Eng Int Syst (2025) 3: 263–273

Engineering
Intelligent Systems

Dynamic Access Control using Blockchain-based Attribute Encryption Scheme for Big Data Cloud Storage

Wei Fu[1,a*], **Lulu Zhang**[2,b] **and Changqun Li**[3,c]

[1] *Department of Information Technology, Anhui Vocational College of Grain Engineering, Hefei 230000, Anhui, China*

As one of the most crucial aspects of cloud computing, cloud storage allows users to overcome a lack of available storage space and speed without having to invest in new devices. Big data refers to a wide range of data characterized by its volume and rate of change. Traditional databases cannot handle the massive amount of information that big data operations generate. Therefore, ideally, the storage and processing of large data should occur on the cloud. However, ensuring privacy and access control is crucial before putting big data on the cloud. This requires encrypting the data and limiting the number of people accessing it. Hence, this study proposes Blockchain-assisted Cohesive Authentication using Attribute-Based Encryption Scheme (BCA-ABES) for dynamic control of access to big data stored in the cloud. The ABE scheme provides less computation overhead in the encryption process and decreases the decryption time required for effective dynamic access control. Organizations may use smart contracts to record their blockchain access control policy and assign appropriate roles to users. The suggested architecture uses smart contracts' access control computation technique to control access to huge data resources in cloud storage. Our suggested approach has been thoroughly tested for security vulnerabilities and shown great computing efficiency, and meets the indistinguishability criteria in theoretical and practical evaluations.

Keywords: Dynamic Access Control, Big Data Analytics, Cloud Computing, Blockchain Technologies, Big Data Cloud Storage.

1. INTRODUCTION

The scalability, open environment, centralization of data processing, and other features inherent to cloud storage pose a unique threat to data and user security because of the dynamic solid nature of extensive data resources, the great diversity of sources, and the characteristics of disseminated management [1]. By storing their information in the cloud, users relinquish the physical possession of their data and put its administration in the hands of a potentially unreliable third party: the cloud service provider (CSP). [2]. Outsourced data in cloud computing faces further risks due to the cloud's lack of security and dependability from the client's perspective [3]. However, because there is no way to keep a local copy of the data, typical integrity verification methods such as data encryptions, signatures, and hash functions are useless in the cloud [4]. However, it is not feasible to download a lot of data at once. When people try to obtain information using mobile devices with limited-capacity, situations worsen [5]. Therefore, what is required is an effective method whereby the authenticity of data stored in the cloud can be verified remotely [6]. The user base for big data is complicated, necessitating specialized access management methods. The cloud is where most big data resides, yet

*Corresponding author. Address for correspondence: Wei Fu, Department of Information Technology, Anhui Vocational College of Grain Engineering, Hefei 230000, Anhui, China. Email: [a]13294958163@163.com, [b]38454391@ qq.com, [c]779352939@qq.com

this lack of control over data processing by users leaves it vulnerable to unauthorized entry [7]. Furthermore, it is difficult for the standard access control model to accommodate the flexible and dynamic requirements of controlling user access to the enormous amounts of data stored in big data clouds [8]. The security issues of massive cloud storage have been addressed by a new proposal facilitated by blockchain technology [9]. The decentralized nature of a blockchain makes it an excellent complement to big data and cloud storage [10]. However, a new challenge has emerged in information security: how to guarantee the security of huge amounts of data stored on the cloud. [11] Therefore, it has become crucial to investigate blockchain-based methods for controlling access to huge amounts of data stored in the cloud [12].

Numerous attribute-based, unique-access control strategies have recently been suggested for cloud storage systems [13]. These encrypt information based on an access structure provided by attributes, and defines a set of attributes to identify users. Therefore, only those users with attributes that conform to the access structure can decode the encrypted data. Based on how attributes relate to ciphertexts and decryption keys, ABE is split into key-policy ABE (KPABE) and ciphertext-policy ABE (CP-ABE). ABE has advantages such as, scalability, high flexibility, and fine-grained access control based on attributes [14]. Recently, it has been extensively applied to secure cloud data storage. It achieves fine-grained access control and can solve the one-to-many encryption and decryption problem in open cloud applications [15]. However, all the aforementioned methods for managing encrypted data access do not take into account the broader issue of duplicate data storage in cloud computing, particularly regarding encrypted data across a wide range of data storage conditions [16]. For massive data that has to be stored securely on the cloud, this is a real problem as these approaches presuppose that user credentials are issued by a centralized body. Since multiple organizations issue user characteristics in clouds, this assumption may not work for many use cases [17].

2. LITERATURE SURVEY

Liu et al. [18] suggested the Fabric IoT for the access control systems in IoT, which is based on the attribute-based access control (ABAC) and Hyperledger Fabric blockchain frameworks. This system has three distinct smart contract categories: Policy Contracts (PC), Device Contracts (DC), and Access contracts (AC). DC allows users to save and query the locations of device-generated data resources. Admins may make use of PC features designed to administer ABAC rules. Regarding typical users, AC is the fundamental program for implementing an access control approach. Fabric-iot enables distributed, granular, and dynamic IoT access control management using ABAC and blockchain technologies. The effectiveness of this approach was tested using two sets of simulations. Fabric-IoT can effectively achieve agreement in a distributed system to guarantee data consistency while maintaining high throughput in a high-volume request scenario.

Tan et al. [19] proposed the Blockchain-empowered Green Smart Device Access Control Framework (BGSD-ACF). Users and Green Smart Devices (GSD) are first given a visual identity (VID) based on the decentralized identifiers (DIDs) standard developed by the World Wide Web Consortium (W3C). Then, the researchers added to the GSD-DIDs protocols a support for the authentication of devices and users. Finally, unified access control systems for GSD were built based on the blockchain's decentralized and non-tamperable qualities. This system encompasses the granting, registration, and revocation of access privileges. The aresearchers code through their paces on the Raspberry Pi hardware and the FISCO-BCOS alliance testbed. The results demonstrate the framework's viability and consistency in assisting users to attain their goals of lightweight, decentralized, fine-grained access management of GSDs.

Li et al. [20] recommended Blockchain-based Public Auditing (BPA) for big data in cloud storage. The proposed method differs from prior aooroaches in that it requires only two specified entities (the cloud service provider and data owner) and eliminates the need for a third-party auditor for data auditing. To decrease the demand on computers and networks while verifying data integrity, data owners may use hashtags to store lightweight verification tags on the blockchain and create evidence by constructing a Merkle Hash Tree. Additionally, the hashtag of each data block is used to construct the Merkle Hash Tree for data integrity verification, which means that, in theory, this approach can attain 100% auditing confidence. The security research demonstrates that the suggested technique can resist 51% of attacks and malicious actors. The experimental findings show some improvement in computational and communicative capabilities.

Saini et al. [21] discussed the Smart-Contract-based Access Control Frameworks (SCACF) for cloud-intelligent healthcare systems for the safe sharing of electronic medical records (EMR). The authors suggest four categories of smart contracts: user verification, access authorization, behaviour detection, and revocation of access. Given the block size of the ledger and the massive amount of patient information, this architecture employs the cryptographic functions of the Edwards-curve digital signature algorithm (EdDSA) and elliptic curve cryptography (ECC) to encrypt EMR before they are stored in the cloud. At the same time, their corresponding hashes are packed into the blockchain. The researchers deployed a private Ethereum network to evaluate the performance of the proposed access control framework in a real-time intelligent healthcare environment.

Bhaskara et al. [22] discussed the Blockchain-based Distributed Data Storage System (BDDSS) for Privacy and Security Guaranteed Internet of Medical Things (IoMT) with Efficient Access Control. for the security of the proposed systems is strengthened by adding decentralized Selective Ring-based Access Control (SRAC) mechanisms, device authentications, and patient records anonymization methods. The researchers tested the suggested blockchain-based system for latency and cost efficiency in data exchange. They performed a logical system analysis, finding that the security and privacy procedures based on the design can meet the requirements of distributed IoMT smart healthcare system. The statistical results show that the fortified-chain-

based healthcare cyber-physical System offers decentralized automated access control, privacy, and security while only necessitating a small fraction of the storage space and having a response period on the order of milliseconds compared to conventional centralized healthcare cyber-physical systems.

Shi et al. [23] introduced the Privacy Protection Method (PPM) for the management of healthcare big data based on risk access controls. This paper addresses the issue of inaccuracy in experimental results caused by a lack of real data when dealing with actual problems by first identifying the key indicators distressing the privacy disclosure of big data in healthcare and then establishing risk access control models based on the fuzzy theory, which has been utilized for the big data management in smart medical treatment. Finally, the Matlab fuzzy tool set is used to evaluate the model's predictions. Results show that the model can accurately forecast a wide variety of risks with an accuracy of more than 90%, proving its usefulness in determining present-day security concerns.

Qin et al. [24] offered Lightweight Blockchain-based Access Control Schemes (LBACS) for IoT. The author believes that cloud services cannot be trusted and assures that blockchain-based proxy re-encryption calculations are accurate. It is important to encourage users to seek authorization through the blockchain and log their access activity there. In this research, the authors presented a user credibility incentive mechanism that uses a reputation score based on the operator's access behaviour to dynamically modify the endorsement protocol. Security analysis and experimental findings validate the robustness and effectiveness of the suggested approach.

Pallavi and Kumar [25] offered Authentication-based Access Control and Data Exchanging Mechanisms (AAC-DEM) for IoT Devices in Fog Computing Environments. An authentication mechanism based on fog nodes is proposed in this work for managing IoT devices securely without the need for a central authority. The suggested authentication technique exploited the advantages of using fog nodes for the authentication mechanism, obviating the need to rely on a third party. This strategy efficiently addressed the storage system's single point of failure while providing other advantages, such as higher throughput and lower costs. The suggested authentication strategy utilizing a fog node outperformed the alternatives in terms of memory consumption (4009.083 KB), processing time (76.915 s), and packet delivery ratio (PDR) (76).

Joshi et al. [26] discussed the Unified Authentication and Access Control (UA-AC) for a mobile communication-based lightweight IoT system utilizing blockchain. The method is based on fog data systems and the concept of blockchain systems; testing results reveal that the proposed mechanism outperforms similar blockchain-based verification systems. The authentication and verification process is carried out using the blockchain method. This approach leverages the benefits of blockchain technology to provide secure authentication mechanisms. The method, structure, and layout the authors propose for using blockchains ensure tamper-proof data while simultaneously facilitating transparency, consistency, and provenance. The article describes the overall architecture of the system, as well as the scenario analysis and implementation that was performed using the prototype system. An encrypted prototype that uses a secure protocol for transmitting data while maintaining a low rate of errors is part of the authentication process.

Kesarwani and Khilar [27] proposed the Mamdani fuzzy method fuzzy C-means clustering (MDM-FCM) for Trust-Based Access Control Models in cloud computing. The author employs a Mamdani fuzzy method to achieve fuzzification with a Gauss membership function and defuzzification with a triangle function. Trust in the resource is determined by considering factors like its performance and adaptability. Workload and reaction time are used as metrics to evaluate performance. Elasticity was determined by factoring in the four characteristics of scalability, availability, security, and user-friendliness. The author employs inaccurate, fake, unapproved, and total requests as trust evaluation factors and applies fuzzy C-means clustering to aggregate. The trust evaluation results are accurate compared to other existing models.

Figueroa-Lorenzo et al. [28] suggested the Performance Analysis based Methodological Framework (PA-MF) for Industrial IoT (IIoT) access control systems based on a permissioned blockchain. To execute the registration stage of access control systems, this research recommends a unique method for dependable data privacy based on a private data-gathering solution proposed by Hyperledger Fabric. This demonstrates the viability of a private data local management system that relies on private data collecting. Finally, the modularity encouraged by Hyperledger Fabric Blockchain enables the best network architectures to be created for the application. The researchers carried out multiple experiments to prove the effectiveness of these strategies using a defined methodological performance framework.

Atlam and Wills et al. [29] recommended Effective Security Risk Estimation Techniques based Fuzzy Inference System (ESRET-FIS) for Access Control Model for IoT. The suggested risk estimate method was validated by interviewing 20 IoT security experts from the UK and elsewhere, and the fuzzy inference rules were built with the utmost precision. The suggested risk estimate method was constructed and tested in simulated network router access control situations. The suggested method is more accurate and realistic than the currently available fuzzy methods in assessing the risks caused by access control procedures in the IoT environment. The simulation findings validate the accuracy, correctness, and realism of the suggested risk assessment method for assessing risks to the security of access control processes.

Chinnasamy et al. [30] presented the Blockchain-based Access Control and Data Sharing System (BAC-DSS) for IoT smart devices. The suggested framework for controlling access to IoT networks is meant to address issues with security and authentication. The system aims to provide secure data transfer via IoT networks employing authentication and encryption. The authors developed a combination of smart contracts, an access control contract, an authentication contract, and a judgment contract to allow effective management of user authorization. Finally, the efficiency of the suggested method was evaluated by comparing it to the cost identification attached to various forms of cryptography and

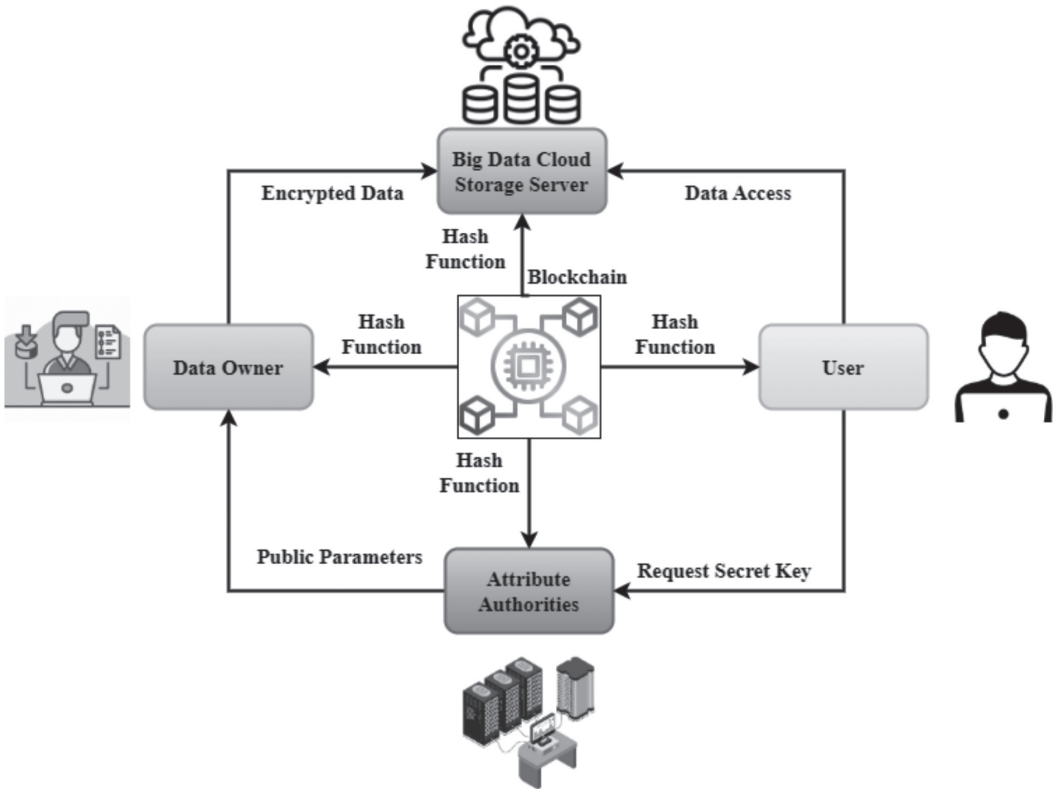

Figure 1 System model.

smart contracts. To further prove the cost-effectiveness of the suggested method, it was compared to other existing methods and shown to be more cost-efficient overall.

Ghaffari et al. [31] introduced the Novel Access Control Method Through Smart Contract (NACM-SC) for Internet-Based Service Provisioning. Blockchain is a technology that paves the way for new forms of dispersed access control and novel business models. The authors proposed an attribute-based access control method for equitably distributing resources among networks and service providers via blockchain. The solution meets the parties' needs while providing dependability, accountability, and immutability. In addition, the lower total cost of the service is to everyone's advantage. As a result, service providers can outsource their access control processes without including a neutral party. The results of trials indicated that the proposed approach can serve as a quick, complete, and scalable access control mechanism.

3. BLOCKCHAIN WITH ATTRIBUTE-BASED ENCRYPTION SCHEME (BABES)

Cloud storage is a method of storing information that uses virtualization and disperses data storage over a network of computers [32]. It facilitates cooperation between servers or data centres, enabling them to easily share and access resources. To use the features of any application at any time, users must first upload their data to the cloud. Cloud computing has several advantages, including portability, automated software updates, resilience to emergencies, low operational costs, to name a few [33]. To use the features of any application at any time, users must first upload their data to the cloud. Since users' data may be compromised while stored in the cloud, protecting users' privacy and security is crucial. Meantime, there is growing public concern about user privacy, which has a significant impact on cloud storage security. On-demand storage of enormous amounts of data is a possibility with big data cloud storage. However, it faces severe data security concerns because of its dynamic and diverse environment. Attribute-based encryption (ABE) was recently created as a basic cryptographic to provide granular control over who may see encrypted data. Access rights and data security policies are determined by the properties of the system in ABE. Therefore, ABE appears to be a useful tool for keeping information secure in cloud computing environments. However, there are limits to the efficiency and scalability of current ABE schemes when it comes to crucial activities in cloud storage environments, such as the revocation of access advantages, key updating, and revocation. Blockchain-assisted Cohesive Authentication using Attribute-Based Encryption Scheme (BCA-ABES) has been proposed for dynamic access control in big data cloud storage.

3.1 System Model

Figure 1 shows the system model.

Blockchain

Blockchain uses a transparent, immutable framework to store users' basic information. Therefore, the suggested architecture ensures non-tamperable and transparent data flow

between its users. The blockchain network guarantees access control and revocation capability using various smart contract features, including encryption, key generation, re-encryption, key update, and decryption.

Attribute Authority

The attribute authority in our concept is the hub of trust and is responsible for producing attribute key shares, disseminating public parameters for the system, and guarding the master secret key.

Cloud storage

Files uploaded to cloud storage by data owners are encrypted before storage. This controls access to stored data and provides associated services.

Cloud Storage Provider

The proxy server used by the cloud storage provider is a semi-trusted third party. Data owners' ciphertexts are re-encrypted by it before being sent to users.

Data Owner

Before sending data to a cloud storage provider, owners should take safeguarding measures such as encrypting files and creating access controls.

Users

Users are not trusted parties; hence, the data cannot be decrypted unless its features satisfy those specified in the policy. Every communication channel must be encrypted in order to send and receive data securely.

3.2 Preliminaries

First, this paper gives a brief explanation of bilinear pairing, which is the main building block of our concrete scheme. Then, the framework of the key aggregate cryptosystem is introduced.

Let H and H_T be two multiplicative cyclic group of prime orders q. Let h be an initiator of H. A bilinear pairing $\widehat{e}\ H \times H \rightarrow H_T$ is a map with the subsequent elements:

Bilinear: $\forall h_1, h_2 \in H$ and $\forall b, a \in Z$, therefore $\widehat{e}\left(h_1^b, h_1^a\right) = \widehat{e}(h_1, h_2)^{ba}$

Non-degenerate: $\widehat{e}\,(h_1, h_2) \neq 1$

Computable: $\forall h_1, h_2 \in H$, there is an effective algorithm for calculating $\widehat{e}\,(h_1, h_2)$

The group H is called a bilinear group. Many classes of elliptic curves feature bilinear groups.

Global Setup: The credible attribute authorization centre performs system setup algorithms. This is a group of generation algorithms that outputs a tuple $(M = q_1 q_2 q_3, H, H_T, \widehat{e}\,)$. Attribute authorization first chooses security parameters λ and runs algorithms $\Phi(\lambda)$ to determine the system variables $(M = q_1 q_2 q_3, H_0, H_T, \widehat{e}\,)$, where H_0 and H_T are two cyclic group of orders M, and q_1, q_2, and q_3 are three dissimilar prime number. H_{q_1}, H_{q_2}, and $H_{q_3}$are three subgroup from H_0, whose initiators are h_1, h_2, and h_3 correspondingly. This study assumes that $\{V = at_1, at_2, \ldots, at_m\}$ is system attribute sets, and $W_1 = \{u_j, 1, u_j, 2, \ldots, u_j, i\}$ is value sets of attributes at_j. For every attribute at_j in systems, attribute authorization produces public keys ql and master keys msl in line with the subsequent stages:

Attribute authorization selects two hash functions in cryptography G: $\{0, 1\}^* \longrightarrow Z_M$ and G_0: $H_0 \longrightarrow Z_M^*$, which are anti-collision.

For every attribute at_jin the system, attribute authorization arbitrarily chooses $y_j, i \in Z_M^*$ and $P_j, i \in H_{q_3}$ and calculates $B_j, i = h^1/y_j, i_1$ where $j \in (1, 2, \ldots m), i \in (1, 2, \ldots .m_j)$.

Attribute authorization randomly chooses $\alpha_0, \alpha \in Z_M^*$ and $P_0 \in H_{q_3}$ aφnd then calculates $X_0 = e(h_1, h_1)_0^{\alpha}andX = e(h_1, h_1)^{\alpha}$.

Attribute authorization describes key distribution functions KF that map session keys to a stream of bits of length κ and two variables ω and β that belong to H_{q_3}.

Attribute authorization publishes the public key $pl = (B_0, h_3, B_j, i\_1 \leq j \leq m, 1 \leq i \leq m_j, X_0, X, KF, \omega, \beta, \kappa, G, G_0)$ and keeps the master private key $msl = (h_1, y_j, i\_1 \leq j \leq m, 1 \leq i \leq m_j, \alpha_0, \alpha)$ secretly.

Key Generation: According to the attribute list of the data access layer, attribute authorization randomly chooses $\lambda_j \in Z_M^*$ for any attribute $j(1 \leq j \leq k)$ and calculates $K_0 = h_0^{\alpha} - \sum_j^k = 1\lambda_{j_1}, K = h^{\alpha} - \sum_j^k = 1\lambda_{j_1}$, and $K_j = h_j^{\lambda}, y_j, i_1$. Then attribute authorization sends the generated private key attribute authorization to the data access layer. Algorithm 1 shows the key generation steps.

Verification Component Generation: To build and upload verification components, the data owner must perform the abovementioned steps. With the help of the attribute authorization's predefined key distribution mechanism, the data owner randomly chooses $w \in Z_M$ and a session key. The owner of the information performs the computations and then transfers them to the distributed ledger.

Data Encryption: The data owner determines the secret value by making it the value of the access tree's parent node. Then, in this study, the leaf nodes are made read-only. All children of nodes other than leaf nodes have an unread status. In the future, the data owner will recursively process all unread nodes. If the non-leaf node uses a threshold value to represent the threshold, the data owner will randomly choose a polynomial degree. Meanwhile, the polynomial is satisfied, and the value is assigned to the child node.

Decryption: The operating system of the outsourced server will carry it out. Two distinct phases make up the algorithm: attribute detection and decryption. The private key's attribute values that do not conform to the access policy will be automatically eliminated during the attribute detection phase. This architecture may avoid the computationally expensive process of bottom-up recursive decryption. For the algorithm to go on to the decryption stage, it must first pass the attribute verification.

Figure 2 shows the proposed BCA-ABES model. The system enables finer control over data access by allowing the owner to reveal secret keys to data users, and encrypt shared data following the policy. A blockchain-based personal data management system has been developed to enable data owners to take responsibility for their information and ensure its confidentiality. An access control framework can authenticate users and protect data privacy in the cloud, and ABE data encryption storage can be carried out after the authentication. The proposed solution includes an attribute-based encryption-based smart contract framework, data storage in untrusted storage, and a blockchain-based

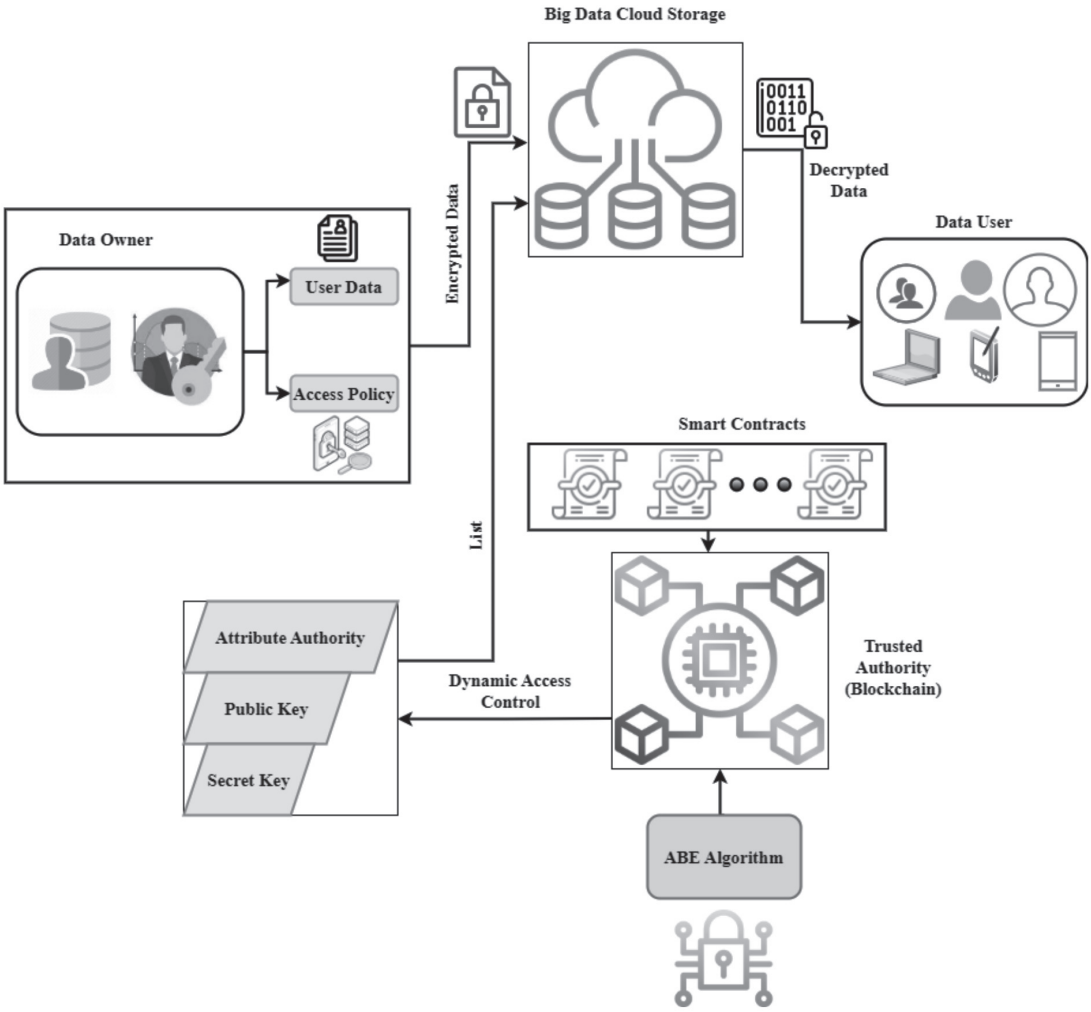

Figure 2 Proposed BCA-ABES model.

transactional access control mechanism. The event logs is the only way to learn the result of the nonconstant function in the smart contract. Consequently, under the aforementioned data-sharing acceptance, the search function's results are only accessible through events. A data user initiated the contract's deployment. The contract's search feature was used, and the data user stored the results. This issue is resolved since only the data user can access the search results. Domain-based Dynamic Access Control allows administrators to set rights and limitations for users to access resources according to predetermined criteria, such as the importance of the data being accessed, the user's task or position, and the parameters of the device.

Figure 3 shows the sequence diagram of the proposed BCA-ABES model. This scheme's implementation comprises a four-stage process: system initialization; encryption key generation; encryption; and decryption.

Certificate Authority

To enable cross-domain attribute management, the certificate authority assigns multiple attribute authority and thresholds to each attribute by invoking the attribute management contract.

Attribute Authority

Attribute authorities partition public attribute keys off-chain, and the public attribute key generation contract reassembles those keys on-chain. The data user is accountable for the data user setup.

Blockchain

Each node in the Ethereum network is responsible for keeping the blockchain's hash chain relationship consistent. As a result, our model's access policy cannot be altered, and data owners may benefit from the granularity and flexibility of dynamic access control due to the blockchain.

Data Owners

In the suggested paradigm, the data owner controls who has access to their information. The resource's owner determines who can use it based on the encryption policy.

Cloud Service Providers

The cloud service provider is accountable for the outsourced information decryption, and the data owner confirms the outsourced decryption outcomes and executes the last decryption.

Algorithm 1: Key Generation Algorithm

Input: Public Key PK, Master Secret Key (MSK), Group Secret Key θ_n and Attribute set $S = \{b_1, b_2, \ldots b_m\}$
Output: User Secret Key SK

1. Determine the group's secret key θ_n linked with the user and compute $K = h^{\frac{\beta+\theta_n}{\alpha_1}}$
2. Random Select $r \in Z_q^*$ for the user and compute $E = h^{\frac{\theta_n+r}{\alpha_2}}$
3. **For** each attribute $b_j \in W$ **do**
4. **Compute** $K_i = h^{\beta} h^{G(b_i)}$
5. **End for**
6. **Return**

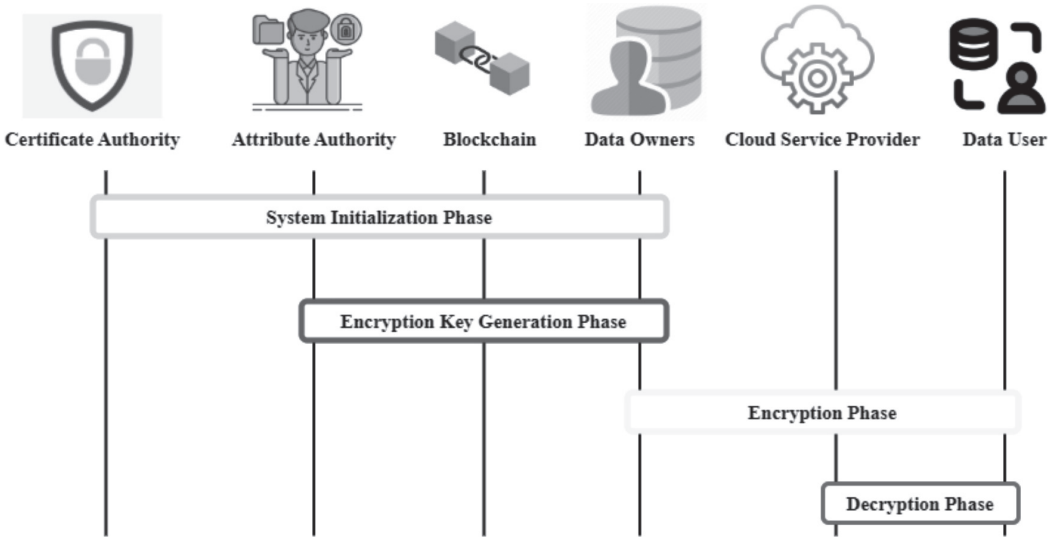

Figure 3 Sequence diagram of proposed BCA-ABES model.

Data Users

In regard to dynamic access control, the data of the user whose attributes comply with the access policy is decrypted so they can download it. The data owner has dynamic access control of the data, and the proposed approach supports attribute-level cancellation without disturbing other users during the collected of the required data by the individual user. Finally, Dynamic Access Control permits the administrator to effortlessly apply auditing and handle access to domain-based data authentication servers. Compared to other existing models, the suggested BCA-ABES system enhances the data access control accuracy and reduces the computational cost, communication complexity and amount of storage overhead.

4. RESULTS AND DISCUSSION

This study presents the Blockchain-assisted Cohesive Authentication using Attribute-Based Encryption Scheme (BCA-ABES) for data dynamic access control in big data cloud storage. The experiment platform consists of a server with a CPU speed of operation of 2.6 GHz, the TensorFlow 1.8.0 network framework, and Python 3.5.2. Information on the precise conditions of the experiment. The simulation experiment design comprises the experimental environment and parameter settings above. To guarantee the reliability of the experimental findings and maintain the consistency of the other experimental settings, MATLAB software is utilized to compute and quantify the experimental results. The performance of the suggested BCA-ABES model is examined based on metrics such as data access control accuracy, computational cost, communication complexity and storage overhead ratio compared to other existing methods.

(i) Data Access Control Accuracy Ratio

Prediction accuracy is substantially similar between the blockchain-based process for controlling early access to large data and the Hadoop-based strategy that uses data sensitivity as its foundation. However, as the number of cycles frequency increases, so does the difference in control accuracy between the two classic approaches. While the conventional approach may have increased control precision, the control technique presented in this study has more control accuracy, which may effectively increase the system's data storage capability. The approach in this study pre-processes the information before executing data access control, increasing access control accuracy while maintaining control efficiency. Figure 4 shows the data access control accuracy ratio.

(ii) Computational Cost Ratio

Data auditing methods, in their roles as verifier and prover, impose varying computational costs on every participant involved. In contrast to the server's computation cost, which reflects the resources needed to calculate a proof for a block, the client's computation cost denotes the resources used by

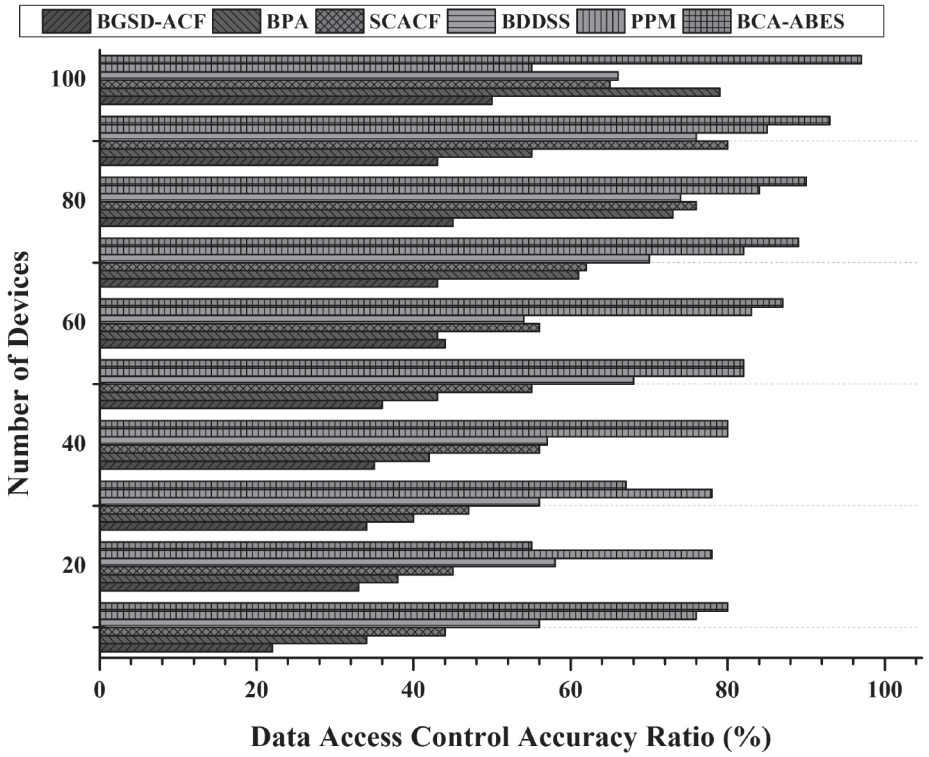

Figure 4 Data access control accuracy ratio.

the client to compute the tags, produce the challenge, and validate the proof message. Because of the prevalence of situations in which numerous shared data sets are encrypted using the same embedded sub-policies, this research devises an efficient approach to enhance the effectiveness of attribute-based data access control in such settings. In particular, when decrypting a file for the first time, the result is saved together with the policy used to decrypt it. This result is known as the 'same policy parameter', and it can be utilized to significantly decrease the computation cost of subsequent decryption activities for additional files embedded with the same policy. Figure 5 presents the various computational costs.

(iii) Communication Complexity Ratio

Communication complexity has emerged in studies of computer-to-computer communication's efficacy and inherent complexity. This model investigates issues for the communication requirements of computations and aims to provide upper and lower limits on the amount of communication needed between processors to solve these problems. The size of the auditor's challenge message delivered to the authority and the size of the authority proof message received by the verifier are components of the complex communication between the server and the auditor. Transactions in a blockchain may be validated by inspecting the associated hash tree. At the user's option, the level of communication complexity may be set rather low. By facilitating a distributed cloud-based communication network, blockchain technology enables the development of seamless connections between software programs. As a result, communication is simplified significantly. Figure 6 shows the communication complexity ratio.

(iv) Storage Overhead Ratio

In this study, as part of the authorization procedure, the storage overhead of the initial configuration file is calculated, as well as the features and session keys. The access policy, identifier, IP address, group identifier, and keys should all be stored in a configuration file on the device. The fixed-access policy configuration file for 12 nodes is simply 1082 bytes in size. Private and public keys associated with these protocols are collected. In regard to protocol storage, private keys are used by one set of users. According to the data, the storage cost is not greatly affected by the number of participants; however, it does increase rapidly when the size of an attribute increases. The proposed technique has three stages: initialization, registration encryption, and uploading. The storage overhead for the initialization phase is 5 kb at 25 attributes; for the registration phase, it is is 9 kb at 25 attributes; for the . encryption and uploading stage, it is 8 kb at 25 attributes. Figure 7 shows the storage overheads.

5. CONCLUSION

This study presents Blockchain-assisted Cohesive Authentication using the Attribute-Based Encryption Scheme (BCA-ABES) for dynamic access control of big data stored in the cloud. Our approach ensures the confidentiality of such data by employing a robust security mechanism. Data sent via a public channel can be viewed only by those with the proper

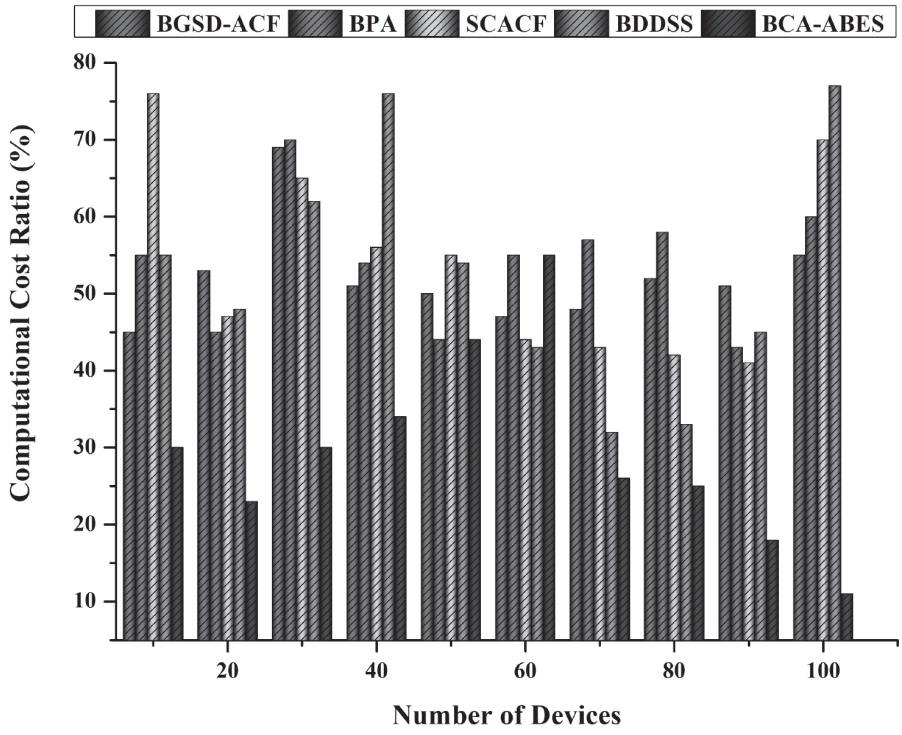

Figure 5 Percentages for computation cost.

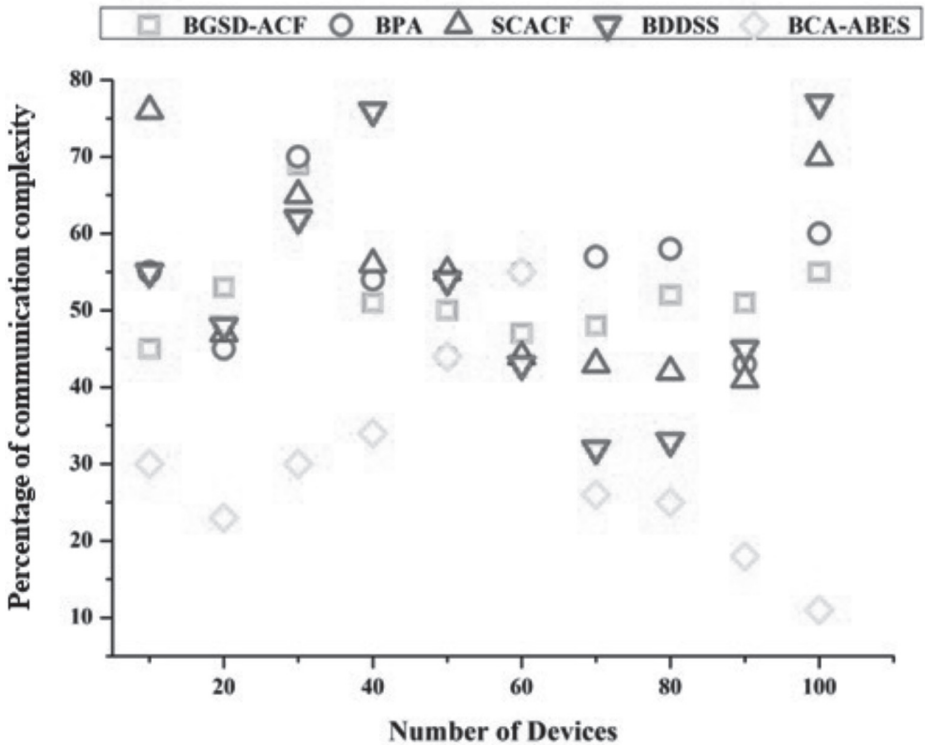

Figure 6 Communication complexity ratio.

credentials due to encryption and security protocols that have been thoroughly tested. Our method is more applicable because of its superior performance in terms of both storage and computation. Our protocol is secure against forgery and replay attacks, preserves user privacy. Appropriate credentials were provided using blockchain technology, and access information was sent securely and reliably. In addition, fraudulent activity was identified, and access to additional permission was limited using a restricted and auditable framework for partnership. The computational cost of both local users and outsourced decryption servers is reduced because of outsourcing and a more effective decryption method. This research leverages smart contracts on the blockchain to construct a decentralized ciphertext verification strategy,

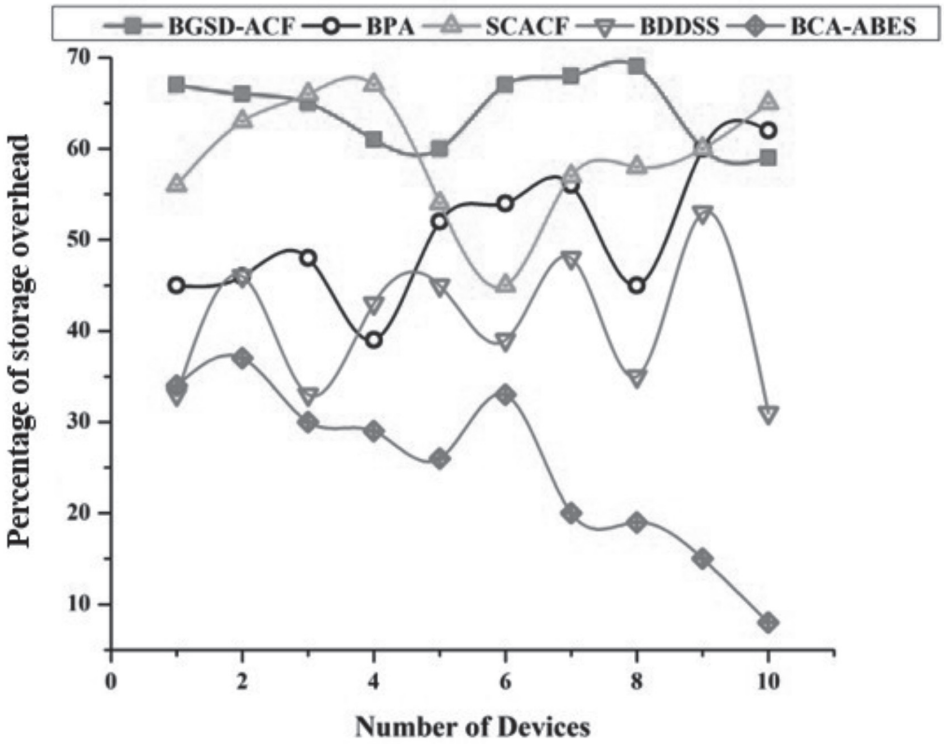

Figure 7 Percentage of storage overhead.

ensuring the validity of decryption results obtained from third-party services. Meanwhile, the conventional scheme's reliance on completely trustworthy cloud servers is reduced by verifying the decrypted data's integrity using a hash of the original information stored on the blockchain platform.

FUNDING

This work was supported by Provincial Excellent Course "Programming Foundation"(2022jpkc041); Provincial Teaching Research Project "Research on the" Double Line "Integration Mode Based on OBE Concept in Programming Courses"(2022jyxm423); Provincial Excellent Course "Information Technology"(2022jpkc042); "Research on the cultivation of employment ability of higher vocational students based on vocational education law"(AZCJ2024121) and "Innovation and practice of teaching mode of big data basic course for cultivating high-skilled talents(Ahly2024016)".

REFERENCES

1. Riad, K., Hamza, R., & Yan, H. (2019). Sensitive and energetic IoT access control for managing cloud electronic health records. IEEE Access, 7, 86384–86393.
2. Golightly, L., Modesti, P., Garcia, R., & Chang, V. (2023). Securing Distributed Systems: A Survey on Access Control Techniques for Cloud, Blockchain, IoT and SDN. Cyber Security and Applications, 100015.
3. Wang, C., Jin, H., Wei, R., & Zhou, K. (2022). Revocable, dynamic and decentralized data access control in cloud storage. The Journal of Supercomputing, 78(7), 10063–10087.
4. Xu, Z. Computational intelligence based sustainable computing with classification model for big data visualization on map reduce environment. Discov Internet Things 2, 2 (2022).
5. Kumar, G. S. (2020). Efficient data access control for cloud computing with large universe and traceable attribute-based encryption. International Journal of Fuzzy System Applications (IJFSA), 9(4), 61–81.
6. Mahmood, G. S., Huang, D. J., & Jaleel, B. A. (2019). A secure cloud computing system by using encryption and access control model. Journal of Information Processing Systems, 15(3), 538–549.
7. Qiu, J., Tian, Z., Du, C., Zuo, Q., Su, S., & Fang, B. (2020). A survey on access control in the age of internet of things. IEEE Internet of Things Journal, 7(6), 4682–4696.
8. Benmenzer, F., & Beghdad, R. (2022). An adaptive formal parallel technique with reputation integration for the enforcement of security policy in the cloud environment. Computer Communications, 196, 207–228.
9. Bertin, E., Hussein, D., Sengul, C., & Frey, V. (2019). Access control in the Internet of Things: a survey of existing approaches and open research questions. Annals of telecommunications, 74, 375–388.
10. Yang, C., Tan, L., Shi, N., Xu, B., Cao, Y., & Yu, K. (2020). AuthPrivacyChain: A blockchain-based access control framework with privacy protection in cloud. IEEE Access, 8, 70604–70615.
11. Qiu, Z., Zhang, Z., Tan, S., Wang, J., & Tao, X. (2019). Hierarchical Access Control with Scalable Data Sharing in Cloud Storage. Journal of Internet Technology, 20(3), 663–676.
12. Sun, P. (2020). Security and privacy protection in cloud computing: Discussions and challenges. Journal of Network and Computer Applications, 160, 102642.
13. Tariq, N., Asim, M., Al-Obeidat, F., Zubair Farooqi, M., Baker, T., Hammoudeh, M., & Ghafir, I. (2019). The security of big data in fog-enabled IoT applications including blockchain: A survey. Sensors, 19(8), 1788.
14. Wazid, M., Das, A. K., Hussain, R., Succi, G., & Rodrigues, J. J. (2019). Authentication in cloud-driven IoT-based big data environment: Survey and outlook. Journal of systems architecture, 97, 185–196.

15. Deepa, N., Pham, Q. V., Nguyen, D. C., Bhattacharya, S., Prabadevi, B., Gadekallu, T. R., ... & Pathirana, P. N. (2022). A survey on blockchain for big data: Approaches, opportunities, and future directions. Future Generation Computer Systems, 131, 209–226.
16. Xue, Y., Xue, K., Gai, N., Hong, J., Wei, D. S., & Hong, P. (2019). An attribute-based controlled collaborative access control scheme for public cloud storage. IEEE Transactions on Information Forensics and Security, 14(11), 2927–2942.
17. Stergiou, C. L., Psannis, K. E., & Gupta, B. B. (2020). IoT-based big data secure management in the fog over a 6G wireless network. IEEE Internet of Things Journal, 8(7), 5164–5171.
18. Liu, H., Han, D., & Li, D. (2020). Fabric-IoT: A blockchain-based access control system in IoT. IEEE Access, 8, 18207–18218.
19. Tan, L., Shi, N., Yu, K., Aloqaily, M., & Jararweh, Y. (2021). A blockchain-empowered access control framework for smart devices in green internet of things. ACM Transactions on Internet Technology (TOIT), 21(3), 1–20.
20. Li, J., Wu, J., Jiang, G., & Srikanthan, T. (2020). Blockchain-based public auditing for big data in cloud storage. Information Processing & Management, 57(6), 102382.
21. Saini, A., Zhu, Q., Singh, N., Xiang, Y., Gao, L., & Zhang, Y. (2020). A smart-contract-based access control framework for cloud smart healthcare system. IEEE Internet of Things Journal, 8(7), 5914–5925.
22. Egala, B. S., Pradhan, A. K., Badarla, V., & Mohanty, S. P. (2021). Fortified-chain: a blockchain-based framework for security and privacy-assured internet of medical things with effective access control. IEEE Internet of Things Journal, 8(14), 11717–11731.
23. Shi, M., Jiang, R., Hu, X., & Shang, J. (2020). A privacy protection method for health care big data management based on risk access control. Health care management science, 23, 427–442.
24. Qin, X., Huang, Y., Yang, Z., & Li, X. (2021). LBAC: A lightweight blockchain-based access control scheme for the internet of things. Information Sciences, 554, 222–235.
25. Pallavi, K. N., & Ravi Kumar, V. (2021). Authentication-based access control and data exchanging mechanism of IoT devices in fog computing environment. Wireless Personal Communications, 116, 3039–3060.
26. Joshi, S., Stalin, S., Shukla, P. K., Shukla, P. K., Bhatt, R., Bhadoria, R. S., & Tiwari, B. (2021). Unified authentication and access control for future mobile communication-based lightweight IoT systems using blockchain. Wireless Communications and Mobile Computing, 2021, 1–12.
27. Kesarwani, A., & Khilar, P. M. (2022). Development of trust based access control models using fuzzy logic in cloud computing. Journal of King Saud University-Computer and Information Sciences, 34(5), 1958–1967.
28. Figueroa-Lorenzo, S., Añorga, J., & Arrizabalaga, S. (2021). Methodological performance analysis applied to a novel IIoT access control system based on permissioned blockchain. Information Processing & Management, 58(4), 102558.
29. Atlam, H. F., & Wills, G. B. (2019). An efficient security risk estimation technique for Risk-based access control model for IoT. Internet of Things, 6, 100052.
30. Chinnasamy, P., Vinodhini, B., Praveena, V., Vinothini, C., & Sujitha, B. B. (2021, February). Blockchain based access control and data sharing systems for smart devices. In Journal of Physics: Conference Series (Vol. 1767, No. 1, p. 012056). IOP Publishing.
31. Ghaffari, F., Bertin, E., Crespi, N., Behrad, S., & Hatin, J. (2021). A novel access control method via smart contracts for internet-based service provisioning. IEEE Access, 9, 81253–81273.
32. Meng, X.(2020). The Analysis of non-significant feature data mining in big data environments. Engineering Intelligent Systems, vol. 28 no. 1, pp. 41–49.
33. Yang, C., Ji, X., Zhao, X., Dong, L., Zhao, Y. (2023). Application of data center knowledge graph based on power system fusion algorithm design. Engineering Intelligent Systems, vol. 30 no. 4, pp. 265–275.