Educational Administration: Theory and Practice
2024, 30(6), 732-742
ISSN: 2148-2403
https://kuey.net/

Research Article

An Efficient and Secured Threat Mitigation System in Cloud Computing Using Blockchain Technology

G. Abarna[1*], Dr. S. Thilagavathi[2],

[1*]Research Scholar, Sri Krishna Adithya College of Arts and Sciencemailtoabarnaganesan@gmail.com
[2]Assistant Professor, Sri Krishna Adithya College of Arts and Sciencethilagavathis@skacas.ac.in

Citation: G. Abarna et al (2024), An Efficient and Secured Threat Mitigation System in Cloud Computing Using Blockchain Technology, *Educational Administration: Theory and Practice*, 30(6), 732-742, Doi: 10.53555/kuey.v30i6.5319

ARTICLE INFO

ABSTRACT

The Blockchain-based Cloud Security Framework is innovative research that seeks to transform cloud security by incorporating blockchain technology. The main goal is to create and execute a strong structure that tackles the changing difficulties in cloud security. This system overcomes conventional methods by integrating decentralized identity and access management, promoting a more secure and transparent cloud environment. Real-time threat detection and incident response methods are essential elements that provide prompt and efficient countermeasures against potential security breaches. The cloud security framework prioritizes compliance and governance to ensure adherence to regulatory standards and inspire user confidence. The incorporation of thorough testing, user education, and knowledge dissemination procedures enhances the overall security stance. The Ciphertext-policy ABE (CP-ABE) model Aided blockchain architecture improves cloud security by utilizing the inherent qualities of blockchain, such as immutability and transparency, to create a tamper-resistant and auditable record of actions. This research represents a substantial advancement in enhancing cloud security procedures, providing a complete solution that tackles existing weaknesses and foresees potential threats in the ever-changing field of cloud computing.

Keywords: Block chain, key, block generation, cloud, privacy, encryption, decryption, and threat.

Introduction

Cloud computing can be defined as a type of computing that offers shared resources such as networks, storage, services, applications, data and servers on demand. It is based on internet and the resources are provisioned and released quickly with minimum organizational effort. The users and enterprises are given with a range of capabilities to store and work with their data either in a privately owned space or in a data center offered by third party provider. This data center is located in a far away remote place from the user, across the world. Cloud achieves coherence and also increase in economy by means of sharing resources to the users, similar to a utility computing like electricity grid over the network.

Cloud computing is the sharing of computing resources on demand over the internet as a pay-as-you-use basis. It means enough to pay only for the resources we used in the cloud and it supports the business to reduce operational expenses. It also manages the workspace infrastructure more effectively. Rather than buying and maintaining the own computing resources, data centers, and infrastructures, simply we can rent any resource such as storage, applications, etc from the cloud. Unlike traditional computing, if you are not using any resources, you need not pay for it.

The computing world has come across several stages in its lifetime. It starts from centralized computing which maintains the data as well as resources in a centralized location. The client should submit their task to the computing point and the server would produce the result to the client. Such a computing paradigm has faced a single-point failure issue that spoils the system. To overcome this issue, the decentralized computing models are arrived, which maintains the data and resources in multiple and distributed locations. This kind of computing model overcomes the single point failure issue but suffers from the cost issue.

The cloud is the environment that provides the number of services at a different level of the computing environment that can be accessed by the users of the environment. The cloud service provider provides several services at different scopes and enables the organizational users to access the services to perform the

required task. Whenever the user requests the service, the service manager finds the required service for the user and access the service for the user, and produces a result to the user.
The data located and stored in the cloud environment has been accessed through number of services. The service has been accessed by number of users of the environment and organizations. Such data access faces various security issues like any network threat faced. Any service visible to the external world faces various challenges and threats like Distributed Denial of Service (DDoS) attack, which involves in generating numerous malformed service access and tries to degrade the service performance. Also, the service data transmitted through the network has been affected by data modification attack which changes the meaning of service access.
Similarly, there are number of security issues can be named which target the service performance. For example, consider a banking application which provides different service to handle various operations. When a user generates a request to perform fund transfer which access the service by providing source, destination account with the amount to be transferred, it has been transmitted through number of network routers and nodes. If there is a malicious node which captures such information and modifies the details of destination account and amount, then the fund transfer has been made to a wrong account. Such threat must be handled with care and should be eradicated to provide the service with more security. Similarly, different services face different threats on the data part which affect the service performance as well as the overall performance of the entire system.
The growing information technology has opened the gate for global users to perform various activities through the web platform. This is not just for the individuals but the organizations also have adapted to different developments of information technology. Organizations store any information related to the customers which includes much information as sensitive and more private. In earlier days, they store their data in a centralized environment with client-server technology, but the failure that occurred on one side affected the entire system. The use of distributed computing has been adapted with many organizations to support the maintenance and access of different data. As the volume of data grows, the space complexity of the data also increases. This increases the requirement of dedicated data servers with more space which cost higher value. Not all organizations are capable of investing much amount to support the process.
In cloud computing, it is generally assumed that the users always trust the provider for provisioning the service honestly and pays to the provider before actually using the service. However, due to the monetary benefits involved, a rational provider may deviate from provisioning the service honestly. In order to address the fair payment problem, existing solutions comprise trusted parties for fair payments between user and provider. Nevertheless, having trusted parties do not solve the problem completely, and an additional financial cost is imposed on both user and provider. Blockchain, with its innovative properties like decentralization, immutability, transparency and smart contracts, emulate the trusted parties. In recent years, fair payment protocols without trusted parties using Blockchain technology are being explored. In current literature, fair payments for cloud services is not addressed adequately, and this motivates us to develop fair payment protocols for cloud services using Blockchain technology.
The mapping of Blockchain characteristics and their potential applications in cloud computing is shown in Table 1. Each characteristic would enhance the quality of cloud computing from the transparency and trust perspectives showing great potential of using Blockchain in cloud computing. The development of Blockchain-enabled solutions for cloud computing has only recently started and focuses on commercial targets. In the traditional cloud models, users are assumed to trust that the machine hardware, software, and cloud administrator all perform as expected. A wide range of things can go wrong, particularly when one wishes to tie the results of such computations to monetized entities such as smart contracts. Proper economic incentives, the cornerstone of any cryptocurrency, can deter many types of errors occurring in ways that simple task repetition cannot.

Table 1. Key characteristics of Blockchain and their potential applications to cloud computing.

Key characteristics of Blockchain	Description	The potential application to cloud computing
Decentralization	No centralized or trusted party controls the Blockchain.	Eliminates the need for trusted parties in the cloud computing environment for services like data auditing, data integrity, data timestamping, data searching, access control, resource allocation, service allocation, service discovery, billing and payments, and federated services.
Immutability	The data stored on the Blockchain can not be modified	Every interaction with cloud data / service can be recorded immutably on Blockchain, providing integrity and thus enabling tamper-proof data auditing. The logging of service interactions helps in monitoring user behaviour. As no party can alter the records stored in the append-only ledger, the billing of services based on these records will be fair and correct.

Transperency	All the interactions with the Blockchain are publicly available	Cloud provider, application developer, and the end-users can thoroughly check and monitor the transactions with equal rights. No party is deprived of its right to monitor the transactions there by instilling more trust and transparency in the Blockchain-enabled cloud services
Persistency	The data stored in the Blockchain are subject to public verifiability. All the transactions recorded on the Blockchain is verified for correctness and any attempt to maliciously change the state of the Blockchain will be thwarted.	Transactions created from all the interactions with cloud data / services are recorded and verified by the cloud provider and users. This verification enhances the persistency and reliability of Blockchain-enabled cloud services.
Auditability	As data is publicly available, it can be traced and audited easily.	Data auditing is one of the most critical tasks in cloud computing. Currently, cloud provider and user mutually distrust each other; hence a trusted party has to be required for performing the data auditing tasks. As data is available publicly, Blockchain eliminates the trusted party and enables provider and user to trace and audit data on their own.
Security and privacy	Blockchain systems employ public-key cryptography for authentication and non-repudiation. Access controls can be transcoded into smart contracts for authorization. Privacy for data can be provided either by employing private Blockchain or some known encryption techniques.	Blockchain supports secure cloud computing by providing distributed trust models with authentication and data privacy. Blockchain helps in protecting the cloud service end-users privacy by masking the real identity of end-users with a pseudonym generated through public-key cryptography. Blockchain also helps in protecting access control policies of cloud data / services from unauthorized entities.
Smart contracts	A smart contract can be thought as a program executed by a trusted global machine (Blockchain network) that will correctly execute every instruction.	A broad spectrum of cloud computing applications can be designed with smart contracts. For example, the service layer agreements can be transcoded into smart contracts and deployed on Blockchain for better trust, transparency and reliability of cloud services.

The solution to the organization comes in the name of the cloud environment. In the cloud environment, the resource provider deploys many resources and services to the environment. The organization and its users would maintain their data and access them through the services provided by the cloud service provider. However, the environment is not an exemption from the network threats available. Cloud services and data face several challenges in security which affect the performance of the service as well as the system. To handle this, there are several security measures and methods recommended by the researchers. Data security has been enforced differently. This paper discusses an efficient user-centric block-level attribute-based encryption to improve data security with block chain.

Related Works

The security of data has been identified as the most dominant factor in the cloud as it works in a loose couple environment. The cloud service provider does not know much about the users. However, securing the user data is more essential, and to handle this, different methods are designed. Some of the methods use ordinary public and private key-based approaches to encrypt the data. Similarly, some methods use profile-based key selection and encryption standards. Further, the security has been enforced with attribute-based encryption and also some techniques use dynamic key generation and encryption standards. This paper covers all these classes of encryption and performs a detailed review on data security in detail. Gai et al. (2020) [10] presents a detailed review on various access control schemes and encryption methods in literature. Also, discusses how blockchain would support the performance of cloud. Nguyen et al. (2020) [11] discusses various challenges in cloud and analyze how blockchain would be applied in improving the security performance.

Bhat et al. (2020) [12] classifies the security threats under different classes and analyze various approaches available in defending them. Also, the author discusses how block chain can be adapted to the problem. In (Cao et al. 2020) [13], argues that Blockchain's decentralized nature is probably going to bring about a low susceptibility to manipulation and forgery by malicious participants. Exceptional thought is given to how Blockchain-based identity and access management systems can address a portion of the key difficulties related with IoT security. The section gives a definite investigation and depiction of the Blockchain's roles in tracking the sources of weakness in supply chains identified with IoT gadgets. Utilizing Blockchain, it is likewise conceivable to contain an IoT security breach in a designated way after it is found. The section additionally examines and assesses drives of associations, between hierarchical organizations, and enterprises on the frontlines of Blockchain.

Liu et al. (2020) [14] introduced Blockchain-Aided Searchable Attribute-Based Encryption (BAS-ABE) uses the alliance Blockchain to create partial tokens. Additionally, the cloud server contained in our plan stores the enormous encrypted information as well as performs search and decryption for clients who just require one exponentiation in bunch G to decode completely. Xia et al. (2017) [15] propose a framework that resolves the issue of Medical Data Sharing (MeDShare) among clinical large information caretakers in a trust-less environment. The framework is Blockchain-based and gives information provenance, examining, and control for shared clinical information in cloud stores between enormous data entities.

Li et al. (2021) [16] present a decentralized and privacy-friendly charging system for electric vehicles, based on Blockchain and fog computing. In this scheme, fog computing is introduced to provide local processing with low latency. The computer network, made up of fog computing nodes, is used to provide localized services. In addition, a flexible Blockchain architecture of the consortium is offered. Wu & Ansari (2020) [17] present a efficient scheme to reduce the power consumption by customizing blockchain. The fog nodes are clustered to enforce effective access control by applying heuristic algorithm with hash values. Miao et al. (2020) [18] propose a distributed public auditing scheme to enforce privacy preservation with block chain. The method uses block chain in challenging the adversaries who generates unpredictable sources. Jabbar et al. (2021) [19] employs Ethereum to develop a solution aimed at facilitating Vehicle-to-Everything communications and parking payments. Moreover, the solution includes Android auto and application modules for automating the communication process.

Rahman et al. (2021) [20] propose a blockchain-Based Security Framework for a Critical Industry (BSF-CI) 4.0 Cyber-Physical System obviates the long-established certificate authority after enhancing the consortium block chain that reduces the data processing delay and increases cost-effective throughput. Liu et al. (2021) [21] explains the Construction of Double-Precision Wisdom Teaching Framework which supports the perception teaching with bigdata. The method uses black chain in analyzing the performance of learners and enables the sharing of resources. Hsiao & Sung (2021) [22] Employing blockchain Technology to Strengthen Security of Wireless Sensor Networks (Awadallah & Samsudin 2021), [23] presents a merkel tree-based approach in efficient data transmission with black chain where hash values are used with time stamp in the verification of data. Iqbal et al. 2021 [24] proposed a block chain orient veterinary management scheme in maintaining the clinical information. The method works based on smart contracts and performs predictive analysis. Yang et al. (2020) [25] presented a block chain technique for Attribute-Based Signcryption Scheme in sharing the data in secure way.

Proposed Methodology

In a cloud environment, data is stored with various features, and multiple users are granted access through provided services. However, users often have limited access to features, whereas services may require access to multiple features. It becomes essential to verify user permissions for different features accessed by services. The system maintains a user profile taxonomy indicating user access grants. To measure Trust Score of Data Level Access (TS-DLA) when service "S001" is requested, which returns user data and diagnosis values, the system estimates the TS-DLA value based on the user profile taxonomy and the specific features accessed by the service. The feature list estimation is given in Equation 1.

$$Feature_{List} = \sum Features \in D \text{---------(1)}$$

Here the value of $Feature_{List}$ is assigned as 8. The list of features which can be accessed by user is estimated using Equation 2.

$$\text{User Feature}_{\text{List}} = \int_{i=1}^{size(Profile_{Taxonamy})} \int_{i=1}^{size(Feature_{List})} Feature_{List}(j) \in PT(i).User == U \text{---------(2)}$$

Where, $Feature_{List}$ is the feature list, $\text{User Feature}_{\text{List}}$ is the access feature list of any service or user has access. According to this in Equation (2) the value of $\text{User Feature}_{\text{List}}$ is measured as 5.

Trust Score based on Previous Access is computed using Equation 3.

$$Trust\ Score_{Previous\ Access} = \frac{\sum_{i=1}^{size(Utilization)} Utilization(i) \cdot User == U \&\& Utilization \cdot Access = Complete}{\sum_{i=1}^{size(Utilization)} Utilization(i) \cdot User == U} \text{---------(3)}$$

The approach to enhancing data security in the cloud environment involves utilizing blockchain techniques instead of traditional access restrictions and encryption standards. Blockchain generates a chain of cryptographically secured data accessed by various users, where data is divided into blocks, each encrypted using a unique encryption scheme and key. Each block contains a hash code for data decryption, providing

information on key, index, and block reference. Unlike standard blockchain approaches with well-known key and scheme indexes, this method dynamically generates blockchain based on the split data blocks. Patient data, with features like Name, Age, Sex, etc., is encrypted with different schemes and keys, then split into blocks based on a randomly chosen number. Encryption keys and schemes are identified for each block, and hash codes are generated based on prime factors of character indexes. This Ciphertext-policy ABE (CP-ABE) model combines blockchain and CP-ABE to enforce data-level security. It starts with identifying user-requested service and data, determining user access to features using user profile taxonomy, and computing TS-DLA. Encryption keys and schemes vary for each feature, and data is split into blocks accordingly, with hash codes linking blocks for secure access. This approach is adaptable to the modern service-oriented environment, offering block-level encryption, time constraints, and tamper-proof security, enhancing performance and data security.

CP-ABE takes a security parameter λ and a set of attributes as input and generates a master secret key (MSK) and a set of public parameters (PP).

$$(MSK, PP) \leftarrow Setup(1^{\lambda}, Attributes) \text{ ---------(4)}$$

This algorithm encrypts a message under a specified access policy using the public parameters.

$$C \leftarrow Encrypt(Message, AcccessPolicy, PP) \text{ ---------(5)}$$

This algorithm generates a decryption key for a user with a set of attributes using the master secret key.

$$SK \leftarrow KeyExtract(MSK, User\ Attrubutes) \text{ ---------(6)}$$

This algorithm decrypts a ciphertext using a decryption key.

$$Message \leftarrow Decrypt(C, SK) \text{ ---------(7)}$$

The security of CP-ABE is typically defined in terms of correctness, confidentiality, and access control.

The organization holds customer data with various features, including sensitive information. Users are granted access to specific features, not necessarily all. When a user requests a service, it's crucial to verify their access grants to gauge trust. The data-level access trust-based approach restricts access by confirming user access grants and measuring trust, particularly through Trust $Score_{Previous\_Access}$. Trust Score of Data Level Access (TS-DLA) is computed based on requested features, user access, and PAT to enforce access restrictions. The TS-DLA scheme is detailed in pseudo-code, computing $Featur_{List}$, User $Feature_{List}$, and Trust Score (Previous Access) to determine TS-DLA for access restriction.

The process of TS-DLA is estimated using Equation 8 and the claimed data is given in Equation 9.

$$\text{TS} - \text{DLA} = \frac{size(\text{User Feature}_{\text{List}})}{size(Feature_{List})} \text{---------(8)}$$

$$D = \int Data \in R \text{---------(9)}$$

This algorithm aims to enforce data-level access trust in a system. It begins by fetching the trace (T), the user request (R), and the profile taxonomy (PT). It then identifies the claimed data set (D) based on the request. The algorithm computes the feature list (Fl) of the data set using Equation (1). Next, it determines the user's access feature using Equation (2). The algorithm measures the trust of previous access value using Equation (3). Using these values, it computes the TS-DLA measure using Equation (8). If the TS-DLA value exceeds a predefined threshold (Th), the algorithm returns true, indicating that access is granted. Otherwise, it returns false, denying access.

The process of generating block chain starts with the features of the data given. Consider, the given data D, which has N number of features, then the method read the scheme and key set first. Now, for each feature f belongs to D, the method selects a unique key k and scheme s from the key and scheme set in a random manner. Features (Fes) of data D using Equation 10 and the data is encrypted using Encryption scheme in E_s in Equation 11.

$$Fes = \int_{i=1}^{size(D)} \sum D(i)\ \varepsilon Feature_{List} \text{---------(10)}$$

$$E_s = \int_{i=1}^{size(\ Attribute_{Taxonamy})} Random(\ Attribute_{Taxonamy}(i) \cdot F == F,\ Attribute_{Taxonamy}(i) \cdot schemes) \text{---------(11)}$$

The appropriate encryption key E_k is selected using Equation 12 and Equation 13.

$$E_k = \int_{i=1}^{size(\ Attribute_{Taxonamy})} Random(\ Attribute_{Taxonamy}(i) \cdot F == F,\ Attribute_{Taxonamy}(i) \cdot kes) \text{---------(12)}$$

$$Fes = Encrypt(Feature, E_S, E_k) \text{ ---------(13)}$$

The final encrypted data is identified using Equation 14 where the random values (R) and data list (d_{list}) are generated using Equation 15 and Equation 16.

$$Encrypted\ Data\ (ED) = Merge(Fes) \text{ ---------(14)}$$

$$R = \int Random\ (3{,}10) \text{ ---------(15)}$$

$$Data_{list} = \int Split(E_r, R) \text{---------(16)}$$

The Block Chain (BC) is created with R blocks using Equation 17. The process of block generation is illustrated in Figure 1.

$$BC = \int_{i=1}^{size(Data_{list})} \sum(Blocks \in BC) \cup GenerateBlock \text{---------(17)}$$

This method encrypts data features using selected keys and schemes, merging them into a single entity. It then generates a blockchain with a random number of blocks (B) and splits the data accordingly. The algorithm selects keys and schemes for each feature, encrypts the data, and merges the encrypted features. It determines the size of the blockchain using Equation (15) and splits the data into the specified number of

blocks using Equation (16). A chain with the determined number of blocks is generated using Equation (17). The resulting blockchain and data blocks are utilized for data encryption to ensure secure communication. The method effectively secures data transfer through the encryption of features and the utilization of blockchain technology.

Each block within the chain comprises three main parts: the hash block, which contains the hash code necessary for data decryption, the data block, and the reference part. The hash code is pivotal in decrypting the data, allowing the receiver to identify the encryption key and scheme being employed. The hash code is generated through a multi-step process. Initially, a random number within the character set is selected. For instance, if the random number is 7, corresponding to the character "w" with an ASCII value of 35, the prime factor of the ASCII value is verified. If the ASCII value is prime, the hash code is generated by combining the character with a random value from the key set. Otherwise, the ASCII value is used as is, with a random value appended from the key set. This process ensures robust encryption, leveraging both randomization and prime factor values.

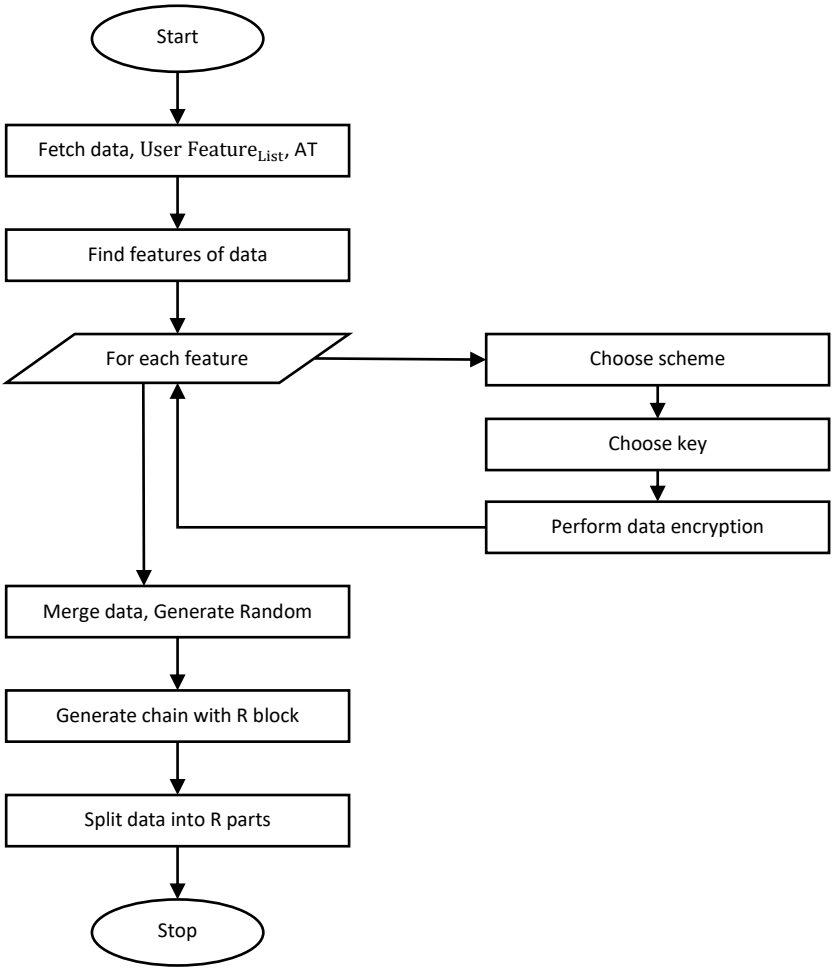

Figure 1. Block Generation

dynamically using the generated hash codes and blocks within the chain. The method iterates through each block, invoking hash code generation processes to encrypt the data according to the selected key and scheme. The encrypted data is then integrated into the block, alongside the hash code, thereby fortifying the blockchain's security. This iterative encryption process is crucial in safeguarding each block and ensuring the overall integrity of data transmission. The hash character generation process is given in Equation 18. The process of Hash generation is given in Figure 2.

$$HashCharachter = \int Random(1, size) \text{---------} (18)$$

Upon receiving the blockchain, decryption is performed at the block level to access the encrypted data. At each block, the hash code is extracted and analyzed, split into characters and numeric values. The ASCII value of the character is determined and verified for primality. If prime, the index of the decryption key is computed, facilitating data decryption. Otherwise, the index is computed based on the complement of the prime value. This meticulous decryption process ensures the confidentiality and integrity of transmitted data, safeguarding against unauthorized access.

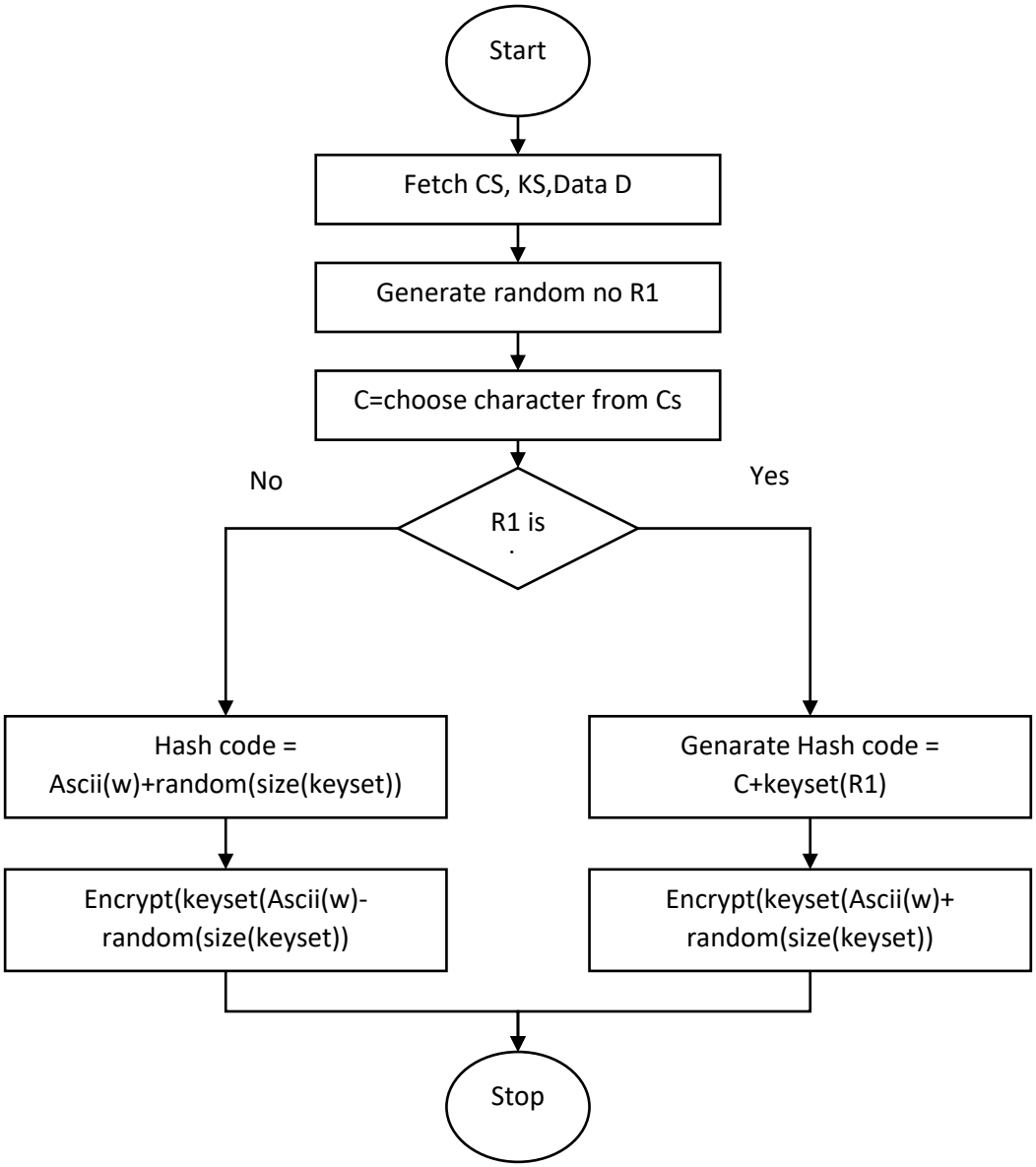

Figure 2. Hash Key Generation

The described process encompasses a systematic approach to data security, employing encryption and blockchain technology. Through the generation of hash codes, dynamic data encryption within the blockchain, and block-level decryption, robust protection against unauthorized access and data breaches is ensured. This comprehensive process underscores the importance of adopting advanced security measures to safeguard sensitive information in modern digital environments.

Result and Discussion

This section presents a detailed analysis of the experimental results obtained by various approaches. The proposed methods are implemented and evaluated for their performance under various constraints. The performances of the methods are measured on various parameters. Such results obtained are populated here and compared with the results of other approaches. The simulation description is given in Table 1.

Table 1. Simulation Setup

Parameter	Value
Tool Used	Advanced Java, IBM Cloud
Number of Users	200
No of Classes	5
No of Features	60

The environment details used for evaluating the performance various approaches are detailed in Table 1. The proposed methods are implemented in the Advanced Java platform and the IBM cloud has been used to

maintain the data. The environment has been considered with 200 users and the data present in the cloud are classified under 5 different classes. Also, the total number of features in the cloud data is considered as 60. According to this, the performances of the methods are measured in various parameters.

Data Security

Data security is the performance measure that represents the efficiency of the method in securing the data from various threats. It has been measured based on the number of threats generated and the number of them identified successfully. The value of data security is measured as follows:

$$Data\ Security\ Performance = \frac{Number\ of\ Threats\ Identified}{Total\ Threats\ Generated} \times 100 \text{---------(19)}$$

The above Equation (19) estimates the data security performance for any approach given according to the number of threats generated and the number of them identified.

Table 2. Comparison of Data Security

Algorithm	50	100	150	200
BSF-CI	72.4	76.3	78.3	80.56
MeDShare	75.1	79.3	80.2	82.56
BAS-ABE	81.2	82.3	83.2	84.45
CP-ABE	83	85.1	86.3	89.47

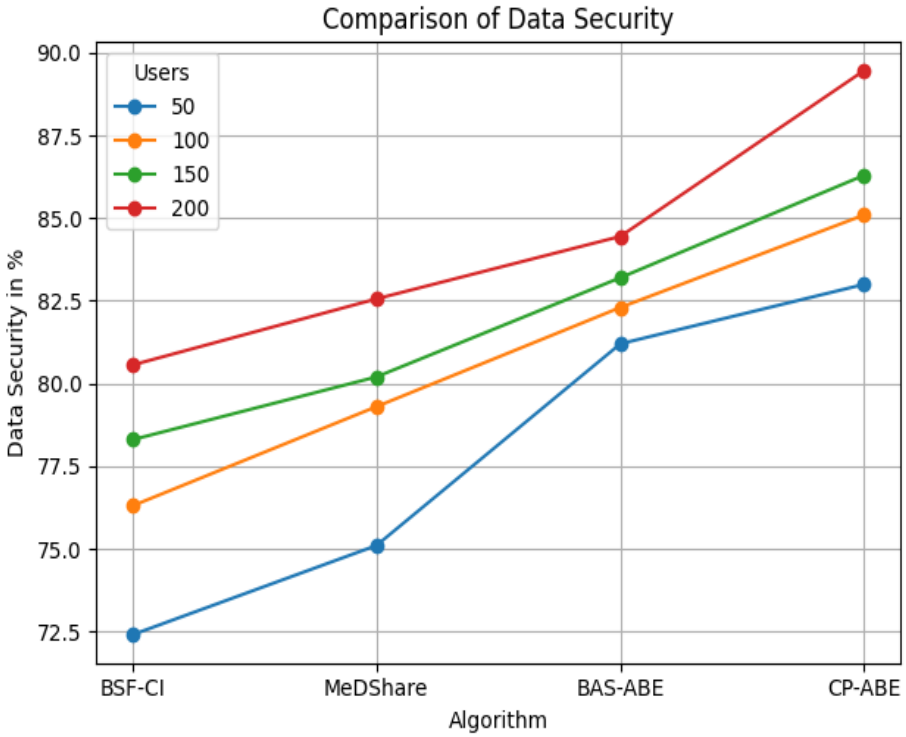

Figure 3. Comparison of Data Security

Throughput Performance

The throughput is a performance measure that defines the efficacy of the method in completing the request. It is measured with number of service requests generated and the number of them handled. It has been measured as follows:

$$Throughput = \frac{Number\ of\ Request\ Handled}{Total\ Request\ Received} \times 100 \text{---------(20)}$$

The above Equation (20) shows how the value of throughput performance is measured.

Table 3. Comparison of Throughput

Algorithm	50	100	150	200
BSF-CI	65	72	73	85.2
MeDShare	66	73.2	74.5	87
BAS-ABE	67	74	75.6	88
CP-ABE	67.9	75.4	76.5	89

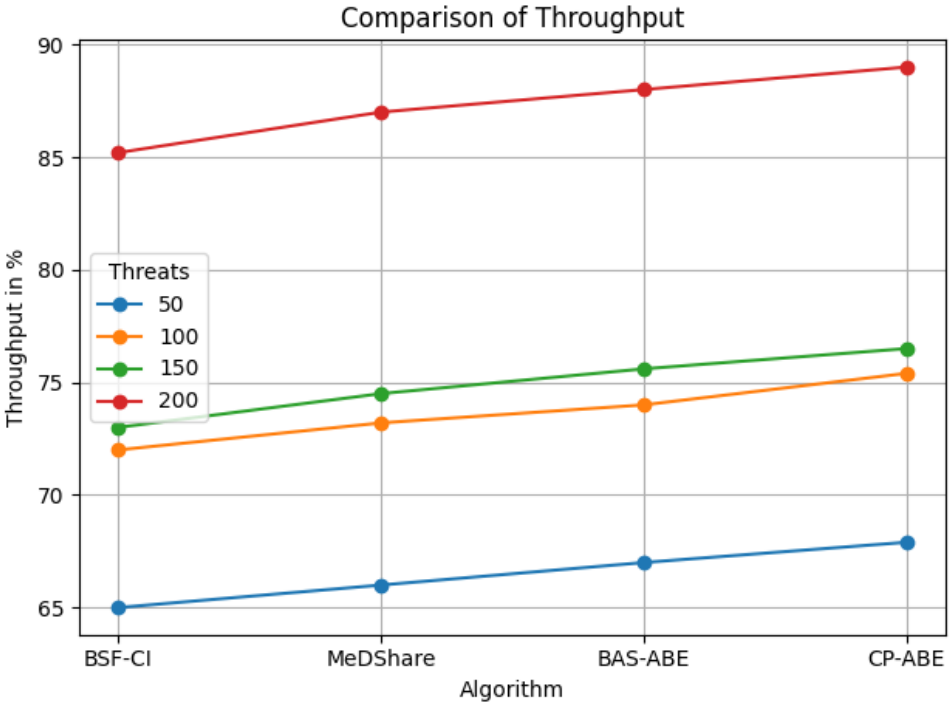

Figure 4. Comparison of Throughput

False Ratio in Access Restriction

The false ratio in restricting the malicious request is computed with the number of total malformed request generated and the number of them unidentified. It is shown in Equation (21) measured as follows:

$$False\ Ratio = \frac{Number\ of\ Malicious\ Request\ Unidentified}{Total\ Malicious\ Request\ Generated} \times 100 \text{---------(21)}$$

Table 5. Comparison of False Ratio

Algorithm	50	100	150	200
BSF-CI	29.3	27.3	24.6	18.4
MeDShare	21.4	20.4	19.02	15.3
BAS-ABE	19.2	18.7	17.34	12
CP-ABE	17.6	16.3	15	7.3

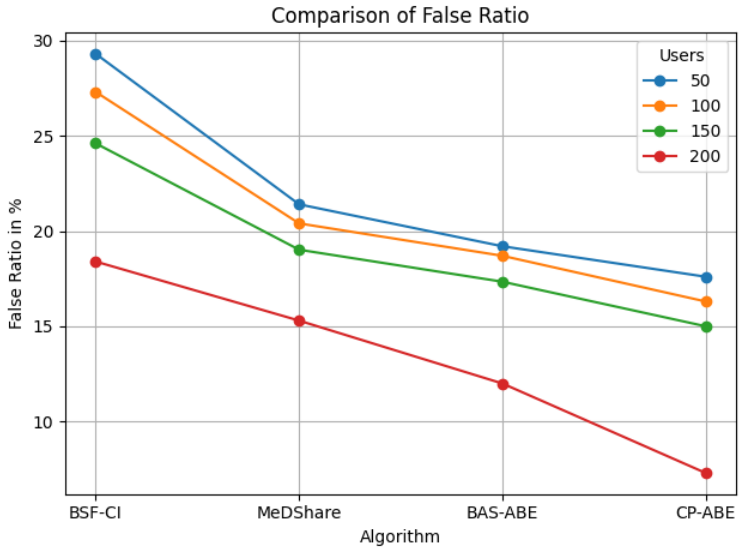

Figure 6. Comparison of False Ratio

In evaluating data security, BSF-CI demonstrates a performance ranging from 72.4% to 80.56%, showing an increase with the escalation of threats but ultimately achieving the lowest security performance among the compared algorithms. MeDShare presents a slightly better range of 75.1% to 82.56%, with moderate

improvement over BSF-CI and further enhancement with an uptick in threats. BAS-ABE showcases the highest security performance, ranging from 81.2% to 84.45%, consistently improving with the rise in threats. CP-ABE surpasses all others, boasting a performance range of 83% to 89.47%, exhibiting competitiveness with BAS-ABE and securing the highest performance level. In terms of throughput, BSF-CI displays a variable range from 65% to 85.2%, showing improvement with increased service requests. MeDShare demonstrates similar trends with moderate improvements over BSF-CI and consistent increments with service requests. Both BAS-ABE and CP-ABE showcase higher throughput, ranging from 67% to 88% and 67.9% to 89%, respectively, with CP-ABE exhibiting the highest throughput. Regarding false ratio in access restriction, BSF-CI shows a declining trend from 29.3% to 18.4%, while MeDShare consistently maintains lower ratios ranging from 21.4% to 15.3%. BAS-ABE demonstrates the lowest false ratio, declining from 19.2% to 12%, while CP-ABE excels with the lowest ratio, ranging from 17.6% to 7.3%. Overall, BAS-ABE and CP-ABE outshine other algorithms in terms of data security, throughput, and false ratio in access restriction. CP-ABE particularly stands out for its highest performance in both data security and throughput, while BAS-ABE excels in maintaining the lowest false ratio, underscoring its effectiveness in handling malicious requests.

Conclusion

This paper presented the detailed implementation of user-centric Dynamic TS-DLA based access restriction with block chain technique. The method collects the data and finds its features. Each feature has been encrypted with a randomly selected key and scheme. Further, they are merged and split into the number of blocks according to the chain generated. Now for each block of data, the method assigns a block in the chain. Each data block has been encrypted with a block-level encryption scheme which performs hash code generation to encrypt the data and generates the hash code to be added to the block. This is iterated for each block of the chin and the receiver receives the chain and decrypts the data using block-level data decryption. The proposed method improves the performance of data security and improves privacy preservation in the cloud environment. The proposed user centric block level attribute-based encryption scheme can be easily adapted to the real-world application because the recent trends are focused on user personalized solutions. So, adapting the proposed model to the real-world solution is not a big issue. Also, as it performs block level CP-ABE with tiny keys to improve data security, there will be no significant hike in time complexity or space complexity.

Reference

1. Han, H., Shiwakoti, R. K., Jarvis, R., Mordi, C., & Botchie, D. (2023). Accounting and auditing with blockchain technology and artificial Intelligence: A literature review. *International Journal of Accounting Information Systems*, *48*, 100598.
2. Di Vaio, A., Hassan, R., & Palladino, R. (2023). Blockchain technology and gender equality: A systematic literature review. *International Journal of Information Management*, *68*, 102517.
3. Malik, N., Appel, G., & Luo, L. (2023). Blockchain technology for creative industries: Current state and research opportunities. *International Journal of Research in Marketing*, *40*(1), 38-48.
4. Liu, W., Liu, X., Shi, X., Hou, J., Shi, V., & Dong, J. (2023). Collaborative adoption of blockchain technology: A supply chain contract perspective. *Frontiers of Engineering management*, *10*(1), 121-142.
5. Shah, V., Thakkar, V., & Khang, A. (2023). Electronic health records security and privacy enhancement using blockchain technology. In *Data-Centric AI Solutions and Emerging Technologies in the Healthcare Ecosystem* (pp. 1-13). CRC Press.
6. Kouhizadeh, M., Zhu, Q., & Sarkis, J. (2023). Circular economy performance measurements and blockchain technology: an examination of relationships. *The International Journal of Logistics Management*, *34*(3), 720-743.
7. Dal Mas, F., Massaro, M., Ndou, V., & Raguseo, E. (2023). Blockchain technologies for sustainability in the agrifood sector: A literature review of academic research and business perspectives. *Technological Forecasting and Social Change*, *187*, 122155.
8. Wenhua, Z., Qamar, F., Abdali, T. A. N., Hassan, R., Jafri, S. T. A., & Nguyen, Q. N. (2023). Blockchain technology: security issues, healthcare applications, challenges and future trends. *Electronics*, *12*(3), 546.
9. Yontar, E. (2023). Critical success factor analysis of blockchain technology in agri-food supply chain management: A circular economy perspective. *Journal of Environmental Management*, *330*, 117173.
10. Gai, K, Guo, J, Zhu, L & Yu, S 2020,'block chain Meets Cloud Computing: A Survey', IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 2009-2030.
11. Nguyen, DC, Pathirana, PN, Ding, M & Seneviratne, A 2019, 'Block chain for Secure EHRs Sharing of Mobile Cloud Based E-Health Systems', IEEE Access, vol. 7, pp. 66792-66806, doi: 10.1109/ ACCESS. 2019.2917555.
12. Bhat, Showkat & Bashir, Ishfaq 2020, 'Edge Computing and Its Convergence With block chain in 5G and Beyond: Security, Challenges, and Opportunities', IEEE Access, vol. 8, pp. 205340- 205373, doi:10.1109/ACCESS.2020.3037108.

13. Cao, L, Kang, Y, Wu, Q, Wu, R, Guo, X & Feng, T 2020, 'Searchable encryption cloud storage with dynamic data update to support efficient policy hiding', China Communications, vol. 17, no. 6, pp. 153-163.
14. Liu, S, Yu, J, Xiao, Y, Wan, Z, Wang, S & Yan, B 2020, 'BC-SABE: block chain-Aided Searchable Attribute-Based Encryption for CloudIoT', IEEE Internet of Things Journal, vol. 7, no. 9, pp. 7851-7867.
15. Xia, Q, Sifah, EB, Asamoah, KO, Gao, J, Du, X & Guizani, M 2017, 'MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via block chain', IEEE Access, vol. 5, pp. 14757-14767, doi: 10.1109/ACCESS.2017.2730843.
16. Li, H, Han, D & Tang, M 2021, 'A Privacy-Preserving Charging Scheme for Electric Vehicles Using block chain and Fog Computing', IEEE Systems Journal, vol. 15, no. 3, pp. 3189-3200.
17. Wu, D & Ansari, N 2020, 'A Cooperative Computing Strategy for block chain-Secured Fog Computing', IEEE Internet of Things Journal, vol. 7, no. 7, pp. 6603-6609.
18. Miao, Y, Huang, Q, Xiao, M & Li, H,2020, 'Decentralized and Privacy-Preserving Public Auditing for Cloud Storage Based on block chain', IEEE Access, vol. 8, pp. 139813-139826, doi: 10.1109/ ACCESS. 2020.3013153.
19. Jabbar, R, Fetais, N, Kharbeche, M, Krichen, M, Barkaoui, K & Shinoy, M 2021, 'Block chain for the Internet of Vehicles: How to Use block chain to Secure Vehicle-to-Everything (V2X) Communication and Payment?', IEEE Sensors Journal, vol. 21, no. 14, pp. 15807-15823.
20. Rahman, Z, Khalil, I, Yi, X & Atiquzzaman, M 2021, 'Block chainBased Security Framework for a Critical Industry 4.0 Cyber-Physical System', IEEE Communications Magazine, vol. 59, no. 5, pp. 128-134.
21. Liu, S, Dai, Y, Cai, Z, Pan, X & Li, C, 2021, 'Construction of DoublePrecision Wisdom Teaching Framework Based on block chain Technology in Cloud Platform', IEEE Access, vol. 9, pp. 11823-11834, doi: 10.1109/ACCESS.2021.3051468.
22. Hsiao, SJ & Sung, WT, 2021,'Employing block chain Technology to Strengthen Security of Wireless Sensor Networks', IEEE Access, vol. 9, pp. 72326-72341,doi: 10.1109/ACCESS.2021.3079708.
23. Awadallah, R & Samsudin, A, 2021, 'Using block chain in Cloud Computing to Enhance Relational Database Security', IEEE Access, vol.9,pp. 137353-137366,doi: 10.1109/ACCESS.2021.3117733.
24. Iqbal, N, Jamil, F, Ahmad, S & Kim, D 2021, 'A Novel block chain Based Integrity and Reliable Veterinary Clinic Information Management System Using Predictive Analytics for Provisioning of Quality Health Services', IEEE Access, vol. 9, pp. 8069-8098, doi: 10. 1109/ACCESS.2021.3049325.
25. Yang, C, Tan, L, Shi, N, Xu, B, Cao, Y & Yu, K 2020, 'AuthPrivacyChain: A block chain-Based Access Control Framework with Privacy Protection in Cloud', IEEE Access, vol. 8, pp. 70604-70615, doi: 10.1109/ACCESS.2020.2985762.