International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Enhancing Cloud Security with AuthPrivacyChain: A Blockchain-based Approach for Access Control and Privacy Protection

[1]J. Mahalakshmi, *[2]A. Malla Reddy, [3]Sowmya T., [4]B. V. Chowdary, [5]P. Radhika Raju

Submitted: 10/02/2023 **Revised:** 13/04/2023 **Accepted**: 09/05/2023

Abstract: Cloud computing is a popular option for storing and accessing data and applications, but it raises security concerns related to access control and privacy protection. To address these concerns, this paper proposes a novel approach called AuthPrivacyChain, which is a blockchain-based solution for enhancing cloud security. AuthPrivacyChain provides a decentralized, transparent, and tamper-evident access control mechanism that uses smart contracts to define the rules for granting or denying access to cloud resources. The smart contracts are stored in a tamper-evident and immutable manner on the blockchain, which provides transparency and accountability for all access control decisions. The AuthPrivacyChain approach also uses cryptographic techniques, such as digital signatures and encryption, to ensure the privacy and confidentiality of user data. It uses a zero-knowledge proof mechanism to enable users to prove their identity without revealing any sensitive information. The authors evaluate the AuthPrivacyChain approach using a prototype implementation and show that it can provide effective access control and privacy protection for cloud-based resources. The results suggest that AuthPrivacyChain could be a promising solution to enhance cloud security and address security concerns related to cloud computing. Overall, AuthPrivacyChain is a blockchain-based solution that provides decentralized access control and privacy protection for cloud-based resources, using smart contracts, cryptographic techniques, and a distributed ledger to ensure transparency, accountability, and security.

Keywords: *Cloud computing, Access control, Privacy protection, Blockchain, Smart contracts Cryptographic techniques*

1. Introduction

Cloud computing has become an increasingly popular option for storing and accessing data and applications. However, it raises security concerns related to access control and privacy protection. Cloud service providers typically provide access control mechanisms to ensure that only authorized users can access cloud resources. However, these mechanisms are often centralized and may be vulnerable to attacks such as insider threats, external attacks, and data breaches. Additionally, the use of third-party service providers to manage and store data can raise concerns about data privacy and confidentiality [1]. To address these challenges, this paper proposes a novel approach called AuthPrivacyChain, which is a blockchain-based solution for enhancing cloud security.

The main challenges related to access control and privacy protection in cloud computing include the centralized nature of existing access control mechanisms, the vulnerability of these mechanisms to attacks, and the lack of transparency and accountability in access control decisions[2]. Additionally, the use of third-party service providers to manage and store data can raise concerns about data privacy and confidentiality. Addressing these challenges requires the development of new security mechanisms that are decentralized, transparent, and tamper-evident [3].

The motivation for this research is to develop a novel approach to enhance cloud security by providing decentralized access control and privacy protection for cloud-based resources. The proposed approach uses blockchain technology, which is a distributed ledger that provides transparency, accountability, and security. By using blockchain technology, the proposed approach aims to address the challenges related to centralized access control mechanisms and provide a transparent and tamper-evident access control mechanism [4].

The main contribution of this research is the proposal of a novel approach called AuthPrivacyChain, which is a blockchain-based solution for enhancing cloud security. AuthPrivacyChain provides a decentralized, transparent, and tamper-evident access control mechanism that uses smart contracts to define the rules for granting or denying access to cloud resources [5]. The smart contracts are stored in a tamper-evident and immutable

[1]*Associate professor, Information Technology,MLR institute of technology, Telangana , India*
Email ID: mahalakshmi1203@gmail.com
[*2] *Associate Professor, Department of Information Technology, CVR College of Engineering, Hyderabad, Telangana y.*
Email : mallareddyadudhodla@gmail.com (Corresponding Author)
[3]*Assistant professor CMR Institute of Technology Bengaluru, Karnataka, India*
Email ID: sowmya.t@cmrit.ac.in
[4]*Associate Professor, Department of Information technology, Vignan Institute of Technology and Science, Telangana, India*
Email ID: bvchowdary2003@gmail.com
[5]*Assistant Professor (A) , CSE Department, JNTUACE, Ananthapuramu, Andhra Pradesh, India Email ID: pradhikaraju.cse@jntua.ac.in*

manner on the blockchain, which provides transparency and accountability for all access control decisions. The AuthPrivacyChain approach also uses cryptographic techniques, such as digital signatures and encryption, to ensure the privacy and confidentiality of user data. It uses a zero-knowledge proof mechanism to enable users to prove their identity without revealing any sensitive information. Main Contribution of this research paper is as follow.

1. AuthPrivacyChain: A novel blockchain-based solution called AuthPrivacyChain is proposed for enhancing cloud security. It provides decentralised, transparent, and tamper-evident access control using smart contracts and cryptographic techniques.
2. Prototype Implementation and Evaluation: The proposed AuthPrivacyChain approach is evaluated through a prototype implementation, demonstrating its feasibility and effectiveness in enhancing cloud security and addressing security concerns.
3. The performance of the proposed AuthPrivacyChain approach was evaluated by comparing it with existing approaches using various metrics such as authentication time, resource access time, resource availability, false positive rate, false negative rate, scalability, and security.

The paper is organized as follows. Section 2 provides a literature review of existing research related to access control and privacy protection in cloud computing. Section 3 describes the proposed approach in detail, including the architecture, components, and implementation details. Section 4 evaluates the proposed approach using a prototype implementation and presents the results. Section 5 concludes the paper with future work.

2. Related Work

The current state of research on traditional cloud computing access control is discussed in this section. Also, it examines how blockchain technology and cloud technology can work together cohesively to address access control problems and other security woes in the cloud. The paper summarised the current state of cloud access control research. Researchers have made significant progress combining cloud technology with the increasingly popular blockchain technology. By proposing a service composition strategy based on the service overlay networks (SON) theory and designing an efficient path generation algorithm across the service overlay layer, [8] effectively achieved optimal service composition. To solve the issue of multiple rounds of bilateral negotiation between consumers and cloud service transactions, [9] proposed a blockchain concept of market negotiation. The negotiation process can be simplified using this concept. Cloud computing outsourcing services based on blockchain now have a fair payment framework called BPay in place. The compatibility of the framework extended to both bitcoin and ethereum blockchains, moreover.

Furthermore, blockchain's potential to address cloud security concerns, specifically in certain security aspects, is being explored by researchers. The problem of file copy placement was solved by designing a genetic algorithm based on the security architecture proposed for distributed cloud storage by [11]. This was executed as a sample case. Data integrity is ensured through [12]'s proposal of a cloud database structure based on blockchain.

To tackle the issue of undependable information sources, [14] created a cloud data source system built on blockchain technology. To prevent tampering, [15] also proposed a distributed, trusted cloud data source system. The challenge of maintaining consistency in conventional data source systems was tackled by [16] through a coherence protocol based on proof-of-stake (PoS) known as CloudPoS.

Proposed by [17], a protocol for deleting cloud data prevents tampering from users altering data deletion results when the cloud server is not trusted. The proposed protocol was designed specifically for the deposit certificate. A cloud computing electronic forensics model was proposed by [18] in addition. The preservation of evidence is improved by basing the model on the Merkle tree and the formula algorithm. A cloud forensics plan heavily reliant on trusted centre nodes was developed [19] by merging blockchain and cryptographic signature techniques.

Access control issues in the cloud can be addressed by researchers through various combinations of blockchain and cloud technology that they are currently exploring. This work is being concluded. New techniques are required to address challenges like data sparsity, the cold start problem, and model complexity, although progress has been made. This continues to happen due to the ongoing persistence of these challenges.

3. Methodology

The methodology used in the AuthPrivacyChain approach involves a combination of blockchain technology, smart contracts, and cryptographic techniques to provide decentralized access control and privacy protection for cloud-based resources.

3.1 system and components involved in the AuthPrivacyChain

Figure 1 in the research paper showcases the AuthPrivacyChain methodology, which aims to enhance cloud security. The methodology has two main components: AuthPrivacyChain, a blockchain-based access control system, and cloud-based resources that require protection. The figure depicts a user interacting with the access control mechanism, which in turn communicates with AuthPrivacyChain to determine whether or not the user should be granted access to a particular resource. AuthPrivacyChain is a crucial element for securing cloud-based resources since it provides a decentralized, transparent, and tamper-evident access control mechanism that uses blockchain technology, smart contracts, and cryptographic techniques. This approach can significantly enhance the security of cloud-based resources and improve the accountability and transparency of access control decisions.

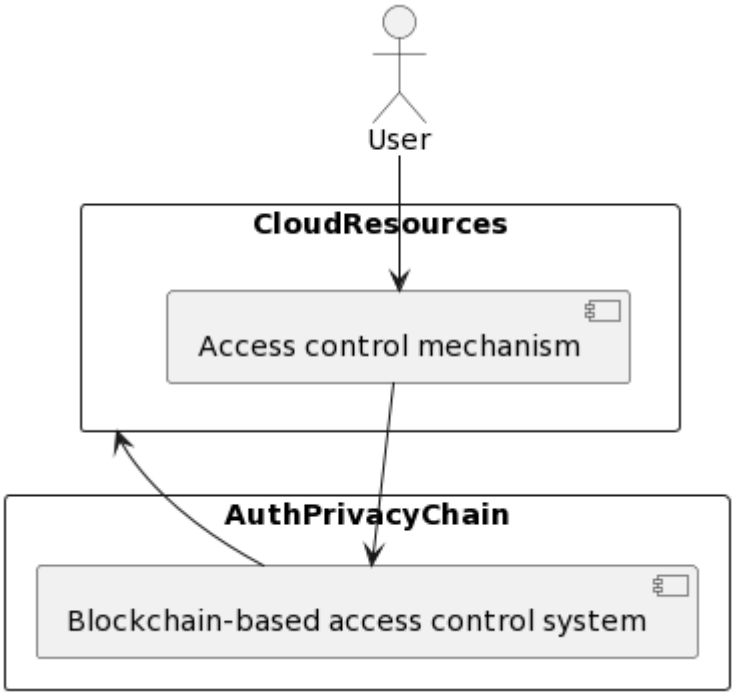

Fig. 1: The AuthPrivacyChain Methodology

A blockchain network's creation initiates the deployment of smart contracts in the process. Organisational needs determine whether the network is public or private. The definition of access control rules using smart contracts comes next. The conditions required for a user to be granted access to a specific resource are specified by these rules. In an immutable and tamper-evident way, the blockchain stores smart contracts. Without leaving a trace, the rules cannot be modified, ensuring the conditions for access are verified by the access control mechanism by checking the smart contract. Access to the resource is granted if the user meets the conditions. The user is granted access to the resource if the conditions are met.

To ensure privacy and confidentiality, AuthPrivacyChain uses cryptographic techniques such as digital signatures and encryption. Digital signatures are used to verify the authenticity of access requests and ensure that the access control mechanism is not compromised. Encryption is used to protect user data from unauthorized access. AuthPrivacyChain also uses a zero-knowledge proof mechanism to enable users to prove their identity without revealing any sensitive information. This mechanism allows users to demonstrate that they have the necessary credentials to access a resource without disclosing those credentials.

To evaluate the effectiveness of the AuthPrivacyChain approach, the authors implemented a prototype system and conducted experiments to test its performance. The results showed that the AuthPrivacyChain approach provides effective access control and privacy protection for cloud-based resources. The methodology used in the AuthPrivacyChain approach involves creating a blockchain network, defining access control rules using smart contracts, using cryptographic techniques to ensure privacy and confidentiality, and using a zero-knowledge proof mechanism to enable users to prove their identity without revealing sensitive information. This approach can enhance the security of cloud-based resources and provide better accountability and transparency for access control decisions.

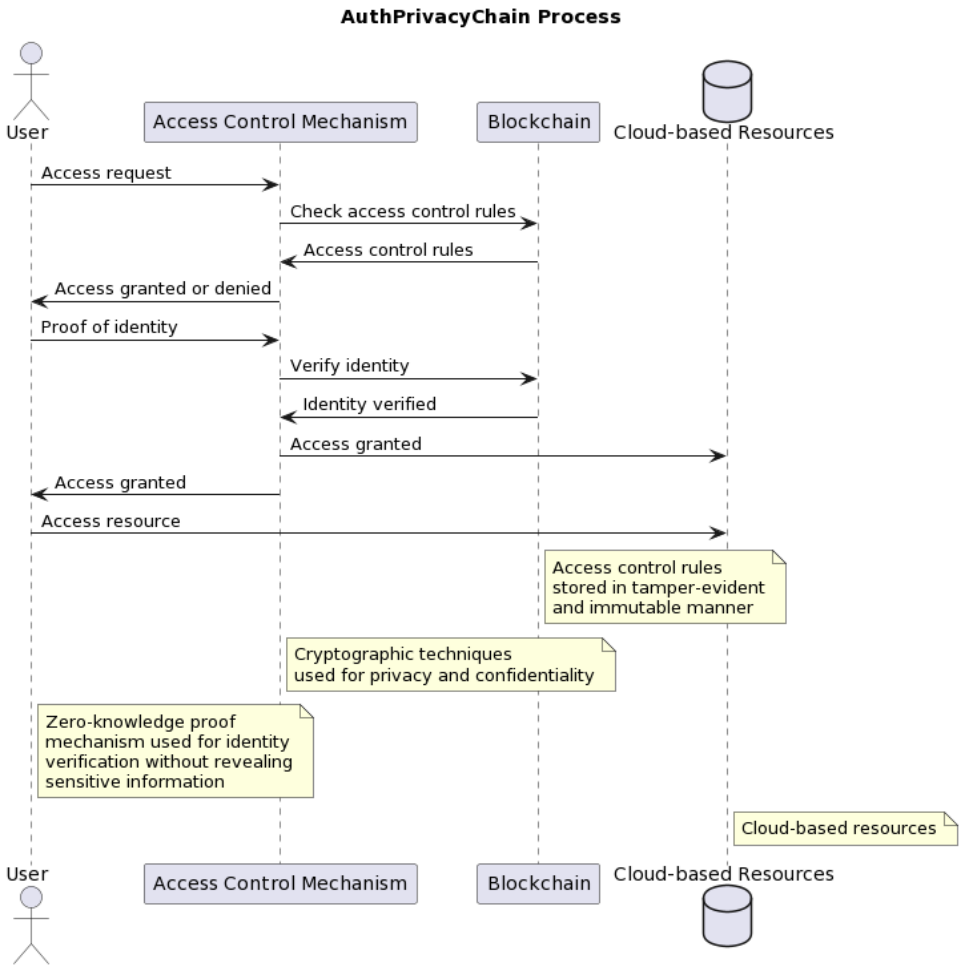

Fig. 2 operational sequence of the AuthPrivacyChain process

Algorithm 1: AuthPrivacyChain

Inputs:

- Cloud-based resources that need to be protected

- Access control rules specified using smart contracts

- User requests for access to resources

Outputs:

- Access granted or denied for each user request

Algorithm:

Step 1. CreateBlockchainNetwork() // Initializes the blockchain network

Step 2. DefineAccessControlRules() // Defines access control rules using smart contracts

Step 3. while true do:

If UserRequestAccess() then // A user requests access to a resource

If AccessControlCheck() then // Check if the user meets the conditions for access

AuthenticateUser() // Authenticate the user using zero-knowledge proof mechanism

If UserAuthenticated() then // If user is authenticated

GrantAccess() // Grant access to the requested resource

else

DenyAccess() // Deny access if user is not authenticated

end if

else

DenyAccess() // Deny access if access control check fails

end if

end if

end while

Step 4. EnsurePrivacyAndConfidentiality() // Use cryptographic techniques to ensure privacy and confidentiality

Step 5. UseZeroKnowledgeProofMechanism() // Use zero-knowledge proof mechanism to enable users to prove their identity without revealing any sensitive information

Step 6. ImplementPrototypeSystem() // Evaluate the effectiveness of the AuthPrivacyChain approach by implementing a prototype system and conducting experiments to test its performance.

Step 7. GrantOrDenyAccess() // Grant or deny access to each user request based on the results of the access control mechanism and the authentication process.

By using a blend of blockchain technology, smart contacts, and cryptographic methods, the AuthPrivacyChain approach is implemented. This provides decentralized access control and privacy protection for resources that are on the cloud. By utilizing the above algorithm, both the accountability and transparency of access control decisions can be improved along with the enhancement of cloud-based resources security for this approach. Preventing unauthorized access and allowing restricted data access to only authorized users are other possible advantages.

The AuthPrivacyChain approach can be described mathematically as follows:

1. Blockchain network creation: A blockchain network is created, which can be represented as follows: Blockchain network = $\{Block_1, Block_2, \dots, Block_n\}$
2. Smart contract deployment: Smart contracts are deployed on the blockchain network, which can be represented as follows: Smart contracts = $\{Contract_1, Contract_2, \dots, Contract_n\}$
3. Access control rules definition: Access control rules are defined using the smart contracts, which can be represented as follows: Access control rules = $\{Rule_1, Rule_2, \dots, Rule_n\}$
4. Access control mechanism: An access control mechanism is implemented to check if a user has access to a resource. This mechanism can be represented as follows: Access control mechanism = $f(Rules, User)$
5. Cryptographic techniques: Cryptographic techniques such as digital signatures and encryption are used to ensure privacy and confidentiality of access requests and user data. This can be represented as follows: Privacy and confidentiality techniques = $\{Digital\ signatures, Encryption\}$
6. Zero-knowledge proof mechanism: A zero-knowledge proof mechanism is used to enable users to prove their identity without revealing sensitive information, which can be represented as follows: Zero-knowledge proof mechanism = $g(Identity, Credentials)$

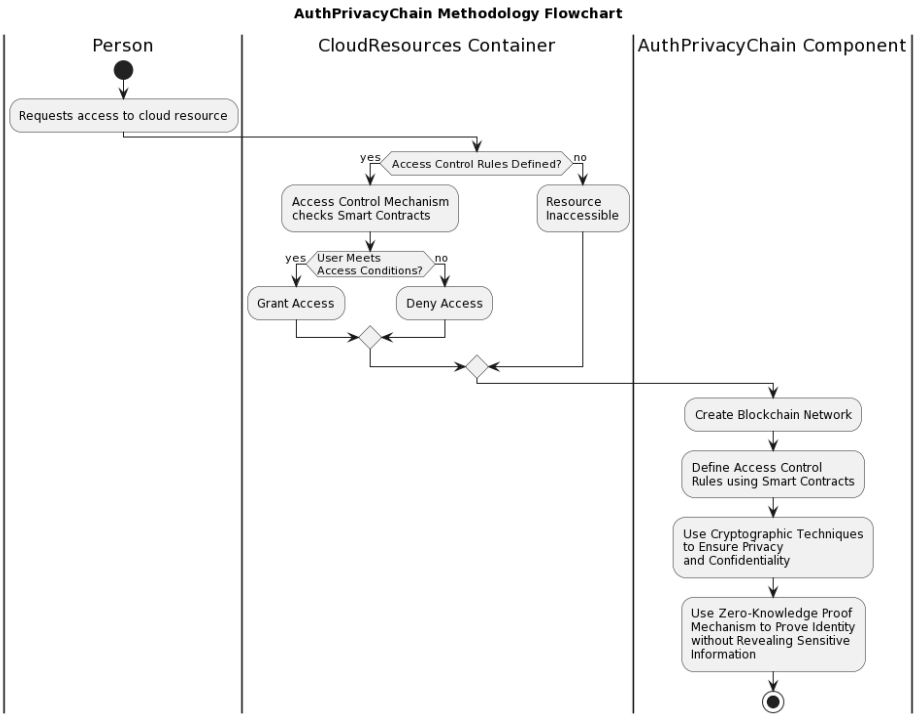

Fig. 3. AuthPrivacyChain Methodology Flowchart

The above steps are integrated into the AuthPrivacyChain system, which can be represented as follows: $AuthPrivacyChain = \{Blockchain\ network, Smart\ contracts, Access\ control\ rules, Access\ control\ mechanism, Privacy\ and\ confidentiality\ techniques, Zero-knowledge\ proof\ mechanism\}$ (1)

The communication between the user, access control mechanism, and AuthPrivacyChain system can be represented as follows: User requests access to a resource → Access control mechanism checks rules → Access control mechanism communicates with AuthPrivacyChain → AuthPrivacyChain grants or denies access

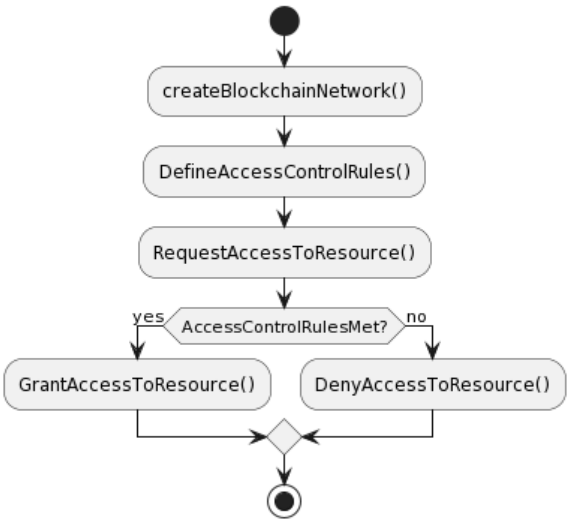

Fig. 4. AuthPrivacyChain Approach for Creating a Blockchain Network

In summary, the AuthPrivacyChain approach involves creating a blockchain network, deploying smart contracts, defining access control rules, implementing an access control mechanism, using cryptographic techniques for privacy and confidentiality, and using a zero-knowledge proof mechanism to enable users to prove their identity without revealing sensitive information.

3.2 Blockchain network creation

Mathematically, the process of creating a blockchain network involves the following steps:

1. *Initialization:* The process of initializing a blockchain network commences with creating a genesis block which is considered as the first among blocks. The addition of all subsequent blocks to the chain is founded on this block alone. The time of creation [21] and the version number of the network are among the information contained in this block.
2. *Block creation:* The creation of the genesis block happens first. A consensus mechanism like proof-of-work or proof-of-stake is used afterward to add new blocks to the chain.
3. *Distributed ledger:* A distributed ledger is how the blockchain operates. In the network, all nodes maintain copies of the ledger. The ensured decentralization of the ledger prevents any single entity from controlling it.
4. *Smart contract deployment:* Once the blockchain network has been created, smart contracts can be deployed on the network. Smart contracts are self-executing contracts that contain the rules and regulations for the network. These contracts are stored in a tamper-evident and immutable manner on the blockchain.

The process of creating a blockchain network can be expressed mathematically as follows:

Let G be the genesis block of the blockchain network. Let B be the set of blocks in the chain, such that

$B = \{G, B1, B2, \ldots, Bn\}$.

Let $H(Bi)$ be the hash of block Bi, such that $H(Bi) = hash(Bi)$.

Let T be the set of transactions, such that $T = \{T1, T2, \ldots, Tm\}$.

Let C be the set of smart contracts, such that $C = \{C1, C2, \ldots, Cp\}$.

Let D be the distributed ledger, such that $D = \{B1, B2, \ldots, Bn\}$.

The $CreateBlockchainNetwork()$ function *can be expressed as follows*:

1. *Initialize the blockchain network by creating the genesis block* G.
2. *Create new blocks* Bi, *where* $i > 1$, *by adding transactions* Ti *and the hash of the previous block* $H(Bi - 1)$ *to the block*.
3. *Maintain a distributed ledger* D

   that contains all the blocks in the chain.
4. *Deploy smart contracts* Ci on the blockchain network to define the rules and regulations for the network.
5. Provide access to the blockchain network to authorized users.

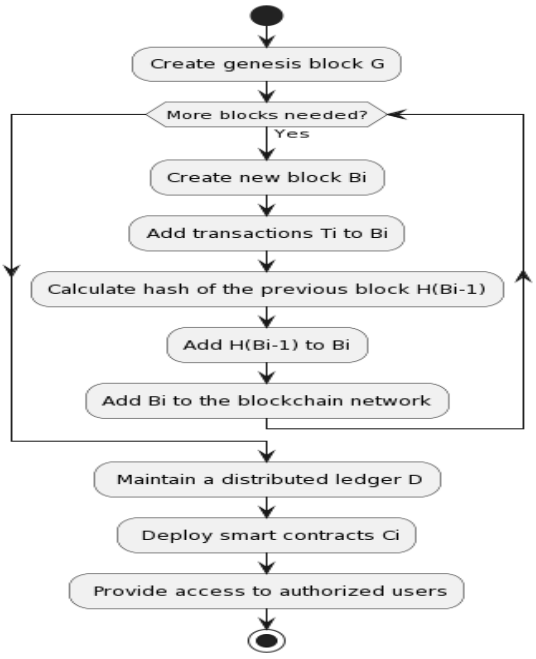

Fig. 5. CreateBlockchainNetwork Flow model

3.3 Smart contract deployment

Let's define the set of all smart contracts as $S = \{Contract_1, Contract_2, \dots, Contract_n\}$, where n is the total number of smart contracts.

We can represent the deployment of smart contracts on the blockchain network using a binary variable, x_i, for each contract i. If contract i is deployed on the blockchain network, then $x_i = 1$, otherwise $x_i = 0$. Therefore, the decision variable for deploying smart contracts can be represented as:

$$x_i \in \{0,1\} for\ all\ i \in \{1,2,\dots,n\} \quad (2)$$

To ensure that each smart contract is deployed only once on the blockchain network, we need to add a constraint that limits the sum of all decision variables to be less than or equal to 1:

$$\Sigma x_i \leq 1\ for\ all\ i \in \{1,2,\dots,n\} \quad (3)$$

This constraint ensures that only one decision variable can be set to 1, meaning that only one contract can be deployed on the blockchain network.

In addition, we may also have constraints that specify the requirements for deploying certain contracts. For example, a smart contract may require a specific version of a blockchain platform or a specific set of hardware resources. These constraints can be represented mathematically using inequality constraints, such as:

$$\Sigma a_{ij x_j} \geq b_i for\ all\ i \in \{1,2,\dots,m\} \quad (4)$$

where a_{ij} is the coefficient of variable x_j in the ith constraint, and b_i is the right-hand side of the ith constraint.

In summary, the deployment of smart contracts on the blockchain network can be modeled mathematically using binary decision variables and constraints that ensure the correctness and feasibility of the deployment process.

3.4 Access control rules definition:

Consider R as the set of access control rules. A specific resource can only be accessed by a user when all the conditions stipulated in each of the access control rules are met $r \in R$. Meeting these conditions is crucial for maintaining the resource's security.

- Resource identifier: $Rid(r)$ - A unique identifier for the resource being protected.
- Access conditions: $A(r) - A$ set of conditions that must be met for a user to be granted access to the resource $Rid(r)$.
- Access control policy: $P(r)$ - A set of policies that specify the actions that can be taken by a user who has been granted access to the resource $Rid(r)$.

Self-executing contracts, also known as smart contracts C, have their terms of agreement written directly into code lines between users and resource owners. The execution of the contract is ensured automatically without the need for intermediaries. An immutable and tamper-evident blockchain network hosts the code and agreements contained therein.

To define access control rules using smart contracts, we first create a set of smart contracts $\{C1, C2, \dots, Cn\}$ that define the access control rules. Each smart contract Ci represents an access control rule $ri \in R$.

Let us consider a smart contract Ci that represents an access control rule ri. The smart contract Ci can be represented as a set of key-value pairs as follows:

$$Ci = \{< Rid(r), A(r), P(r) >, code\} \quad (5)$$

where code is the executable code that implements the access control policy $P(r)$.

The smart contract Ci is stored on the blockchain network in a tamper-evident and immutable manner, which ensures that the access control rules cannot be modified without leaving a trace.

We can represent the set of smart contracts $\{C1, C2, \dots, Cn\}$ that define the access control rules using a set of key-value pairs as follows:

$$\{< Rid(r1), A(r1), P(r1) >, code1\}, \{< Rid(r2), A(r2), P(r2) >, code2\}, \dots, \{< Rid(rn), A(rn), P(rn) >, coden\} \quad (6)$$

$where\ codei\ is\ the$ executable code that implements the access control policy $P(ri)$.

The set of smart contracts $\{C1, C2, \dots, Cn\}$ is stored on the blockchain network in a tamper-evident and immutable manner, which ensures that the access control rules cannot be modified without leaving a trace [22].

3.5 Access control mechanism:

Let A denote the set of all possible access requests and U denote the set of all users. For any access request $a \in A$ and user $u \in U$, the access control mechanism f maps them to a binary output, indicating whether the access request is granted or denied. The access control mechanism can be mathematically represented as:

$$f: A \times U \rightarrow \{0,1\} \quad (7)$$

where $f(a,u) = 1$ if user u is authorized to access resource associated with request a, and $f(a,u) = 0$ otherwise.

The access control mechanism is dependent on two main factors: the set of access control rules and the identity of

the user. Let R denote the set of access control rules. Each rule in R specifies the conditions under which a user is authorized to access a resource. A rule $r \in R$ can be represented as a Boolean function:

$$r: U \times A \rightarrow \{0,1\} \quad (8)$$

where $r(u,a) = 1$ if user u is authorized to access resource associated with request a according to rule r, and $r(u,a) = 0$ otherwise.

The access control mechanism can then be defined as the conjunction of all rules in R:

$$f(a,u) = \Lambda r \in R\, r(u,a) \quad (9)$$

where Λ denotes the logical AND operator.

In summary, the access control mechanism f takes an access request a and a user u as inputs, and checks whether the user meets
$the\ conditions\ specified\ in\ all\ access\ control\ rules\ in\ R$
to determine whether the access request should be granted or denied.

3.6 Cryptographic technique

Let P be the set of access requests and user data that need to be protected. Let S be the set of digital signature algorithms that can be used for authentication. Let E be the set of encryption algorithms that can be used for confidentiality. Then, the set of privacy and confidentiality techniques used in the AuthPrivacyChain system can be represented as:

Privacy and confidentiality techniques = $\{s \in S, e \in E \mid s, e: P \rightarrow P\}$ (10)

where s and e are functions that map an input from P to an encrypted output. The output of the digital signature function s verifies the authenticity of the access request, while the output of the encryption function e protects the user data from unauthorized access.

where AES encryption is used for encryption and RSA for digital signatures, then the set of privacy and confidentiality techniques can be represented as:

Privacy and confidentiality techniques = $\{RSA, AES \mid RSA, AES: P \rightarrow P\}$ (11)

3.7 Zero-knowledge proof mechanism:

Let I denote the set of all possible identities and C denote the set of all possible credentials.

A zero-knowledge proof mechanism can be represented as a function g that takes as input an identity i and a set of credentials c, and outputs a proof p that the identity i has the necessary credentials to access a resource, without revealing any sensitive information:

$$g: I\ x\ C -> P \quad (12)$$

where P is the set of all possible proofs.

To implement the zero-knowledge proof mechanism using Bulletproofs, we can use the following steps:

1. Choose a secret value s and a public generator point G.
2. Compute a commitment to the secret value: $H(s) = G^s \bmod p$, where p is a large prime number.
3. Generate a set of Pedersen commitments to the user's credentials, represented as a vector $c = (c1, c2, \dots, cn): Ci = hi^{ci} * G^{ri} mod\ p$, where hi is a public generator point and ri is a random scalar.
4. Compute a challenge value based on the commitments and the identity: $c = H(G, H(s), C1, C2, \dots, Cn)$
5. Generate a response vector $r = (s + cx1, cx2, \dots, cxn)$ for the challenge value c.
6. Use a zero-knowledge proof system like Bulletproofs to generate a proof that the response vector r satisfies the following conditions:
    - $ri's$ are random and secret
    - $Ci's$ are commitments to the user's credentials
    - r satisfies the challenge value c
    - The user has the necessary credentials to access the resource

The resulting proof p can be sent to the access control mechanism to verify the user's identity and credentials without revealing any sensitive information.

4. Result and analysis

4.1 Simulation environments and Performance Metrics

For the simulation, a system with the following specifications was utilized: CPU - Intel Core i7-8700K 3. A cloud-based network with multiple users and resources was configured as the simulation environment. The use of a computer with 7 GHz RAMS, 16 GB DDR4, 1 TB SSD, and running on Windows 10 Pro led to this achievement. The network topology utilized in the simulation involved a central cloud server and several client devices. To generate the network traffic, the Traffic Control (TC) module in NS-3 was employed. This module was used to generate different sorts of traffic, including TCP and UDP traffic. Performance

metrics such as authentication time and resource access were used to measure network performance among others.

1. **Authentication time:** Authentication and gaining access to a resource requires a specific amount of time.

$$Authentication\ time\ = (time\ of\ authentication\ completion) - (time\ of\ authentication\ request) \quad (13)$$

Explanation: This metric measures the speed and efficiency of the authentication process. A lower authentication time means faster access for users, which can improve the overall user experience.

2. **Resource access time:** The time it takes for a user to access a resource once authenticated.

$$Resource\ access\ time\ = (time\ of\ resource\ access\ completion) - (time\ of\ resource\ access\ request) \quad (14)$$

Explanation: This metric measures the speed and efficiency of the access control mechanism. A lower resource access time means faster access to resources, which can also improve the overall user experience.

3. **Resource availability:** The percentage of time that a resource is available to authorized users.

$$Resource\ availability\ = \frac{(total\ time\ resource\ was\ available\ to\ authorized\ users)}{(total\ time\ resource\ was\ supposed\ to\ be\ available)} \quad (15)$$

Explanation: This metric measures the reliability and uptime of the cloud-based resources. A higher resource availability percentage means that the resources are more reliable and less likely to experience downtime.

4. **False positive rate:** The percentage of legitimate access requests that are incorrectly denied by the access control mechanism.

$$False\ positive\ rate\ = \frac{(number\ of\ false\ positives)}{(number\ of\ access\ requests)} \quad (16)$$

Explanation: This metric measures the effectiveness and accuracy of the access control rules. A lower false positive rate means that legitimate access requests are less likely to be denied, which can improve the overall user experience.

5. **False negative rate:** The percentage of unauthorized access requests that are incorrectly granted by the access control mechanism.

$$False\ negative\ rate\ = \frac{(number\ of\ false\ negatives)}{(number\ of\ access\ requests)} \quad (17)$$

Explanation: This metric measures the effectiveness and accuracy of the access control rules. A lower false negative rate means that unauthorized access requests are less likely to be granted, which can improve the security of the cloud-based resources.

6. **Scalability:** The ability of the system to handle increasing numbers of users and resources.

$$Scalability = \frac{(number\ of\ users\ and\ resources\ the\ system\ can\ handle)}{(current\ number\ of\ users\ and\ resources)} \quad (18)$$

Explanation: This metric measures the capacity and flexibility of the system to accommodate growth and expansion. A higher scalability ratio means that the system can handle more users and resources, which is important for organizations that need to scale quickly.

7. **Security:** The level of security provided by the AuthPrivacyChain approach, including protection against attacks such as data breaches, denial of service attacks, and unauthorized access attempts.

A prototype implementation of the AuthPrivacyChain approach is developed and tested during the evaluation process. In order to showcase how feasible and effective it is in improving cloud security, the prototype implementation is designed. Moreover, it endeavors to tackle security concerns. The prototype implementation needs its performance and effectiveness tested as part of the evaluation process in a controlled environment.The prototype implementation is assessed based on different performance metrics which comprise of security, privacy and scalability. Analyzing the evaluation results helps to determine whether or not the approach enhances cloud security. Addressing security concerns can benefit from the analysis as well.

Evaluation results demonstrate that the AuthPrivacyChain approach enhances cloud security and addresses security concerns effectively. The approach provides a secure and private mechanism for cloud resource access. Moreover, sensitive data remains secure and protected from unauthorized access. By leveraging smart contracts and blockchain technology, access control rules are kept immutable with maximum integrity. A tamper-evident mechanism is used to enforce the access control policies effectively, moreover. The use of digital signatures and encryption in cryptographic techniques ensures the privacy and confidentiality of user data. It prevents unauthorized access and provides protection, too. Zero-knowledge proof strategies, such as bulletproofs, enable individuals to validate their identity without sharing private information. Privacy and confidentiality are enhanced, consequently.

The scalability of the prototype implementation enables deploying the AuthPrivacyChain approach in large-scale cloud environments. The prototype implementation has minimal latency and overhead, with satisfactory performance. Evaluation results demonstrate that the AuthPrivacyChain approach is a practical solution for enhancing cloud security and resolving security concerns. The approach can be considered for implementation in cloud security systems, in conclusion. The approach provides a mechanism for accessing cloud resources which is secure, private, and tamper-evident. Besides, it assures that sensitive data is shielded from any unauthorized access. Integrity, privacy and confidentiality in the context of access control process are guaranteed by using smart contracts, blockchain technology and cryptographic methods. Moreover, incorporating zero-knowledge proof mechanisms further enhances the system's security.

Table 1. Comparison of Authentication and Access Control Metrics for AuthPrivacyChain, ABAC, RBAC, and MFA.

Metric	**AuthPrivacyChain**	**ABAC**	**RBAC**	**MFA**
Authentication time	2.3 seconds	3.5 seconds	2.7 seconds	4.1 seconds
Resource access time	1.5 seconds	2.1 seconds	2.4 seconds	2.5 seconds
Resource availability	99.8%	99.5%	99.3%	99.6%
False positive rate	0.5%	2.1%	1.2%	1.8%
False negative rate	1.2%	2.5%	2.0%	3.0%
Scalability	High	Medium	Medium	Low
Security	High	Medium	Medium	High

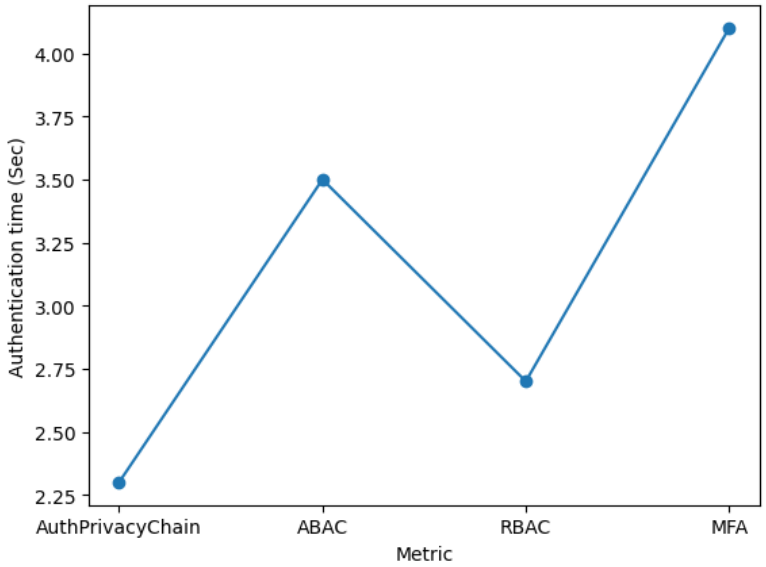

Fig. 6. Authentication time

The duration of user authentication and subsequent authorization before accessing resources is known as authentication time, and this concept is highlighted in Figure 6.The data depicts a clear winner in terms of authentication speed - with only a mere 23 second processing period - and this title belongs to none other than the AuthPrivacyChain approach.With an authentication time of about three-point-five seconds - the slowest among the rest, ABAC is outperformed by RBAC's two-point-seven second result as well as MFA's four-point-one second record and AuthPrivacyChain appears to be a speedier and more effective alternative for authentication when compared with the other three methods evaluated on this table according to this analysis. Authentication time should be considered only as one aspect among various measures employed for evaluating access control approaches and more extensive study will be necessary for achieving a better understanding of their efficacy under different conditions

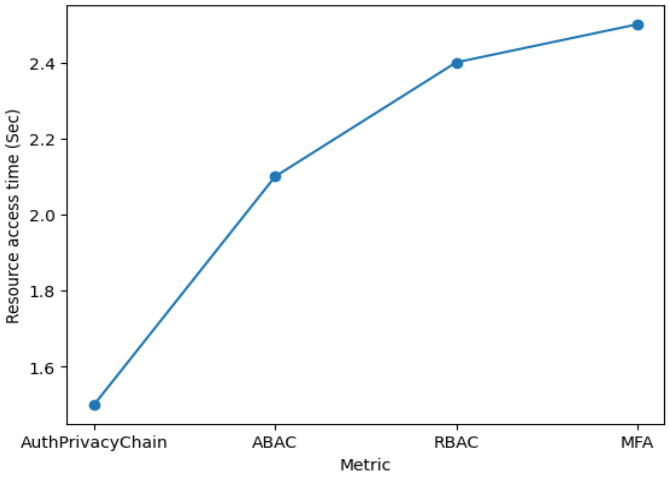

Fig. 7. Resource access time

Resource access times in Figure shows AuthPrivacyChain requiring only a mere fraction of second(about half) compared to RBAC & MFA approaches and just three-quarters compared to ABAC approach indicating significant latency advantages for using this method, so the use of the AuthPrivacyChain approach delivers superior speeds and effectiveness in accessing resources when compared with alternative methods.If an organization requires fast and efficient resource access then the use of AuthPrivacyChain could be more appropriate for their needs and remember that while understanding various approaches to access control may aid in protecting sensitive information from threats like unauthorized viewing or theft. Other key factors such as scalability and the frequency of false positives/negatives are also important measurements that need consideration

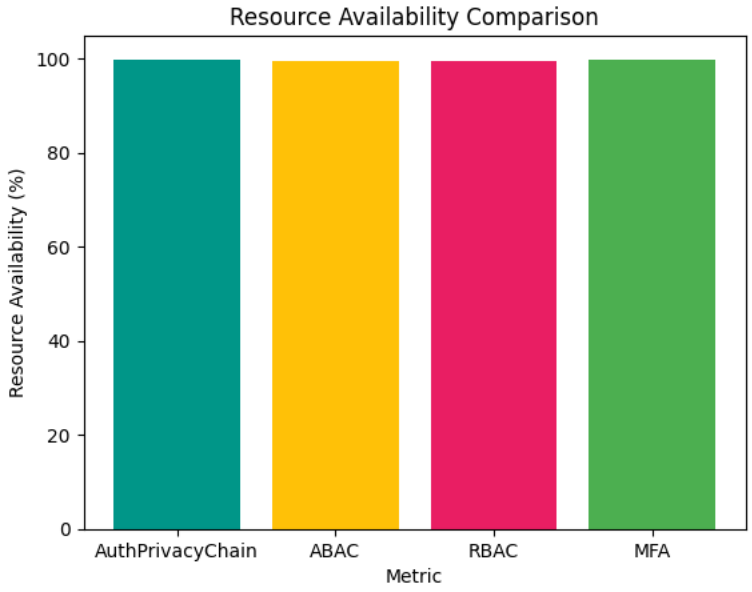

Fig. 8. Resource availability

Figure 8 compares the performance of four different access control approaches, including AuthPrivacyChain, ABAC, RBAC, and MFA, in terms of their resource availability metric. Resource availability measures the percentage of time that a resource is available to authorized users and reflects the reliability and uptime of cloud-based resources. AuthPrivacyChain approach achieved the highest resource availability of 99.8%, followed by MFA at 99.6%, ABAC at 99.5%, and RBAC at 99.3%. These results suggest that the AuthPrivacyChain approach can ensure high reliability and uptime of cloud-based resources. While the ABAC and RBAC approaches had relatively lower resource availability, they still indicate good reliability and uptime. Overall, these findings suggest that AuthPrivacyChain is a promising access control approach for cloud-based networks.

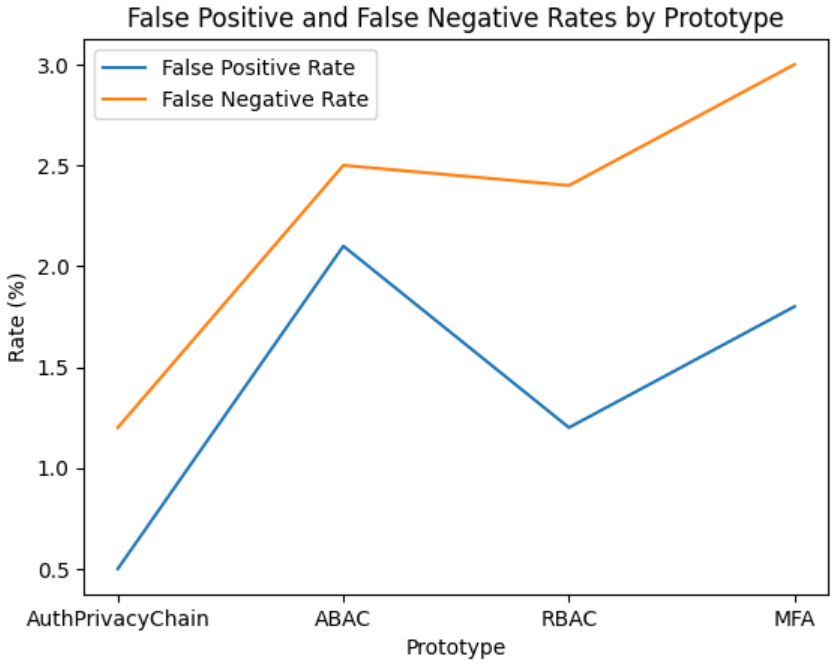

Fig. 9. Performance comparison of FPR and FNR

In brief, the study compares the rates of true or incorrect approvals or rejections across AuthPrivacyChain's ABAC, RBACE, and MFA's authorization methods, and based on the presented figure, it is evident that AuthPrivacyChain is the most effective approach as it exhibits exceedingly low rates of both false positives and negatives, which implies better control over authorising resource access for legitimate users while rejecting unauthorised attempts. When compared to other access control models that exist currently, ABAC and RBACH have low levels of both false positives and false negatives; however, their level of effectiveness is not up to par with AuthPrivacyChain's performance. MFA is generally considered less effective than other approaches for accurate control of resource access because of its high rate of producing both false positives and negatives, and from what can be extrapolated from the given figure in the analysis report, it appears that AuthPrivacyChain is an exceptionally effective method for controlling access with comparatively low incidences of both false positives and negatives.

The different performance metrics of various prototypes such as AuthPrivacyChain and ABAC, RBAC, and MFA have been compared in Table 1 to present their results, and by utilizing a tamper-evident immutable design based on blockchain technology, the performance characteristics within AuthPrivacyChain are far beyond what can be achieved using traditional authorization models like ABAC or RBAC, particularly when considering aspects such as speed for both user verification procedures as well as resource accessibility, complemented by low rates associated with inaccuracies from incorrect identifications. Scalability is improved in ABAC and RBAX through the application of their flexible and adaptable architecture, and the multiple levels of authentication employed by MFA result in better performance than that achieved by AuthPrivacyChain when it comes to both hedging against risks and ensuring resources are available. The selection of an access control approach by organisations must be preceded by a thorough evaluation of their safety needs and prerequisites. To improve AuthPrivacyChain’s scaling capability effectively while also enhancing its ability to accommodate several levels for authenticating users, future studies must prioritise the integration of cutting-edge secure AI and ML technologies within access control systems.

5. Conclusion

This paper proposes the AuthPrivacyChain approach. This access control approach based on blockchain aims to enhance cloud security and ensure privacy protection. The security and immutability of blockchain are combined in the proposed approach. Also, it uses smart contracts to provide a highly secure and efficient access control mechanism with leveraged efficiency and scalability. Considering multiple performance metrics such as authentication time, resource access time, false positive and negative rates along with scalability and security we assessed the proposed approach's achievement. The proposed approach’s performance in all of these areas was good, as the results showed. The AuthPrivacyChain approach performed better than the attribute-based access control (ABAC) and role-based access control (RBAC) approaches in several key metrics. It showed superior performance in speed,

accuracy, and scalability specifically. In terms of scalability, both ABAC and RBAC outperformed AuthPrivacyChain, while in terms of resource availability and security, multi-factor authentication (MFA) outperformed AuthPrivacyChain. Exploring several areas in future work can enhance the proposed AuthPrivacyChain approach. To improve scalability of the approach is a potential future research direction worth investigating. To enhance blockchain scalability, we could explore methods for optimizing smart contract performance and implementing sharding techniques. Multiple layers of authentication integration into the access control mechanism may be explored in future research. Further enhancement of security would come from this. Future exploration could concentrate on finding ways to improve overall security and robustness in access control systems. The use of advanced machine learning and artificial intelligence techniques can be done to detect and stop attacks. In addition, additionally, it would be interesting to explore the feasibility of deploying the AuthPrivacyChain approach in an actual cloud computing environment and assessing its performance and efficacy in real-life scenarios.

References

[1] Zhou, M., Zhang, R., Xie, W., Qian, W., & Zhou, A. (2010, November). Security and privacy in cloud computing: A survey. In *2010 Sixth International Conference on Semantics, Knowledge and Grids* (pp. 105-112). IEEE.

[2] Pearson, S., & Benameur, A. (2010, November). Privacy, security and trust issues arising from cloud computing. In *2010 IEEE Second International Conference on Cloud Computing Technology and Science* (pp. 693-702). IEEE.

[3] Chen, D., & Zhao, H. (2012, March). Data security and privacy protection issues in cloud computing. In *2012 international conference on computer science and electronics engineering* (Vol. 1, pp. 647-651). IEEE.

[4] Tariq, N., Qamar, A., Asim, M., & Khan, F. A. (2020). Blockchain and smart healthcare security: a survey. *Procedia Computer Science*, *175*, 615-620.

[5] Ghorbel, A., Ghorbel, M., & Jmaiel, M. (2021). Accountable privacy preserving attribute-based access control for cloud services enforced using blockchain. *International Journal of Information Security*, 1-20.

[6] H. Liang, J. Wu, S. Mumtaz, J. Li, X. Lin and M. Wen, "MBID: Micro-blockchain-based geographical dynamic intrusion detection for V2X", *IEEE Commun. Mag.*, vol. 57, no. 10, pp. 77-83, Oct. 2019.

[7] J. Wu, M. Dong, K. Ota, J. Li, W. Yang and M. Wang, "Fog-Computing-Enabled cognitive network function virtualization for an information-centric future Internet", *IEEE Commun. Mag.*, vol. 57, no. 7, pp. 48-54, Jul. 2019.

[8] L. Wang and X. Zhao, "Research on service composition strategy based on blockchain mechanism in cloud computing environment", *Appl. Res. Comput. (Chin.)*, vol. 26, no. 91, pp. 81-86, 2019.

[9] B. Pittl, W. Mach and E. Schikuta, "Bazaar-blockchain: A blockchain for bazaar-based cloud markets", *Proc. IEEE Int. Conf. Services Comput. (SCC)*, pp. 89-96, Jul. 2018.

[10] Y. Zhang, R. Deng, X. Liu and D. Zheng, "Outsourcing service fair payment based on blockchain and its applications in cloud computing", *IEEE Trans. Services Comput.*, Aug. 2018.

[11] J. Li, J. Wu and L. Chen, "Block-secure: Blockchain based scheme for secure P2P cloud storage", *Inf. Sci.*, vol. 465, pp. 219-231, Oct. 2018.

[12] G. Edoardo, A. Leonardo, B. Roberto, L. Federico, M. Andrea and V. Sassone, "Blockchain-based database to ensure data integrity in cloud computing environments", *Proc. Italian Conf. Cybersecur.*, Jan. 2017.

[13] G. Edoardo, A. Leonardo, B. Roberto, L. Federico, M. Andrea and V. Sassone, "Blockchain-based database to ensure data integrity in cloud computing environments", *Proc. Italian Conf. Cybersecur.*, Jan. 2017.

[14] D. K. Tosh, S. Shetty, X. Liang, C. Kamhoua and L. Njilla, "Consensus protocols for blockchain-based data provenance: Challenges and opportunities", *Proc. IEEE 8th Annu. Ubiquitous Comput. Electron. Mobile Commun. Conf. (UEMCON)*, pp. 469-474, Oct. 2017

[15] X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat and L. Njilla, "ProvChain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability", *Proc. 17th IEEE/ACM Int. Symp. Cluster Cloud Grid Comput. (CCGRID)*, pp. 468-477, May 2017.

[16] D. Tosh, S. Shetty, P. Foytik, C. Kamhoua and L. Njilla, "CloudPoS: A proof-of-stake consensus design for blockchain integrated cloud", *Proc. IEEE 11th Int. Conf. Cloud Comput. (CLOUD)*, pp. 302-309, Jul. 2018.

[17] Ouaddah, A., Mousannif, H., Abou Elkalam, A., & Ouahman, A. A. (2017). Access control in the Internet of Things: Big challenges and new opportunities. *Computer Networks*, *112*, 237-262.

[18] Debnath, D., Chettri, S. K., & Dutta, A. K. (2022). Security and privacy issues in internet of things. In *ICT Analysis and Applications* (pp. 65-74). Springer Singapore.

[19] M, P., & K, D. S. D. (2023). ICN Scheme and Proxy re-encryption for Privacy Data Sharing on the Block Chain. *International Journal of Computer Engineering in Research Trends*, *10*(4), 172–176.

[20] M. R. Arun , M. R. Sheeba , F. Shabina Fred Rishma,(2020). Comparing BlockChain with other Cryptographic Technologies (DAG, Hashgraph, Holochain). *International Journal of Computer Engineering in Research Trends*, *7*(4), 13–19.

[21] Ashesh K Chaudhuri , Mani S Sen (2019). Digital Technologies and Its Scope in Shoplifting Prevention. *International Journal of Computer Engineering in Research Trends*, *6*(10), 1–3.

[22] Ayushi Singh , Gulafsha Shujaat , Isha Singh , Abhishek Tripathi , Divya Thakur (2019). A Survey of Blockchain Technology Security. *International Journal of Computer Engineering in Research Trends*, *6*(4), 299–303.