as RTS. In doing so, we were able to highlight several advantages associated with selecting RTS over the other available options for the Internet of Things applications. To provide flexibility, interoperability, and data sharing across the members of the consortium, we included a novel concept in the architectural design for the processing of data about access control.

All of the components of the system, including its services, statement, resources, token generation protocol profiles, and membership service were dissected along with its authorization process. Secondly, we analysed the need for data storage with IoT access control and compared the operational aspects of databases with those of blockchains with their level of safety. During our conversation, we discussed the integration architecture as well as the benefits that come with using a database that is built on blockchain technology as the IoT-RTS data store. To demonstrate that it is possible to implement IoT-RTS, a concept-proof prototype was created and tested to see how well it would perform in terms of both safety and functionality.
Our IoT-RTS strategy produced encouraging results and was a suitable match for network applications for medical, cities and businesses. Despite the promising outcomes of our method, we continue to examine and further explore mainly the security and privacy of blockchain-based databases for access control in Industrial IoT networks and modern application
s.

REFERENCES

[1] L.P. de la Horra, G. de la Fuente, J. Perote, (2019) The drivers of Bitcoin demand: a short and long-run analysis, Int. Rev. Financ. Anal. Volume 62, pp 21–34, https://doi.org/ 10.1016/j.irfa.2019.01.006

[2] Ziroozjaei, Mahdi & Ghorbani, Ali & Kim, Hyoungshick & Song, Jaeseung. (2020). Hy-Bridge: A Hybrid Blockchain for Privacy-Preserving and Trustful Energy Transactions in Internet-of-Things Platforms. Sensors. 20. 928. 10.3390/s20030928.

[3] Meng Shen, Gaopeng Gou, Qi Xuan, (2023) Security and privacy of blockchain, Blockchain: Research and Applications, Volume 4, Issue 1,2023,100130, ISSN 2096-7209,https://doi.org/10.1016/j.bcra.2023.100130.

[4] Lydia Negka, Angeliki Katsika, Georgios Spathoulas, Vassilis Plagianakos, (2023) Blockchain state channels with compact states through the use of RSA accumulators, Blockchain: Research and Applications, Volume 4, Issue 1, ISSN 2096-7209, https://doi.org/10.1016/j.bcra.2022.100114.

[5] Jens Ducrée, (2020) Research – A blockchain of knowledge, Blockchain: Research and Applications, Volume 1, Issues 1–2,2020,100005, ISSN 2096-7209, https://doi.org/10.1016/j.bcra.2020.100005.

[6] Biswas S, Sharif K, Li F, Maharjan S, Mohanty SP, Wang Y. (2019). Pobt: a lightweight consensus algorithm for scalable IoT business blockchain. IEEE Internet of Things Journal, Volume 7, Issue 3, :2343–2355.DOI 10.1109/JIOT.2019.2958077.

[7] Bouras MA, Lu Q, Zhang F, Wan Y, Zhang T, Ning H. (2020). Distributed ledger technology for e-health identity privacy: state of the art and future perspective. Sensors 20(2):483. DOI 10.3390/s20020483.

[8] Camero A, Alba E. (2019). Smart city and information technology: a review. Cities 93(0):84–94.DOI 10.1016/j.cities.2019.04.014.

[9] Dhelim S, Ning H, Bouras MA, Ma J. (2018). Cyber-enabled human-centric smart home architecture. In: IEEE Smart World, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI). Piscataway: IEEE, 1880–1886.

[10] Paul, N. & Raj, D. (2021). Enhanced Trust Based Access Control for Multi-Cloud Environment. Computers, Materials & Continua. 69. 3079-3093. 10.32604/cmc.2021.018993.

[11] Bouij-Pasquier, I., Ouahman, A.A., El Kalam, A.A. and de Montfort, M.O., (2015), November. SmartOrBAC security and privacy in the Internet of Things. In IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA) pp. 1-8.

[12] El Bouanani, S., El Kiram M.A., Achbarou O. and Outchakoucht A., (2019). Pervasive-Based Access Control Model for IoT Environments. IEEE Access, Volume 7, pp.54575-54585.

[13] Maesa, D.D.F., Mori, P. and Ricci, L., (2017), Blockchain based access control. In IFIP international conference on distributed applications and interoperable systems, Springer, Cham. pp. 206-220.

[14] Ding, S., Cao, J., Li, C., Fan, K. and Li, H., (2019). A Novel Attribute-Based Access Control Scheme Using Blockchain for IoT. IEEE Access, 7, pp.38431-38441.

[15] Novo, O., (2018). Blockchain meets IoT: An architecture for scalable access management in IoT. IEEE Internet of Things Journal, Volume 5, Issue 2, pp.1184-1195.

[16] Alphand, O., Amoretti, M., Claeys, T., Dall'Asta, S., Duda, A., Ferrari, G., Rousseau, F., Tourancheau, B., Veltri, L. and Zanichelli, F., (2018), .IoTChain: A blockchain security architecture for the Internet of Things. In IEEE Wireless Communications and Networking Conference (WCNC) IEEE pp. 1-6.

[17] Juniper Research. "Internet of Things'' connected devices to triple by 2021, reaching over 46 billion units. Available at https://www.juniperresearch.com/press/press releases/%E2%80%98internet-of-things%E2%80%99-connected-devices-triple-2021 (accessed 10 October 2021).

[18] McConaghy T, Marques R, Müller A, De Jonghe D, McConaghy T, McMullen G, Henderson R, Bellemare S, Granzotto A. (2016). Bigchaindb: a scalable blockchain database. white paper, Big-Chain-DB.

[19] Nakamura Y, Zhang Y, Sasabe M, Kasahara S. (2019). Capability-based access control for the Internet of things: an Ethereum blockchain-based scheme. In: IEEE Global Communications Conference (GLOBECOM). Piscataway: IEEE, 1–6.

[20] Nakamura Y, Zhang Y, Sasabe M, Kasahara S. (2020). Exploiting smart contracts for capability-based access control in the Internet of Things. Sensors Volume 20, Issue 6: ISSN 1793 DOI 10.3390/s20061793 .

[21] Ouaddah A, Mousannif H, Abou Elkalam A, Ouahman AA. (2017). Access Control in the Internet of Things: big challenges and new opportunities. Computer Networks Volume 112, Issue 2: pp 237–262.DOI 10.1016/j.comnet.2016.11.007.

[22] Singh J, Pasquier T, Bacon J, Ko H, Eyers D. (2015). Twenty security considerations for cloud-supported Internet of Things. IEEE Internet of Things Journal Volume 3, Issue 3: pp-269–284 DOI 10.1109/JIOT.2015.2460333.

[23] Tseng L, Yao X, Otoum S, Aloqaily M, Jararweh Y. (2020). Blockchain-based database in an IoT environment: challenges, opportunities, and analysis. Cluster Computing Volume 23, Issue 3: pp-2151–2165.DOI 10.1007/s10586-020-03138-7.

[24] Xu R, Chen Y, Blasch E, Chen G. (2018). Blendcac: a blockchain-enabled decentralized capability-based access control for its. In: IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom), and IEEE Smart Data (Smart Data). Piscataway: IEEE,1027–1034.

[25] Xu R, Chen Y, Blasch E, Chen G. (2018). A federated capability-based access control mechanism for the Internet of Things (IoT). In: Sensors and Systems for Space Applications XI, Volume 10641.Bellingham: International Society for Optics and Photonics, 106410U.

[26] Xu R, Chen Y, Blasch E, Chen G. (2019). Exploration of blockchain-enabled decentralized capability-based access control strategy for space situational awareness. Optical Engineering Volume 58, Issue 4: ISSN 041609.

[27] Yaqoob I, Ahmed E, Hashem IAT, Ahmed AIA, Gani A, Imran M, Guizani M. (2017). Internet of things architecture: recent advances, taxonomy, requirements, and open challenges. IEEE Wireless Communications Volume 24, Issue 3: pp-10–21.

[28] Jiang, R., Han, S., Zhang, Y., Chen, T., Song, J. (2022): Medical big data access control model based on UPHFPR and evolutionary game.Alex. Eng. J. Volume 61, Issue 12, pp-10659–10675.

[29] Shi, M., Jiang, R., Hu, X., Shang, J. (2020): A privacy protection method for health care big data management based on risk access control. Health Care Manag. Sci. Volume 23, Issue 3, pp-427–442.

[30] Aloqaily, M., Bouachir, O., Al Ridhawi, I (2021). Blockchain and FL based network resource management for interactive immersive services. IEEE Global Communications Conference(GLOBECOM).

[31] Lu, X., Fu, S.:(2021) A trusted data access control scheme combining attribute-based encryption and blockchain. Volume 3, pp- 7–14.

[32] Hassanzadeh-Nazarabadi, Y., Ku¨pc¸u¨, A., O¨ zkasap, O (2021): Light chain: Scalable dht-based blockchain. IEEE Trans. Parallel Distrib. Syst. Volume 32, Issue 10, pp-2582–2593.

[33] Fisch, B., Bonneau, J., Greco, N., Benet, J (2018).: Scaling proof-of replication for file coin mining. Protocol Labs, San Francisco.

[34] Qi, X., Zhang, Z., Jin, C. and Zhou, A. BFT-store (2020): storage partition for permissioned blockchain via erasure coding. IEEE 36th International Conference on Data Engineering (ICDE).

[35] Liu, X., Wang, Z., Jin, C., Li, F., Li, G. (2019): A blockchain-based medical data sharing and protection scheme. IEEE Access. Volume 7, pp-118943–118953.

[36] Pal, P., Sahana, B.C., Ghosh, S., Poray, J., Mallick, A.K. (2021). Voice Password-Based Secured Communication Using RSA and ElGamal Algorithm. In: Panigrahi, C.R., Pati, B., Pattana yak, B.K., Amic, S., Li, KC. (eds) Progress in Advanced Computing and Intelligent Engineering. Advances in Intelligent Systems and Computing, volume 1299. Springer, Singapore. https://doi.org/10.1007/978-981-33-4299-6_32

Fundings

This work was not supported by any funding.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

We would like to show our gratitude to Prof. A. K. Mallick, Retired Professor at, Indian Institute of Technology, Kharagpur, India for sharing his pearls of wisdom with us during this research.