North Asian International Research Journal of Sciences, Engineering & I.T.

IRJIF. I.F. : 3.821

ISSN: 2454-7514 Vol. 9, Issue-6 June-2023

Index Copernicus Value: 52.88 Indian Citation Index Thomson Reuters ID: S-8304-2016

NAIRJC

A Peer Reviewed Refereed Journal

DOI: 10.5949/nairjseit.2023.10.6.4

BLOCKCHAIN-DRIVEN ACCESS CONTROL: A COMPREHENSIVE SURVEY

BATTULA V. SATISH BABU[1], DR. KARE SURESH BABU[2]

[1]JNTUH, CSE, Hyderabad 500085, India
[2]Professor of CSE, School of IT, JNUTH

ABSTRACT

Access control mechanisms play a vital role in ensuring the security and privacy of digital systems, while blockchain technology offers decentralization, tamper-resistant data storage, transactional transparency and many other features. This comprehensive study aims to review existing literature and technologies on the fusion of access control mechanisms and blockchain technology. It explores the current state of research, identifies trends, and assesses the advantages and challenges of integrating these two domains. Comparative analysis and deliberation of methodologies applied in blending access control mechanisms with blockchain technology provide insights into the strengths and limitations of various approaches. Furthermore, we present future research directions and opportunities for leveraging this integration to enhance security, privacy, and trust in digital systems.

KEYWORDS*: blockchain; ledger; policies; revocation; privacy; encryption; RBAC; ABAC*

I. INTRODUCTION:

In order to guarantee the security, privacy, and integrity of digital systems, access control is crucial. The fundamental components of access control involve establishing mechanisms that enable user identification, authentication, authorization, policy enforcement, auditing, and system management. Through efficient management of these elements, organizations can establish a secure and regulated access to their digital systems and resources.

Access control mechanisms hold significant importance in ensuring secure data access and management, preserving privacy, implementing non-repudiation, preventing unauthorized activities, complying with regulatory requirements, maintaining accountability and auditability, and facilitating efficient access delegation and revocation.[1]

On the other hand, users can store and share information safely and transparently using blockchain technology

system. The way transactions are recorded in blocks is similar to that of a digital ledger or record book. In blockchain, each block consists of a collection of transactions, and these blocks are linked together to create a chain. The unique characteristic of blockchain lies in its immutability. Once a block becomes part of the chain, the data within it becomes highly resistant to alteration or removal. This creates a high level of security and trust in the system.

In blockchain, there is no single person or organization that controls everything. It works through a network of people, called nodes, who collaborate to verify and approve transactions. Blockchain technology has the power to revolutionize various industries through its secure, transparent, and efficient approach to recording and validating information. It has the potential to reshape how businesses and organizations manage and authenticate data.[2]

In this paper, we present a thorough examination of the integration between access control mechanisms and blockchain technology. The subsequent sections of this paper are structured as follows: Section II of the paper provides a concise overview of blockchain technology, outlining its key features and functionalities. Section III details the methodology employed in conducting the survey, explaining the systematic approach used to gather and analyze relevant information. Moving on to Section IV, a comprehensive survey on the synergy between blockchain and access control mechanisms is presented, covering various aspects and trends in the field. Section V offers a comparative analysis, exploring different methodologies and approaches used in combining these two domains. Section VI focuses on future directions and research opportunities for further advancements in the integration of blockchain and access control. Finally, the paper concludes by summarizing the key findings and implications discussed throughout the survey.

II. BLOCKCHAIN TECHNOLOGY:

Blockchain is an innovative technology that facilitates the decentralized and distributed maintenance of a digital ledger. It enables multiple participants to collaborate on a shared database securely and transparently. Operating on a peer-to-peer network, each participant, known as a node, possesses a complete copy of the blockchain and autonomously verifies transactions. [3]

The blockchain is composed of a sequence of blocks, with each block containing a collection of transactions. These blocks are interconnected through cryptographic hashes, forming a chain-like structure. Each block has its own unique hash, timestamp, and a reference to the hash of the previous block, creating a chronological sequence of linked blocks.

Once a new transaction takes place, it is shared with the network of nodes. These nodes employ consensus mechanisms, such as proof of work (PoW) or proof of stake (PoS), to validate the transaction and achieve consensus on its legitimacy. This consensus process helps prevent double-spending and ensures agreement among the nodes regarding the validity of the transaction.

After a transaction undergoes validation, it is grouped together with other validated transactions to form a new block. This block is subsequently appended to the existing blockchain, and the data it contains is replicated across all nodes participating in the network. The decentralized nature of the blockchain ensures that no single entity has

exclusive control over the network, thereby making it challenging for malicious actors to tamper with the data stored within the blockchain. A visual representation of the key concepts and components of blockchain technology is provided in Figure 1.

Immutability is a fundamental characteristic of blockchain. Once a block becomes part of the chain, modifying or removing the data within it becomes exceptionally difficult. This inherent immutability, combined with the transparent nature of the blockchain, strengthens the security and reliability of the system, instilling trust in the integrity of the data stored within the blockchain.

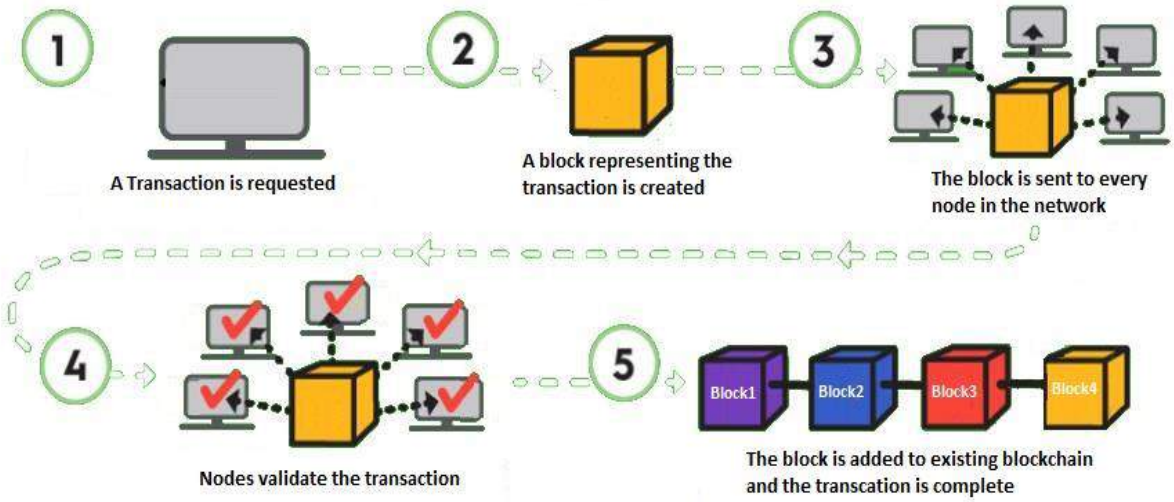

Figure 1. Overview of Blockchain technology

Blockchain technology can be leveraged to improve various aspects such as traceability, immutability, pseudonymity, auditing, data integrity, secure time stamping, identity and privacy, data sharing, reliability, and the history of transactions.

III. METHODOLOGY:

The survey paper employed a systematic approach to explore the relationship between blockchain and access control mechanisms. The research process involved conducting a thorough review of pertinent literature and technologies in the field. Extensive research was carried out, including the examination of multiple academic databases, as well as the analysis of over 300 research articles and conference proceedings related to blockchain based access control mechanisms.

This rigorous data collection process aimed to gather a comprehensive range of information and insights related to the topic at hand. Thorough analysis was conducted on the collected data to identify recurring patterns, noteworthy trends, and emerging concepts concerning the fusion of blockchain and access control mechanisms.

This approach ensures the reliability and credibility of the survey findings, making it valuable for researchers, practitioners, and policymakers working in the field of blockchain and access control.

IV. SYNERGY BETWEEN BLOCKCHAIN AND ACCESS CONTROL MECHANISMS:

In this section, we will explore different access control mechanisms and examine various contemporary studies that highlight the integration of access control mechanisms with blockchain technologies.

A) Role Base Access Control (RBAC):

RBAC is an access control mechanism where users are assigned roles within an organization, and permissions are linked to these roles rather than individual users. It grants access based on predefined roles, simplifying permission management and enhancing security. RBAC adheres to a defined format and structure, consisting of the following fundamental elements:

- **Roles:** Roles signify distinct job functions or responsibilities within an organization. Examples include "Administrator," "Manager," or "Employee." Each role is linked to specific permissions.
- **Permissions:** Permissions outline the actions or operations that users are authorized to perform within a system. These permissions encompass activities such as reading, writing, deleting, executing, or accessing specific resources or functionalities.
- **Users:** Users are individuals granted access to the system. Their access privileges are determined by assigning them one or more roles that align with their responsibilities and job functions within the organization.
- **Role Hierarchy:** In certain scenarios, roles may exhibit a hierarchical arrangement where certain roles inherit permissions from higher-level roles. For example, a "Manager" role may possess additional permissions compared to an "Employee" role, demonstrating the concept of role hierarchy.
- **Role Assignment:** Users are allocated roles based on their job responsibilities and requirements. This assignment can be performed either manually by administrators or through automated processes that consider user attributes or job roles.
- **Role-Based Policies:** RBAC operates under policies that define the access rights of roles to specific resources and actions. These policies are established to ensure compliance, security, and proper enforcement of access control measures.

Recent works have been actively exploring the synergies between blockchain technology and RBAC. The inclusion of temporal and spatial constraints in access policies has been a common approach in many of these works. These constraints enable the management of time-sensitive resource access activities, as well as facilitate functionalities such as revocation and auditing.

The FairAccess framework [4] is built upon the Organization-based Access Control (OrBAC) model and introduces an identity-based access control system with permissioned access policies. The Organization Based Access Control (OrBAC) model is designed to be context-aware and aims to resolve challenges present in extended RBAC models. However, OrBAC falls short in managing collaboration-related aspects and is primarily suited for centralized structures.

However, the level of granularity provided by OrBAC is insufficient for implementing digital asset management, particularly considering that the organization structure it employs may remain relatively unchanged

over time. To address these limitations, the authors propose integrating the OrBAC model into the FairAccess Framework, enabling the expression of access control policies that can overcome the aforementioned shortcomings.

Researchers have sought to address the limitations of FairAccess through the development of smart contract-based access control (SCBAC) [5]. SCBAC is a solution designed to enhance computing capabilities and enable the implementation of diverse access control models. It extends the functionalities of FairAccess to achieve distributed and trustworthy access control specifically for Internet of Things (IoT) systems. In many cases of access control, the incentive mechanism within SCBAC is unclear and unnecessary. Additionally, the consensus algorithm employed by SCBAC can lead to wastage of computing resources.

To enable small and medium organizations to participate and have full control over their roles, a combination of blockchain as a trusted third party and Role-Based Access Control (RBAC) can be implemented. This approach ensures that users have the ability to manage their roles effectively within a cross-organizational RBAC system [6].

In this system [6], users do not have the authority to create roles without proper permission. Additionally, any individual can verify whether a subject has access to a resource, even if that access is granted based on a role within a different organization. Users are not allowed to delegate their authority, but they have the capability to endorse each other. The authors also suggested a challenge-response algorithm for authenticating subject roles using a smart contract. Despite the heavy-weighted transactions caused by storing all smart contracts in a single-level blockchain, the current implementation of the smart contract and challenge-response authentication protocol does not address the integration of metadata.

In the BRBAC BN method [7] of Blockchain Role-Based Access Control, organizations utilize their keys to authorize users and assign roles to them. During an attempt by a user to access a dataset, the verification smart contract or transaction examines whether the user possesses a role with the necessary access rights to that specific data. Based on the outcome provided by this smart contract, the user is either granted or denied access accordingly.

The SRBAC [8] model offers a solution for delegating resource access rights to users within complex and large organizations. It introduces structural relationships that facilitate the delegation process, allowing for effective management of access control in these intricate environments. Furthermore, this model empowers users to possess context or profile-based access rights on resources. According to their suggested architecture, when a Smart Contract is executed on the public blockchain, it will generate an access token that grants access to a specific resource. The access token is provided to both regular users and third-party users, allowing them to grant and revoke access to resources effectively.

PERBAC-BC [9] is a system that merges blockchain, proxy re-encryption, and the RBAC model. It employs reencryption technology to ensure the privacy of access control policies stored on the blockchain. The decentralized and tamper-proof blockchain serves as a decentralized entity responsible for publishing access control policies. Despite its benefits, PERBAC-BC still encounters the challenge of role explosion commonly associated with RBAC. Additionally, integrating the key generation center with the blockchain becomes problematic, making it difficult to address the issue of centralization effectively.

The authors of [10] introduced a distributed storage system that facilitates the data sharing process. This system utilizes blockchain technology as its foundation to enable effective supervision and monitoring of data circulation within the platform. The attribute token, built upon the concept of colored coins, is utilized to achieve multidimensional authorization for users and accurately identify their permissions. Access control policies are stored as key/value pairs within smart contracts. By leveraging the automatic execution of smart contracts, decentralized access control decisions are implemented, effectively addressing the vulnerabilities associated with centralized security management.

B) Attribute Based Access Control (ABAC):

Attribute-Based Access Control (ABAC) model relies on attributes to make authorization decisions. In ABAC, access is determined by evaluating the attributes associated with users, objects, and environmental factors. By considering these attributes, ABAC enables more granular and flexible access control decisions based on specific attributes of the entities involved in the access request. The primary elements of Attribute-Based Access Control (ABAC) consist of:

- **Subject:** The subject represents the entity that is attempting to gain access to a resource or system. It can include users, devices, applications, or any other entity that interacts with the system.
- **Resource:** The resource refers to the specific object or system that is being accessed. This can include files, databases, networks, or any other form of digital or physical resource that is the target of the access request.
- **Action:** The action represents the specific operation or activity that a subject intends to carry out on a resource. It encompasses actions such as reading, writing, executing, deleting, or any other specific action that can be performed on the resource.
- **Environment:** The environment comprises contextual information and conditions that can impact access control decisions. It encompasses factors such as the time of access, location, network conditions, or any other pertinent environmental aspects that may influence the authorization process.
- **Policy Decision Point (PDP):** The PDP evaluates access requests by considering the access control policies and attributes associated with the subject, resource, action, and environment.
- **Policy Enforcement Point (PEP):** The PEP enforces the access control decisions made by the PDP. It acts as a gateway between the subject and the resource, ensuring that access is granted or denied in accordance with the established policies.
- **Policy Information Point (PIP):** The PIP supplies the essential attribute information to the PDP, enabling access control decisions. It retrieves attribute values from different sources like user directories, databases, or external systems.
- **Attribute Authority (AA):** The AA oversees the management and issuance of attribute values linked to subjects, resources, or other entities within the system. It guarantees the accuracy, reliability, and integrity of attribute information.

These components collaborate to assess access requests, enforce access control policies, and ascertain whether a subject should be allowed or denied access to a specific resource. Recent works have been actively exploring the synergies between blockchain technology and ABAC.

Maesa et al. [11] enhanced the conventional attribute-based access control model (ABAC) by employing blockchain as a substitute for traditional databases. This allowed them to store policies and manage access policies using transactions within the blockchain infrastructure. Nevertheless, this approach has limitations as it is applicable only to specific scenarios and supports single access control, rendering it unsuitable for IoT scenarios that necessitate one-to-many encryption.

ABAC enhances RBAC by considering subject attributes for permission granting, but as the number of subjects and services increases, the policy management system becomes complex and overburdened. Additionally, ABAC relies on centralized servers to store access control lists (ACLs), creating a single point of failure. To address this, decentralized ABAC systems utilizing blockchain have been proposed for data sharing [12], enabling data owners to control access through ABAC while sharing secret keys via decentralized key management systems.

The multi-authority architecture [13] enables multilevel access delegation, where each delegator has the ability to permit or deny further delegations. Moreover, the scheme allows for the specification of the maximum number of delegations permitted for a specific attribute through the attribute authority (AA) responsible for administering that attribute. While this scheme offers flexible and delegatable access to users, there is a notable computational overhead when revoking a particular attribute from a user. This overhead arises from the necessity to send new attribute tokens to all users who possess the revoked attribute, except for the user being revoked. Achieving attribute revocation can be easily accomplished by generating a signed revocation transaction.

In [14], the authors proposed a smart contract-based ABAC scheme where ABAC policies are stored in external databases, while their corresponding URLs are stored on the blockchain. When subjects attempt to access an object, they provide the URL of the relevant policy to a smart contract responsible for access control of the subject-object pair. The smart contract retrieves the policy from the external databases and carries out the access control process. However, a major drawback of this scheme is the storage of policies and attributes in external databases, which exposes them to potential tampering attacks. Consequently, the trustworthiness of the policies and attributes cannot be guaranteed.

To tackle the challenge related to URL-based issues presented in [14], a solution was proposed in [15]. In this approach, instead of storing policies in smart contracts, each policy is transferred into its own dedicated smart contract. While both schemes highlight the potential of blockchain-based ABAC systems, they share the common characteristic of one-to-many access control. This means that each policy is linked to a specific object and handles access requests from multiple subjects. However, this approach may impose a substantial policy management burden, particularly in large-scale IoT systems such as smart cities.

In [16], blockchain serves as a platform for validating attributes and ABAC policies, while also functioning as a policy enforcement point for any access request in the system. In this system, policies are represented as boolean expressions that specify access rules to resources based on attributes and their corresponding values. To resolve conflicts between attributes, a unique identifier is generated for each attribute.

However, process of defining attributes consistently within a single domain or across multiple domains can

become increasingly challenging and complex as the number of devices grows. Furthermore, the attribute-based access control (ABAC) model does not inherently support user-driven strategies or delegation, further adding to the complexity of policy management.

In [17] proposed an attribute-based access control (ABAC) mechanism where the owner of an object can define access rules and store them in the Blockchain. During an access request, the owner examines the conditions specified in the access control policy and sends the authorization token to the requester only if the requester satisfies those conditions.

Fabric-IOT [18] is an access control system based on blockchain technology. The administrator holds the responsibility of managing the blockchain system, including tasks such as adding new smart contracts and upgrading existing contracts. On the other hand, the common user, who is the device owner, obtains the resource URL by submitting an authorization request based on attributes to the blockchain system. Here ABAC method employs three types of smart contracts: one for storing data URLs generated by devices, another for storing ABAC policies, and a third for implementing access control methods. However, the primary challenge of this approach lies in its limited scalability when applied to a large-scale environment.

A secure, lightweight, and cross-domain access control system for IoT can be developed using a permissioned blockchain (HLF), attribute-based access control (ABAC), and identity-based signature (IBS) in [19]. Their system divides the infrastructure into multiple domains and sets up a dedicated local blockchain ledger for each domain. Within each local blockchain ledger, relevant information such as attributes of domain entities, digests of policy files, and access decisions are recorded.

In ABAC, attribute values such as usernames, IP addresses, current locations, and request times are utilized. However, this data may contain personal information or sensitive details, leading to potential privacy concerns and user data leakage issues. To address this, a solution called DID-based ABAC [20] has been proposed. This method replaces the required user attribute value with a verifiable credential during the access request. Verifiable credentials consist of a collection of claims that can uniquely identify a user, offering a privacy-enhancing approach to address the exposure of personal data in ABAC.

C) ABE Access Control (ABEBAC):

ABE Access Control is a security mechanism that integrates attribute-based encryption (ABE) with access control principles, aiming to safeguard sensitive data. ABE, or Attribute-Based Encryption, is a cryptographic technique that enables access to encrypted data based on attributes instead of individual identities. In ABE, users are assigned attribute sets, and data is encrypted using a policy that defines the required attributes for decryption.

Only users possessing the corresponding attributes can successfully decrypt and gain access to the data. By leveraging this approach, ABE provides a flexible and fine-grained access control mechanism, enhancing data security and privacy in scenarios where access permissions need to be dynamically managed.

To ensure secure management of access to encrypted data based on user attributes, the process of Attribute-

Based Encryption (ABE) Access Control typically involves the following steps:

- **Attribute Assignment:** attributes are established according to the specific criteria desired for access control. These attributes can encompass various aspects such as user roles, clearances, or any other pertinent characteristics. Subsequently, each user or entity is allocated a distinct set of attributes based on their respective roles or characteristics.
- **Attribute Encryption:**In the Data Encryption step, the owner of the sensitive data employs ABE to encrypt it. The encryption policy is formulated, taking into account the desired access control regulations.
- **Access Request:** In this phase, a user or entity formally seeks access to the encrypted data. In this process, the user presents their attribute set along with the access request, indicating the specific attributes they possess that should grant them access to the data.
- **Attribute-Based Decryption:** the access control system assesses the attributes of the user in relation to the encryption policy linked to the data. If the user possesses the attributes stipulated in the policy, the access control system authorizes access to the data.
- **Data Decryption:** Upon successful authorization, if access is granted, the user is able to decrypt the encrypted data using their private key or employing other cryptographic methods. Subsequently, the decrypted data becomes accessible to the user, enabling them to perform additional processing or view its contents.

The aforementioned process provides a basic understanding of how attribute-based encryption and access control are integrated to manage access to encrypted data based on user attributes. Recent works have been actively exploring the synergies between blockchain technology and ABEAC.

In [21], In the insurance system, a combination of blockchain technology and ciphertext-policy attribute-based encryption (CP-ABE) system is utilized to manage the storage and updates of insurance records. These records are stored in the InterPlanetary File System (IPFS) storage environment. Under this scheme, the encryption of insurance records is delegated to a fog node, which aims to enhance staff efficiency. Additionally, the encrypted insurance records are securely stored on IPFS.

In reference to [22], a combination of Blockchain and CP-ABE is employed for access control in order to enhance security However, traditional systems often rely on a trusted third-party key distribution center for generating public parameters and distributing keys. While this approach improves efficiency, it poses a security risk as the key distribution center requires direct access to a collection of user attributes, which is deemed insecure.

According to [23], data owners are provided with fine-grained one-to-many access control through CP-ABE (ciphertext-policy attribute-based encryption) and utilize smart contracts to distribute private keys. This approach eliminates the need for direct interaction between data owners and data users, thereby reducing the data sharing burden on data owners. Furthermore, the use of a trusted blockchain eliminates the requirement for a trusted third party, resulting in an automated, trustworthy, and efficient data sharing process

In blockchain-based secure data sharing platform and fine-grained access control (BSDS-FA) [24] an new

hierarchical attribute-based encryption (HABE) algorithm has been introduced, where users are assigned to different authorization centers for management purposes. In this approach, smart contracts are utilized to verify the validity of user access rights and perform partial decryption on HABE ciphertext. This implementation helps alleviate the computational burden on data consumers and enhances decryption performance.

In reference to [25], the authors propose the utilization of blockchain as a decentralized infrastructure for managing access control. To demonstrate this concept, a proof-of-concept prototype has been developed using the Multichain platform and ciphertext-policy attribute-based encryption (CP-ABE). However, it is important to note that the mentioned work does not encompass the scenario of resource protection specifically in the context of inter-organizational collaboration.

Ciphertext policy attribute-based encryption (CP-ABE) holds significant potential as a solution for distributed systems. However, the decryption phase of CP-ABE often poses computational challenges due to its intensive nature. To address this limitation, the decryption phase of CP-ABE is commonly outsourced to a consortium blockchain [26]. Moreover, the blockchain is leveraged to establish accountability mechanisms to deter and track malicious behaviors effectively.

The paper introduces a novel access control model called Timely CP-ABE [27], which incorporates two key features. Firstly, it implements a decentralized access control mechanism by verifying user legitimacy through Blockchain nodes. Secondly, it introduces a temporal dimension to file sharing using CP-ABE, enabling access authorization with validity periods without incurring additional revocation costs. The Timely CP-ABE model is implemented as a proof of concept using the CP-ABE toolkit and the Multichain solution.

Temporal ABE-DAC (Dynamic Access Control) [28], a system combining attribute-based encryption (ABE) with blockchain technology to facilitate fine-grained sharing of encrypted private data. TABE-DAC offers traceability to ensure accountability for malicious users who leak private keys. Additionally, the proposed solution enables dynamic access control, granting data owners the flexibility to update access control policies as needed. This approach aims to enhance data security, privacy, and provide greater control over access to sensitive information.

Many existing blockchain-based access control schemes primarily provide one-way access control, which may not fulfill the requirements of users seeking two-way access control. To address this limitation, a dual strategy attribute-based encryption (ABE) scheme [29] has been proposed. This scheme combines two existing approaches, namely, ciphertext-policy ABE and key-policy ABE and produce two access structures. The ciphertext holds the primary access structure and the secondary attributes, while the user's private key contains the secondary access structure and the primary attributes. Access to the ciphertext is granted only when the primary attribute set fulfills the primary access structure, and the secondary attribute set satisfies the secondary access structure. This incorporation of the dual strategy empowers users to fulfill both primary and secondary access control requirements, thereby enhancing data security and privacy.

To address issues such as access policy and attribute privacy leakage, blockchain-based access control schemes have been proposed. However, these schemes bring new challenges, including the potential inference of private

attributes from embedded access policies in ciphertexts, especially in CP-ABE schemes. Therefore, to establish a secure and trustworthy access control scheme based on blockchain, it is necessary to design a CP-ABE scheme that conceals access policies and attributes, ensuring privacy and confidentiality.

In [30], the authors introduced the initial attribute-hiding multi-authority attribute-based encryption (ABE) schemes based on decentralized IPE (Identity-based Encryption). However, these schemes were only capable of hiding the overall set of attributes, while still revealing the attributes controlled by each authority. Consequently, there is an urgent need to achieve complete attribute privacy protection when obtaining the secret key in CP-ABE (ciphertext-policy attribute-based encryption) based on blockchain.

The existing research on CP-ABE schemes with hidden access policies can be classified into two forms: full hidden [31] and partial hidden [32]. In the fully hidden approach, none of the attributes can be revealed through the access policies, ensuring stronger privacy protection. On the other hand, the partially hidden approach focuses on concealing a sensitive subset of attributes that are revealed in the access policies, offering improved efficiency. It's worth noting that while fully hidden access policies guarantee better privacy, partially hidden access policies provide enhanced efficiency.

Trust Access in [33] propose an optimized hidden policy CP-ABE (Hidden Policy Ciphertext-Policy Attribute-Based Encryption) called HP-CP-ABE is proposed. The main objective of HP-CP-ABE is to ensure policy privacy while meeting the access requirements for a large universe of attributes. Additionally, ElGamal homomorphic encryption is employed to safeguard attribute privacy during authorization validation. Furthermore, the security of Trust Access is theoretically proven by considering both blockchain operations and HP-CP-ABE.

To address the requirements of decentralized authorization and flexible revocation, the Key-Policy Attribute-Based Encryption scheme with Multiple Authorities and Flexible Revocation (MAFR-KP-ABE) has been introduced. In MAFR-KP-ABE [34], the user's identity is incorporated into the decryption key to enable traceability, making it particularly suitable for scenarios involving paid data sharing. Multiple authorities are responsible for generating the decryption key for users independently, without requiring collaboration with each other. User revocation is carried out by relevant authorities, eliminating the need for involvement from unrelated authorities and users.

D) Capability Based Access Control (CapBAC):

Capability-based access control is well-suited for distributed architectures and resource-constrained devices. In this model, each capability serves as a token that represents a specific permission or privilege. These tokens act as keys that hold assigned privileges for their respective holders. When a requester intends to perform an action associated with a token, they need to send both the request and the token to the resource provider. In this scenario provider only needs to verify the validity of the token, ensuring that it is authentic and grants the necessary permissions.

Capability-based access control offers a more detailed and adaptable method of access control, as access decisions depend on possessing specific capabilities rather than relying solely on user identities or attributes. The primary elements of Capability-based Access Control (CapBAC) consist of:

- **Capabilities:** They are tokens or objects that symbolize specific permissions or privileges. They act as evidence of authorization and are linked to particular resources or actions. Capabilities can be possessed, shared, delegated, and revoked.
- **Subjects:** Subjects are entities or users who aim to access resources. They may hold capabilities that provide them with specific access rights.
- Objects: Objects denote the resources or entities that necessitate protection. They can encompass files, data, devices, or any other resource that requires access control.
- **Access Control Lists (ACLs):** ACLs are data structures that link subjects with their associated capabilities and the objects they can access. These lists establish the connections between subjects, objects, and capabilities.
- **Access Control Policies:** Access control policies dictate the criteria for granting or denying access based on the possession of valid capabilities. These policies establish the rules and conditions for making access control decisions.
- **Capability Management:** Capability management encompasses the creation, issuance, distribution, and revocation of capabilities. It ensures the secure generation of capabilities, restricts their sharing to authorized entities, and ensures proper management throughout their lifecycle.
- **Enforcement Mechanism:** The enforcement mechanism is tasked with assessing access requests, validating the possession of valid capabilities, and enforcing access control policies.
-

These components collaborate to establish a capability-based access control system, offering a flexible and detailed approach to access authorization and control. In recent studies, there has been a notable focus on exploring the potential synergies between blockchain technology and CapBAC.

The authors of [4] presented a CapBAC (Capability-Based Access Control) scheme that utilizes the Bitcoin blockchain as its foundation. Within this scheme, capability tokens are stored in Bitcoin transactions, and each token represents the access rights assigned to a specific subject for one or more objects. By leveraging the inherent transaction functionality of Bitcoin, the scheme enables the secure storage and transfer of capability tokens, facilitating controlled access to objects based on the possession of these tokens.

Just like the transfer of coins, the CapBAC scheme allows for the transfer of capability tokens between subjects through transactions. In the context of accessing an object, the subject provides its token to the object's owner as a means of demonstrating its possession of the necessary access rights. This mechanism serves as proof that the subject is authorized to access the object, similar to how the transfer of physical tokens can grant permission or access to certain resources.

The CapChain [35] approach represents access control as a sequence of capability delegations. Users have the ability to create and manage their own chains of delegations, with the option to assign an expiration time for each delegation. Furthermore, users can receive or delegate capabilities from different domains using a single account. By utilizing the depth value, the owner of the chain can monitor subsequent transactions and observe which users have been granted access rights. However, it should be noted that controlling the length of the chain is only feasible

when a user denies permission grant, as there are no predefined restrictions in place.

BlendCAC [36] is a system that enables hierarchical and multi-hop delegation in access control. It leverages smart contracts on a blockchain protocol to create a mechanism for authorizing and revoking delegates using a token management strategy. When a service request is initiated, the user's token status is verified within the smart contract. BlendCAC also considers context-aware conditions that the user token must satisfy to ensure proper access control.

In Nakamura et al. [37] scheme, a smart contract is created for each object to store and manage the capability tokens (i.e., data structures recording granted access rights) assigned to the related subjects, and also to verify the ownership and validity of the tokens for access control. Different from previous schemes which manage the tokens in units of subjects, i.e., one token per subject, our scheme manages the tokens in units of access rights or actions, i.e., one token per action. Authors clained that the experimental results outperform the BlendCAC scheme in terms of the flexibility, granularity, and consistency of capability delegation at almost the same monetary cost.

The DCACI (Decentralized Capability-Based Access Control) [38] framework introduces a decentralized approach to access control, ensuring privacy and integrity of Capability tokens through the use of Masked Authenticated Messaging (MAM) technology. This framework empowers device owners and users to Grant, Update, Delegate, and Revoke capability tokens. A proof-of-concept implementation of the DCACI framework has been deployed on a resource-constrained machine. Unlike BlendCAC [36], the DCACI framework does not require any prior registration of objects or identities before issuing capability tokens. In addition, unlike Fair Access, DCACI supports delegation and revocation of capability tokens, providing comprehensive privacy and integrity protection.

E) Blockchain Based Access Control (Blockchain BAC):

Blockchain-based access control involves using blockchain technology to strengthen access control mechanisms by leveraging the decentralized and immutable characteristics of blockchain. Its purpose is to enhance security, transparency, and accountability in managing access to resources and sensitive data. The main components found in blockchain-based access control:

- **Blockchain:** Acts as a foundational distributed ledger technology, forms the basis of the access control system by maintaining a decentralized and immutable record of access control-related transactions and events. It ensures the secure and transparent storage of information pertaining to access control within the system.
- **Smart Contracts:** Smart contracts, residing on the blockchain, are code-based self-executing contracts that enforce access control rules and conditions, facilitating automated and tamper-proof execution of access control policies.
- **Identity Management:** These mechanisms validate and manage the identities of users and entities involved in the access control system, ensuring that access requests are linked to authorized and legitimate individuals or entities.

- **Access Control Policies:** These policies consist of predefined criteria and rules that govern the granting or denial of access. These policies, often defined within smart contracts, encompass user attributes, roles, permissions, and contextual information, shaping the access control decision-making process.
- **Consensus Mechanism:** Algorithms or mechanisms employed to attain agreement among distributed nodes within a blockchain network. These mechanisms guarantee that access control decisions are collectively acknowledged by network participants, safeguarding against unauthorized alterations to the access control records.
- **Encryption and Digital Signatures:** Protect access control-related data and ensure the authenticity and integrity of transactions. Encryption safeguards sensitive information, while digital signatures offer evidence of the origin and integrity of access requests and control decisions.
- **Auditing and Monitoring:** Utilized to track access control events and generate audit logs. These logs encompass details such as access requests, permission grants, revocations, and other access control-related activities, ensuring transparency and accountability within the system

Through the integration of these components, blockchain-based access control systems offer heightened security, transparency, and efficiency in managing access to resources and sensitive data. Each component plays a vital role in enforcing access control policies and upholding system integrity.

Xue et al. [39] introduced a access control model for smart homes based on private blockchain to prevent unauthorized access. The model involves an online administrator server responsible for managing policies and user verification. When a visitor is granted a token by the administrator, resource-constrained IoT devices provide the requested data. By utilizing a private blockchain, access records are securely stored, reducing redundant computations and incorporating the security benefits of blockchain. The blockgen algorithm validates visitor credentials with the administrator, and private information is stored on the blockchain.

In their work, Maesa et al. [40] expanded upon the implementation of a blockchain-based access control system by storing subject attributes and access control policies in a smart contract. This approach ensures both the policies and the attributes required for policy evaluation are auditable on the blockchain. However, attribute values cannot be directly edited and necessitate a new transaction on the attributes blockchain, leading to increased encryption computations. They also conducted experiments to measure the time performance of the system in both laboratory and real-world Ethereum environments, considering a scenario where resources are protected by smart contracts.

Authors in [41] addressed the challenges of high latency in the consensus process and limited adaptability to dynamic changes in the network environment in blockchain-based access control. They introduced a framework that consists of three types of chaincodes: Policy Management Chaincode (PMC), Access Control Chaincode (ACC), and Credit Evaluation Chaincode (CEC). The PMC and ACC are deployed on the same data channel, facilitating the management of access control policies and authorization of access.

Blockchain-based permission token segmentation scheme [42] involves splitting permission tokens into smaller parts to generate new tokens. The key idea is to map permissions to tokens, which simplifies permission management in a distributed environment by enabling token transfer between users.

Combining blockchain with searchable access to present a dynamic verifiable ciphertext retrieval scheme [43]. This scheme not only enables efficient searching of encrypted data but also supports forward and backward security. By leveraging blockchain technology, their approach enhances the security and verifiability of ciphertext retrieval while allowing for dynamic updates to the system.

Decentralized blockchain-based marketplace for medical data, where sellers utilize smart contracts to exchange their records with buyers [44]. In this marketplace, sellers can enforce access control on encrypted records without disclosing any sensitive information. Additionally, the system allows for the verification of record correctness, ensuring the integrity and reliability of the shared medical data.

To address the challenges of data storage, sharing, and ensuring data privacy and access authorization in the cloud, this study [45] presents a blockchain-based scheme for cloud data access authorization updates with keyword retrieval capabilities. Firstly, by employing separate ciphertext storage, the risk of collusion attacks is significantly reduced. Secondly, through the method of splitting and managing proxy re-encryption key parameters, the scheme achieves deterministic authority updates, requiring key parameter management updates only when access authority changes. This approach enhances data security and facilitates efficient authorization updates in cloud environments.

In order to address the limitations of fine-grained access control, a Multi-layer Access Control mechanism called BMAC [46] is introduced, leveraging blockchain technology. This mechanism assigns a security level to each resource data and utilizes an InfoMap algorithm to establish credibility-based user grouping. Furthermore, a multi-blockchain structure is designed, enabling the establishment of a flexible and fine-grained trusted data access control mechanism. This approach enhances the control and security of data access while leveraging the benefits of blockchain technology.

Authors in [47] employ Blockchain technology to generate and manage access tokens that represent subject access rights for specific resources. They introduce two novel transaction types: Policy Creation Transaction (PCT) and Right Transfer Transaction (RTT). The PCT is initiated by the resource owner to generate and transfer an access token when the subject attributes meet the access policies. Access decisions are made through the interaction between the resource owner and an external authorization system that stores access policies and user attributes for evaluating access requests. The RTT is utilized when the access token is passed from the current subject to another, facilitating controlled access transfers.

Model in [48], the links to access the documents are stored on the blockchain, ensuring tamper-proof and transparent access control. Initially, the data owner uploads the encrypted documents to the cloud. These documents are encrypted using the HABSE encryption technique, providing an additional layer of security. To decrypt the documents, authorized users can utilize the aggregate key provided by the data owner. This approach ensures secure and controlled access to the stored data in the cloud.

V. COMPARATIVE ANALYSIS AND DISCUSSION

Selecting the optimal access control model relies on several factors, encompassing an organization's specific requirements, contextual considerations, and security objectives. For example, RBAC proves to be a suitable choice

when access control based on predefined roles suffices, while ABAC demonstrates effectiveness in enabling dynamic access control with contextual awareness.

On the other hand, ABE emerges as beneficial for ensuring secure data sharing among authorized entities. When it comes to decentralized and fine-grained access control, Capability access control proves to be a fitting choice. Blockchain provides a tamper-proof audit trail, which ensures accountability and fosters trust among users. Additionally, it enables fine-grained access control, allowing for precise control over data and resources.

However, it is essential to conduct a meticulous assessment of your organization's needs and take into account factors such as scalability, complexity, and the specific use case. By thoroughly considering these aspects, you can determine the most suitable access control model that aligns with your requirements.

Within Table I, our objective is to conduct a comparative analysis of access control mechanisms, evaluating their respective merits and drawbacks in order to ascertain their individual strengths and weaknesses.

Access control methods	**Pros**	**Cons**
Role-Based Access Control (RBAC)	• Separation of duties • Promoting accountability • Facilitate audits • Adapting to organizational changes • Comply with regulatory requirements • Scalability • Simplified Administration	• Fine-grained control • Role Explosion • Limited adaptability to dynamic environments • Challenges in managing hierarchical relationships • Potential role explosion • Lack of contextual awareness • Inadequate support for risk-based access control
Attribute-Based Access Control (ABAC)	• Fine-Grained Control • Dynamic Adaptability • Policy Expressiveness • Risk-Based Access Control • Attribute-Based Decision Making • Integration and Interoperability • Temporal and Spatial constraints representation	• Complexity of Implementation • Attribute Management • Attribute Proliferation • Performance Overhead • Privacy Concerns • Lack of standardization
Attribute-Based Encryption Access Control (ABEAC)	• Fine-grained access control • Flexible access policies • Data confidentiality • Privacy-preserving • Compliance and regulatory	• Complex to design, implement, and maintain. • Encryption and decryption computation overhead • Key management is critical

	requirements • Revocation and policy updates • Data sharing and collaboration	• Limited interoperability • Scalability • Based on trust assumptions • Complexity of access policy management
Capability Access Control (CapBAC)	• Fine-grained access control • Decentralized access control • Follows Least privilege principle • Dynamic access management • Simplified access control administration • Support for resource sharing and delegation • Enhanced security and isolation	• User management and administration overhead • Increased complexity for resource sharing • Limited granularity • Complexity of access revocation • Scalability challenges • Complexity of implementation
Blockchain based access control	• Enhanced Security • Transparency • Accountability • Data Integrity • Decentralization • Fine-Grained Access Control • Efficiency and Automation • Trust and Collaboration • Data Privacy • History based audit • Immutability	• Scalability • slower transaction speeds • regulatory compliance • More computational power • Lack of Standards

Table.1 Pros and Cons of Access Control Mechanisms

In addition to the merits and demerits outlined in Table 1, our extensive examination of the integration between blockchain and access control mechanisms has revealed additional contemporary research methods in order to enhance the security of access mechanisms.

The categorization and mappings of these methods across various access control mechanisms in blockchain perspective are presented in Table 2. It provides a comprehensive overview of how they align with different access control features.

AC/ Approach	Dual AC	Key Abuse	privacy	Audit	Cross domain	Dynamic AC	Context Aware	Access delegation	Hiding Polices
ABAC	✔	✔	✘	✘	✘	✔	✔	✔	✔
RBAC	✘	✘	✘	✔	✔	✘	✔	✔	✔
ABE AC	✔	✔	✔	✘	✘	✔	✘	✔	✔
CapBAC	✘	✘	✔	✘	✔	✔	✘	✔	✘
BCBAC	✘	✘	✘	✔	✔	✔	✘	✔	✘

Table.2 Mapping of Access control mechanisms to important features

VI. FUTURE DIRECTIONS AND RESEARCH OPPORTUNITIES

Our future work aims to enhance existing access control mechanisms to ensure improved data security. Based on our comprehensive survey, there remains a significant research gap in the integration of blockchain technology with access control mechanisms. Moving forward, we intend to explore new-generation access control mechanisms, such as UCON (Usage Control), from a blockchain perspective.

VII. CONCLUSION:

Access control mechanisms play a crucial role in ensuring the security and integrity of data and resources. Models such as RBAC, ABAC, ABE, and CapBAC, as well as blockchain-based access control, offer distinct advantages and disadvantages depending on an organization's specific requirements and context. Our comprehensive survey conducted a comparative analysis of integrating blockchain and access control mechanisms. The results indicated that the integration of blockchain technology with access control has immense potential in enhancing security, transparency, and accountability. To determine the most suitable mechanism, careful evaluation is necessary, considering factors such as scalability, complexity, and the specific use case.

REFERENCES:

[1]. Y. Ding et al., "Blockchain-based Access Control Mechanism of Federated Data Sharing System," 2020 IEEE Intl Conf on Parallel & Distributed Processing with Applications, 2020, pp. 277-284, doi: 10.1109/ISPA-BDCloud-SocialCom-SustainCom51426.2020.00060.

[2]. Materializing Block chain technology to maintain digital ledger of land records", ICCII, AISC,volume 1090,SPRINGER NATURE, ISSN 2194- 5365,pp no:201-211,2018, https://doi.org/10.1007/978-981-15-1480-7_16Babu, B.V.S., Babu K.S. (2021).

[3]. The purview of blockchain appositeness in computing paradigms: A survey. Ingénierie des Systèmes d'Information, Vol. 26, No. 1, pp. 33-46. https://doi.org/10.18280/isi.260104

[4]. A. Ouaddah, A. Elkalam, and A. Ouahman, "Fairaccess: A new blockchain-based access control framework for the Internet of Things: Fairaccess: A new access control framework for IoT," Security Commun. Netw., vol. 9, no. 18, pp. 5943–5964, Feb. 2017

[5]. Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, and J. Wan, "Smart contract-based access control for the internet of things," IEEE Internet of Things Journal, vol. 6, no. 2, pp. 1594–1605, 2018.

[6]. J. P. Cruz, Y. Kaji, and N. Yanai, ‘‘RBAC-SC: Role-based access control using smart contract,’’ IEEE Access, vol. 6, pp. 12240–12251, 2018, doi: 10.1109/ACCESS.2018.2812844.

[7]. Uchibeke, Uchi & Schneider, Kevin & H. Kassani, Sara & Deters, Ralph. (2018). Blockchain Access Control Ecosystem for Big Data Security. 1373-1378. 10.1109/Cybermatics_2018.2018.00236.

[8]. F. Sabrina, "Blockchain and Structural Relationship Based Access Control for IoT: A Smart City Use Case," 2019 IEEE 44th LCN, 2019, pp. 137-140

[9]. Z. Wang and L. Chen, "Re-encrypted Data Access Control Scheme Based on Blockchain," 2020 IEEE 6th International Conference on Computer and Communications (ICCC), Chengdu, China, 2020, pp. 1757-1764, doi: 10.1109/ICCC51575.2020.9345281.

[10]. Y. Ding et al., "Blockchain-based Access Control Mechanism of Federated Data Sharing System," 2020 IEEE Intl Conf, pp. 277-284, doi: 10.1109/ISPA-BDCloud-SocialCom-SustainCom51426.2020.00060.

[11]. D. D. F. Maesa, P. Mori, and L. Ricci, ‘‘Blockchain based access control,’’ in Proc. IFIP Int. Conf. Distrib. Appl. Interoperable Syst., in Lecture Notes in Computer Science, vol. 10320. Cham, Switzerland: Springer, 2017, pp. 206–220.

[12]. S. Wang, Y. Zhang, and Y. Zhang, “A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems,” IEEE Access, vol. 6, pp. 38 437–38 450, 2018.

[13]. H. S. G. Pussewalage and V. A. Oleshchuk, “Attribute based access control scheme with controlled access delegation for collaborative ehealth environments,” Journal of Information Security and Applications, vol. 37, pp. 50 – 64, 2017

[14]. C. Dukkipati, Y. Zhang, and L.C.Cheng, “Decentralized, Blockchain based access control framework for the heterogeneous Internet of things,” in Proc. of 3rd Workshop on Attribute Based Access Control, 2018, pp. 61–69.

[15]. D. D. F. Maesa, P. Mori, and L. Ricci, “A blockchain based approach for the definition of auditable access control systems,” Computers & Security, vol. 84, pp. 93 – 119, 2019

[16]. M. A. Islam and S. Madria, "A Permissioned Blockchain Based Access Control System for IOT," 2019, pp. 469-476, doi: 10.1109/Blockchain.2019.00071.

[17]. S. Shafeeq, M. Alam, and A. Khan, ‘‘Privacy aware decentralized access control system,’’ Future Gener. Comput. Syst., vol. 101, pp. 420–433, Dec. 2019.

[18]. Liu, Han & Han, Dezhi & Li, Dun. (2020). Fabric-iot: A Blockchain-Based Access Control System in IoT. IEEE Access. 8. 1-1. 10.1109/ACCESS.2020.2968492.

[19]. S. Sun, R. Du, S. Chen and W. Li, "Blockchain-Based IoT Access Control System: Towards Security, Lightweight, and Cross-Domain," in IEEE Access, vol. 9, pp. 36868-36878, 2021, doi: 10.1109/ACCESS.2021.3059863.

[20]. B. Kim, W. Shin, D. -Y. Hwang and K. -H. Kim, "Attribute-Based Access Control (ABAC) with Decentralized Identifier in the Blockchain-Based Energy Transaction Platform," 2021, ICOIN, 2021, pp. 845-848, doi: 10.1109/ICOIN50884.2021.9333894.

[21]. J. Sun, X. Yao, S. Wang and Y. Wu, "Non-Repudiation Storage and Access Control Scheme of Insurance Data Based on Blockchain in IPFS," in IEEE Access, vol. 8, pp. 155145-155155, 2020, doi: 10.1109/ACCESS.2020.3018816.

[22]. Y. Zhang, D. He, and K.-K. R. Choo, “BaDS: Blockchain-Based Architecture for Data Sharing with ABS and CP-ABE in IoT,” Wirel. Commun. Mob. Comput., vol. 2018, p. 2783658, 2018.

[23]. S. Li, R. Li, Y. Zhang and Y. Huang, "CBI: A Data Access Control System Based on Cloud and Blockchain Integration," 2020 IEEE 22nd International Conference on HPCC; 2020, pp. 715-721, doi: 10.1109/HPCC-SmartCity-DSS50907.2020.00093.

[24]. H. Xu, Q. He, X. Li, B. Jiang and K. Qin, "BDSS-FA: A Blockchain-Based Data Security Sharing Platform with Fine-Grained Access Control," in IEEE Access, vol. 8, pp. 87552-87561, 2020, doi: 10.1109/ACCESS.2020.2992649.

[25]. M. Jemel and A. Serhrouchni, "Decentralized access control mechanism with temporal dimension based on blockchain," in 2017, ICEBE, IEEE, 2017, pp. 177–182.

[26]. W. Yang, Z. Guan, L. Wu, X. Du and M. Guizani, "Secure Data Access Control with Fair Accountability in Smart Grid Data Sharing: An Edge Blockchain Approach," in IEEE Internet of Things Journal, vol. 8, no. 10, pp. 8632-8643, 15 May15, 2021, doi: 10.1109/JIOT.2020.3047640.

[27]. M. Jemel and A. Serhrouchni, "Decentralized Access Control Mechanism with Temporal Dimension Based on Blockchain," 2017, ICEBE,2017, pp. 177-182, doi: 10.1109/ICEBE.2017.35.

[28]. L. Guo, X. Yang, and W.-C. Yau, ''TABE-DAC: Efficient traceable attribute-based encryption scheme with dynamic access control based on blockchain,'' IEEE Access, vol. 9, pp. 8479–8490, 2021, doi: 10.1109/ACCESS.2021.3049549.

[29]. D. Han, J. Chen, L. Zhang, Y. Shen, X. Wang and Y. Gao, "Access control of blockchain based on dual-policy attribute-based encryption," 2020 IEEE 22nd International Conference on High Performance Computing and Communications, 2020, pp. 1282-1290

[30]. Y. Michalevsky and M. Joye, "Decentralized policy-hiding attributebased encryption with receiver privacy," IACR Cryptology ePrint Archive, pp. 1-29, 2018.

[31]. J. Katz, A. Sahai, and B. Waters, "Predicate encryption supporting disjunctions, polynomial equations, and inner products," in Proc. of Annual International Conference on the Theory and Applications of Cryptographic Techniques, 2008, pp. 146-162.

[32]. T. Nishide, K. Yoneyama, and K. Ohta, "Attribute-based encryption with partially hidden encryptor-specified access structures," in Proc. of Applied Cryptography and Network Security, 2008, pp. 111-129

[33]. S. Gao, G. Piao, J. Zhu, X. Ma and J. Ma, "TrustAccess: A Trustworthy Secure Ciphertext-Policy and Attribute Hiding Access Control Scheme Based on Blockchain," in IEEE Transactions on Vehicular Technology, vol. 69, no. 6, pp. 5784-5798, June 2020

[34]. M. Xiao, Q. Huang, Y. Miao, S. Li and W. Susilo, "Blockchain Based Multi-Authority Fine-Grained Access Control System with Flexible Revocation," in IEEE Transactions on Services Computing, vol. 15, no. 6, pp. 3143-3155, 1 Nov.-Dec. 2022

[35]. T. Le and M. W. Mutka, "Capchain: A privacy preserving access control framework based on blockchain for pervasive environments," in IEEE International Conference on Smart Computing (SMARTCOMP). IEEE, 2018, pp. 57–64.

[36]. R. Xu, Y. Chen, E. Blasch, and G. Chen, "Blendcac: A smart contract enabled decentralized capability-based access control mechanism for the IoT," Computers, vol. 7, no. 3, p. 39, 2018.

[37]. Nakamura, Yuta, Yuanyu Zhang, Masahiro Sasabe, and Shoji Kasahara. 2020. "Exploiting Smart Contracts for Capability-Based Access Control in the Internet of Things" Sensors 20, no. 6: 1793. https://doi.org/10.3390/s20061793

[38]. S. K. Pinjala and K. M. Sivalingam, "DCACI: A Decentralized Lightweight Capability Based Access Control Framework using IOTA for Internet of Things," 2019, WF-IoT, 2019, pp. 13-18, doi: 10.1109/WF-IoT.2019.8767356.

[39]. J. Xue, C. Xu, and Y. Zhang, “Private blockchain-based secure access control for smart home systems.” KSII Transactions on Internet & IS, vol. 12, no. 12, 2018.

[40]. D. D. F. Maesa, P. Mori, and L. Ricci, “A blockchain based approach for the definition of auditable access control systems,” Computers & Security, vol. 84, pp. 93–119, 2019.

[41]. Y. Feng, W. Zhang, X. Luo and B. Zhang, "A Consortium Blockchain-Based Access Control Framework with Dynamic Orderer Node Selection for 5G-Enabled Industrial IoT," in IEEE Transactions on Industrial Informatics, vol. 18, no. 4, pp. 2840-2848, April 2022, doi: 10.1109/TII.2021.3078183.

[42]. J. Shi and R. Li, "Permission Token Segmentation Scheme Based on Blockchain Access Control," 2020, TrustCom, 2020, pp. 1956-1964, doi: 10.1109/TrustCom50675.2020.00267.

[43]. C. Jia, Y. Geng and S. Sun, "Research on Data Access Management Based on Blockchain Engine," 2022 International Conference on Big Data, Information and Computer Network (BDICN), Sanya, China, 2022, pp. 465-468, doi: 10.1109/BDICN55575.2022.00091.

[44]. A. Alsharif and M. Nabil, "A Blockchain-based Medical Data Marketplace with Trustless Fair Exchange and Access Control," GLOBECOM 2020 - 2020 IEEE Global Communications Conference, Taipei, Taiwan, 2020, pp. 1-6, doi: 10.1109/GLOBECOM42002.2020.9348192.

[45]. Y. Lei, Z. Jia, Y. Yang, Y. Cheng and J. Fu, "A Cloud Data Access Authorization Update Scheme Based on Blockchain," 2020 3rd International Conference on Smart BlockChain (SmartBlock), Zhengzhou, China, 2020, pp. 33-38, doi: 10.1109/SmartBlock52591.2020.00014.

[46]. Y. Hou, W. Liu, H. Lin and X. Wang, "Multi-layer Access Control Mechanism based on Blockchain for Mobile Edge Computing," 2020 IEEE Intl Conf on Parallel & Distributed Processing with Applications, 2020, pp. 285-291, doi: 10.1109/ISPA-BDCloud-SocialCom-SustainCom51426.2020.00061.

[47]. Maesa, D. D. F., Mori, P., and Ricci, L. Blockchain based access control. In: IFIP International Conference on Distributed Applications and Interoperable Systems. Springer, Cham, 2017. p. 206-220

[48]. S. Desai, O. Deshmukh, R. Shelke, H. Choudhary, S. S. Sambhare and A. Yadav, "Blockchain based Secure Data Storage and Access Control System using Cloud," 2019