

Design of access control framework for big data as a service platform

Santosh Kumar Sharma¹, Ajay Pratap¹, Harsh Dev²

¹Amity Institute of Information Technology, Amity University, Noida, India

²Department of Computer Science, Pranveer Singh Institute of Technology, Kanpur, India

Article Info

Article history:

Received Oct 10, 2022

Revised Jul 25, 2023

Accepted Aug 7, 2023

Keywords:

Access control

Attribute based encryption

Big data as a service

Blockchain

CloudSim tool

ABSTRACT

Big data as a service (BDaaS) platform is widely used by various organizations for handling and processing the high volume of data generated from different internet of things (IoT) devices. Data generated from these IoT devices are kept in the form of big data with the help of cloud computing technology. Researchers are putting efforts into providing a more secure and protected access environment for the data available on the cloud. In order to create a safe, distributed, and decentralised environment in the cloud, blockchain technology has emerged as a useful tool. In this research paper, we have proposed a system that uses blockchain technology as a tool to regulate data access that is provided by BDaaS platforms. We are securing the access policy of data by using a modified form of ciphertext policy-attribute based encryption (CP-ABE) technique with the help of blockchain technology. For secure data access in BDaaS, algorithms have been created using a mix of CP-ABE with blockchain technology. Proposed smart contract algorithms are implemented using Eclipse 7.0 IDE and the cloud environment has been simulated on CloudSim tool. Results of key generation time, encryption time, and decryption time has been calculated and compared with access control mechanism without blockchain technology.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Ajay Pratap

Amity Institute of Information Technology, Amity University

Amity Rd, Sector 125, Noida, Uttar Pradesh, India

Email: chitransi.ajay@gmail.com

1. INTRODUCTION

In this digital era, data has become crucial asset for each and every organization as most of the decisions are based on these data. These data are generated from various sources like data from sensor-based devices, social media data, data of educational organizations, and government data [1]. Security is one of the major concern for these data once they are collected to some repository [2]. Blockchain technology was first developed for the exchange of digital currencies, but it has various applications for securing and protecting data, including internet of things (IoTs) [3]. These various sorts of data may be completely unstructured, partially structured, or both. Big data as a service (BDaaS) is a technique that combines the facility of storing data with computing capabilities of cloud computing environment wrapped with the processing capability of big data. This model is useful for delivering the data, analyzing the data and database, and also a platform for processing, along with other service models like platform as a service (PaaS), software as a service (SaaS), and infrastructure as a service (IaaS). BDaaS is known as cloud-based framework which provides end-to-end solutions related to big data on the basis of user demand. It can also be understood as system with joint capabilities of data as a service, Hadoop as a service and data analytics as a service. Various service models can be chosen to fulfill the specific demands of users. Although there are ample benefits for using BDaaS

platform but feature of security as well as privacy of the data kept in this environment becomes very critical issue. Researchers have developed various methods, frameworks, and architectures that can cater the issues related to the security and privacy of the data but still, there is a scope to address the issues of security and privacy such as access control, exposure of data, data breaches, and malicious adversary by cloud users [4]. Thus, we come to know that level of protection that is needed for big data security and privacy are not assured by the cloud providers.

It has been observed that, blockchain technology has become one of the good solutions for providing secure and decentralized environment for data [5]. Blockchain technology is useful in other areas of application which provide privacy and security to the data of smart home [6], smart city, education sector, and health sector. Bitcoin is one of the most well-known utilizations of the blockchain tasks. Technically, blockchain can be termed as distributed and decentralized blocks or ledgers that holds entire exchanges gathered in blocks that has finished at any point in the N/W. Blockchain is also popular distributed ledger technology (DLT). Working of blockchain technology is based on point to point (P2P) network in which every node is required to maintain a copy of the blockchain ledger. Blockchain databases are not governed by any central regulatory authority in this system. This technology also ensures that blockchain database is secured and protected from the various types of cyber-attacks. The objective of using blockchain technology in BDaaS kept on cloud storage architecture is to provide a more protected and secured environment for the users. Here we are not focusing on any specific resources in a single server, instead the blockchain network distributes all of them among nodes [7], [8]. We are the approach of decentralization concept of blockchain for security purposes. This is the area where a lot of work is to be done using the fusion of different techniques and methods.

A method called ciphertext policy-attribute based encryption (CP-ABE) is used to retrieve the data for given set of attributes and prohibits individuals with different attributes from accessing data. This technique creates a secret key for users that is based on set of attributes. In this situation, decryption of the ciphertext is possible only when the attribute of the user's secret key matches with decryption policy CP-ABE technique is used to control access that is proposed in IoT environment, and furthermore, it employs a hashing algorithm to conceal the access policy and implements a signature verification scheme to safeguard against insider attacks [9], [10]. CP-ABE-based access control and revocation of services mechanism has been proposed on blockchain-based cloud storage system [11]. Maesa *et al.* [12] presents the encryption of data stored in the blockchain network using a combination of CP-ABE and symmetric key algorithms. All possible aspects of using blockchain concept on cloud has been discussed by Gong and Navimipour, [13]. Use of block chain in different fields has been explored and case study of healthcare system has been presented [14]. This technique dynamically switches between full encryption and partial encryption based on a prudent decision strategy using a machine learning (ML) algorithm. This scheme addresses various aspects, including authorization, authorization revocation, access control, and real-time data auditing [15]. According to Saini *et al.* [16], a novel approach for creating an access control framework using smart contracts on a blockchain has been suggested. Authors has performed review of application of blockchain technology for securing cloud storage [17].

A strong cryptographic technique for access control and granular sharing on encrypted data is attribute based encryption (ABE). This functionality of ABE leads the adoption of ABE in encrypted cloud storage for flexible data sharing [18], [19]. Blockchain-based anonymous authentication with selective revocation for smart industrial applications (BASS) offers support for attribute privacy, selective revocation, and credential soundness, aiming to enhance security and privacy within smart industrial environments [20]. The basic architecture of BDaaS has been presented in [21] which is considered for this research paper. Random oracle model is used to handle security requirements such as mutual authentication and user anonymity and it also resists various malicious attacks [22]. Secure cloud storage framework with access control that combines the Ethereum blockchain and CP-ABE, has been proposed for secured access control [23], [24] presents the review, opportunities and challenges of transforming big data using cloud computing resources. CP-ABE can enhance the security of access control on shared data with efficient authority verification [25]. Homomorphic encryption, order-preserving encryption schemes, and ABE are also in trend as a good technique to provide data confidentiality and integrity. Thus, we can see that blockchain technology ABE are the technologies which are being used for various security aspects. Many authors have used different combination of technologies and concepts to handle different set of problems.

It has been observed that the combination of these two technologies can produce more better results. We have identified the following problems after the literature survey, which are as: i) owner of the data/software/services available at BDaaS environment, are not able to decide about the people who can access the data at run-time; ii) it is difficult to decide attributes for which access can be made possible for the users at the time of request; and iii) dependency of access control architecture on semi-trusted authority.

We have proposed an access control framework and designed algorithm for secure access control of data kept on BDaaS in cloud platform. The proposed framework uses CP-ABE algorithm to provide secured data access. Access information is stored in the blockchain in the form of smart contracts which are designed

in the form of algorithm. Contributions of the research paper are as: i) access control framework for BDaaS has been proposed using decentralized and secure blockchain technology. Sequence of entire process is also presented in the paper through diagram; ii) the proposed framework contains all the access policies in the smart contracts of blockchain network using customized form of CP-ABE algorithm which is among very popular algorithms for access control. It also uses the digital signature for the authentication of data; and iii) algorithm for user key generation, attribute authority key generation, user key generation, encryption, and decryption has been designed in this research paper.

2. PROPOSED METHOD

We need to understand the relation between big data, IoT, and BDaaS. Sensors are installed to collect the data that is very huge in amount and sometimes complex also. This data is termed as big data. Now users want to access data from this big data with the help of cloud provider to help organizations to management and analysis. Among these all-existing techniques of data access, we are using attribute-based access control techniques. In this technique, the qualities of users, systems, and environmental factors are used to evaluate a set of rules, regulations, and relationships in order to allow or deny access to data and services. CP-ABE technique is used for secured access control on blockchain environment. Fusion of these two technologies are making more secured access control environment in the proposed work.

2.1. Ciphertext policy-attribute based encryption algorithm

The highly popular access control mechanism known as ABE depends on characteristics to create the secret key of user and the ciphertext. ABE comes under symmetric-key encryption and has two types, which are key-policy attribute-based encryption (KP-ABE) and CP-ABE. In this research paper, our access control algorithm is derived from the CP-ABE algorithm which is implemented on the blockchain platform. Access control is a way to limit the access of any system or resources physically or virtually. We may also describe it as a security method that limits who can view or access information.

Basic steps of CP-ABE algorithm are as: i) generate public key (PK) and master key (MK), ii) encrypt the message along with the access structure of all attributes, then final output will be the ciphertext, iii) generate private key (SK) using MK and the attributes used, iv) decrypt the message using PK and SK, and v) if required, we can perform delegate step that will take the secret key and return the secret key for given set of attributes.

2.2. Workflow of proposed blockchain based access framework using CP-ABE

In this section, we have shown the workflow of the proposed model. The workflow is based on working of three major technologies in which the BDaaS available on cloud is secured for access control using CP-ABE algorithm and blockchain technology. Figure 1 presents the framework of proposed access control using blockchain and CP-ABE algorithm.

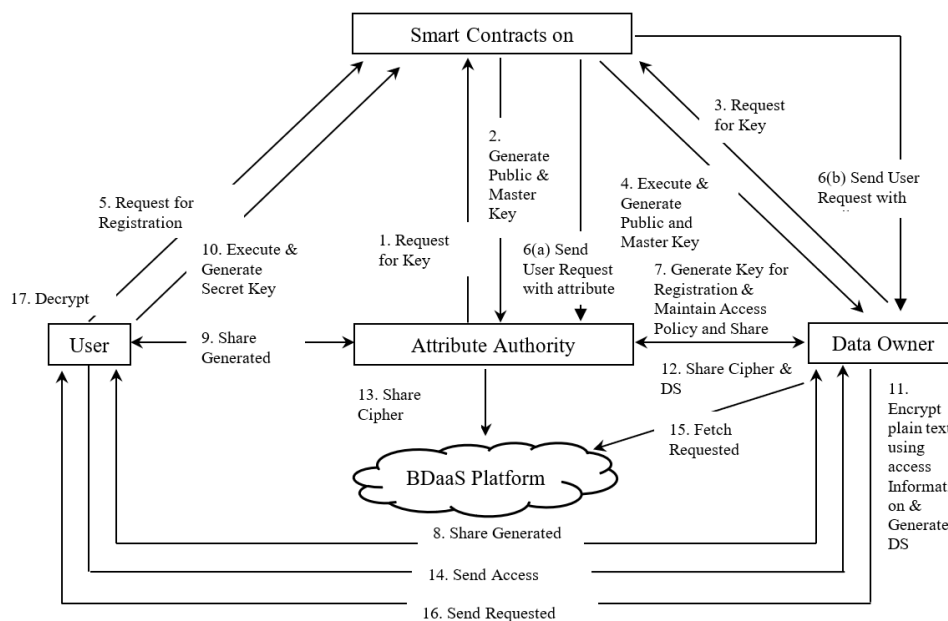


Figure 1. Proposed architecture for blockchain based access control in BDaaS

2.3. Workflow of given framework

Data owners and attribute authorities transmit requests for the production of public and MK, as well as global parameters, in order to register in the suggested architecture. This framework is initiated by attribute authority. Entire workflow of proposed framework is as:

- Step 1. Attribute authorities send request to blockchain network for key generation requests.
- Step 2. Blockchain network generates public key [PK(AA)] and master keys [MSK(AA)] for registration in the proposed architecture and sends to attribute authorities.
- Step 3. Service owner send request to blockchain network for key generation.
- Step 4. Blockchain network generates public key [PK(DO)] and master keys [MSK(DO)] for registration in the proposed architecture and sends to service owner.
- Step 5. User sends the request for registration to the blockchain network.
- Step 6. Blockchain network sends the details [U(AT)] (attributes such as ID, Name, Contact No, Email ID) of user to the service owner and attribute authority.
- Step 7. The service owner and the attribute authority save the details of user and generates an access key using CP-ABE algorithm corresponding to the user's list of attributes and shares with attribute authority.
- Step 8. Service owners shares the generated access key [SK (DO, User)] with the user.
- Step 9. Attribute authority shares the access key [SK (AA, User)] with the user and also generate access key for attribute group key [SK* (AA, User)].
- Step 10. Now user generates secret key [SK(USER)] by executing key generation algorithm by using the keys generated by service owner and attribute authority.
- Step 11. Service owner encrypts the plain text into ciphertext and digital signature.
- Step 12. Service owner shares the cipher text with attribute authority.
- Step 13. Cipher text generated in Step-11 is outsourced to BDaaS platform on cloud.
- Step 14. Whenever the user sends the request for access to data owner, then data owner takes it from BDaaS platform on cloud and shares with the user.
- Step 15. The user performs decryption process on cipher text and verify the digital signature. User can do it only if they are authenticated user.

2.4. Designing of smart contract algorithms for proposed framework

All the parameters of access control are handled by using smart contract which are simple programs and stored at blockchain. These programs execute when predefined condition given in smart contract are met. In the proposed model, entire access control is managed using different algorithms which will be written in CP-ABE. CP-ABE algorithm is based on four fundamental concepts, which are setup, encrypt, generation_of_key (KeyGen) and decrypt. Setup algorithm takes implicit security parameters and provides public parameters PK and MK. Encrypt algorithm takes parameters as PK, message (M) and access structure (A) which is represented as encrypt (PK, M, A) and after encryption it provides cipher text (CT) which can be decrypted by only those users who possess attributes defined in access structure. Key generation algorithm takes two parameters as MK and set of attributes (S) as an input which is represented as KeyGen (MK, S) and produces SK. After this the decrypt algorithm comes in the picture and takes PK, CT with access policy and SK with set of attributes as an input and represented as decrypt (PK, CT, SK) that produces message M after decryption if set of attributes satisfies the access structure.

All smart contracts functions will be designed using CP-ABE algorithm and data owner and attribute authorities are involved to provide all required services to the users. By analyzing the workflow of proposed framework, we are identifying all smart contract algorithm used for access control, which are as: i) PK and MK generation for registration process, ii) user key generation algorithm, iii) algorithm for encryption, iv) algorithm for re-encryption, and v) algorithm for decryption.

2.4.1. Algorithm for setting security parameters

This is section, we set up security parameters for the proposed model. It is represented by setup (GP, U) that takes the general security parameters and universal attribute set and generates the SK and MK for the owner and attribute authority. KeyGen (DO) (GP) and KeyGen (AA) (GP,c,d) are the two algorithms that are the parts of this setup.

2.4.2. Key generation algorithm for data owner

In this proposed framework data owner generates the keys using key generation algorithm. This algorithm takes general security parameters as an input and generates SK and MK for the data owner. Propose algorithm for key generation of data owner is shown in the Algorithm 1.

Algorithm 1. Key generation for data owner

Input: General Security Parameter (GP)

Output: Private Key of Owner [PK (DO)], Master Key of Data Owner [MSK (DO)]

Algorithm:

This algorithm will be denoted as KeyGen (DO) (GP) \rightarrow {PK(DO), MSK(DO)}

Step 1- Start

Step 2- Choose a random number 'a' from the finite field over prime number p.

 $a \in \mathbb{Z}_p$

Step 3- Choose a generator 'g' which fulfill the criteria:

 $b \leftarrow ga$ Here b is also from the finite field over prime number p. i.e. $b \in \mathbb{Z}_p$ Step 4- PK(DO) $\leftarrow b$ Step 5- MSK(DO) $\leftarrow a$

Step 6- Stop

2.4.3. Key generation algorithm for attribute authority

Attribute authority of proposed framework generate keys using Algorithm 2. This algorithm accepts general security parameters and two random numbers from group under multiplication modulo of p. SK and MK of attribute authority are output of this algorithm.

Algorithm 2. Key generation for attribute authorityInput: General Security Parameter (GP), Random Numbers c and d from \mathbb{Z}_p^*

Output: Private Key of Attribute Authority [PK (AA)], Master Key of Attribute Authority [MSK (AA)]

Algorithm:

This algorithm will be denoted as KeyGen(AA) (GP,c,d) \rightarrow {PK(AA) , MSK(AA)}

Step 1- Start

Step 2- Choose a random number c from \mathbb{Z}_p^* .Step 3- Choose a random number d from \mathbb{Z}_p^* .Step 4- PK (AA) $\leftarrow e(g,g)^c$ Step 5- MSK (AA) $\leftarrow gc$ Step 6- PK* (AA) $\leftarrow gd$

Step 7- Stop

2.4.4. Key generation algorithm for users

Attribute authority and data owners receive the attributes of user and generate access keys with the help of Algorithm 3. These access keys are used to generate a secret key for the user. We can use some such protocol by which they can generate a secret key without telling their own keys. Two party computation function can be used to generate such key.

Algorithm 3. Key generation for users

Input: Master Key MSK (DO) and MSK (AA), User Attribute U (AT)

Output: User Secret Key [SK (USER)]

Algorithm:

This algorithm will be denoted as UserKeyGen (MSK(DO), MSK(AA), U(AT)) \rightarrow SK(USER)

Step 1- Start

Step 2- Attribute Authority and Data Owner authenticate the User

Step 3- Data Owner selects random exponent which is unique and secret to user i.e. $m \in \mathbb{Z}^*P$ Step 4- Attribute authority selects random exponent i.e. $n \in \mathbb{Z}^*p$

Step 5- Define two party computation function as

 $F = 2PC(DO(m,a), AA(c)) = (c + m) a$

Step 6- Data Owner computes the parameter M

 $M = g(F/n) = g(c + m) a / n$

Step 7- Attribute Authority compute the parameter N

 $N = M(1/a^2) = g(c + m) / n a$

Step 8- Data Owner sent parameter M to Attribute authority and attribute authority sent the parameter N to data owner using 2PC for computation of secret key.

i. Attribute Authority generate secret key

 $SK(AA, User) = N n = g(c + m) / a$

ii. Data Owner generates secret key

 $SK(DO, User) = (D_i = g n \cdot H(i)R_i, D_i = gR_i)$ For all $i \in \text{Tree}$ and $R_i \in \mathbb{Z}^*P$

iii. Attribute authority generates another secret key for attribute group key

 $SK^*(AA, User) = H(User)C$

Step 9- Secret keys of data owner and attribute authority is used to generate

 $SK(USER) = \{SK(AA, User), SK(DO, User)\}$

Step 10- Stop

2.4.5. Algorithm for data encryption and digital signature

Algorithm 4 is executed by data owner to encrypt the data according to the given access tree structure. After the encryption of data, data owner sent it to the big data platform available on cloud. This algorithm requires three parameters which are PK, data to be encrypted, and access structure. Here PK of two parties i.e. data owner and attribute authority are involved so, both PK of data owner $PK_{[DO]}$ and $PK_{[AA]}$ will be used for encryption.

Algorithm 4. For data encryption and digital signature

Input: Public Key of Data Owner $[PK(DO)]$, Public Key of Attribute Authority $[PK(AA)]$, Plain Text/Data $[M]$, Access Tree Structure $[ATS]$
Output: Digital Signature $[DS]$, Cipher Text $[CT]$

Algorithm:

This algorithm is denoted as $EncryptSign(PK(DO), PK(AA), M, ATS) \rightarrow DS, CT$

Step 1- Start

Step 2- For each node x in access tree ATS Choose a polynomial P_x

Step 3- If node is Root Node then Set $P_x(0) = s$ else

Step 4- If x is any other point of polynomial

Step 5- Set $P_x(0) = P_{parent(x)}(index(x))$

Step 6- Calculate parameter $C' = M \cdot e(g, g)$ as

Step 7- Calculate parameter $C = h s$, else

Step 8- If node y is leaf node then

Step 9- Calculate parameter $CY' = g^{Py(0)}$

Step 10- Calculate parameter $CY = H(attr(Y) Py(0))$

Step 11- Calculation of Final Cipher Text is done as:

Step 12- $CT = [ATS, Sign = h(M), C' = M \cdot e(g, g) \text{ as } C = hs, (CY = H(attr(Y) Py(0)), CY' = g^{Py(0)} \text{ for all } x)]$

Step 13- Stop

2.4.6. Algorithm for data decryption and verification

Data decryption and user verification are two main tasks of this algorithm. Algorithm take secret key of user, CT , and digital signature of user. If verification is successful, then data decryption is performed. Detailed algorithm is designed as shown in Algorithm 5.

Algorithm 5. For data decryption and verification

Input: Secret Key of User $[SK(USER)]$, Cipher Text $[CT]$, Digital Signature $[DS]$
Output: Digital Signature Verification [Success/ Failure], Plain Text / Data $[M]$

Algorithm:

This algorithm is denoted as $Decryptify(SK[USER], PK[AA], CT) \rightarrow Success/ Failure, M$

Step 1- Start

Step 2- When x is leaf node && if $i \in S$ and $i = order(x)$ then

Step 3- $Decryptify(SK[USER], PK[AA], CT, x) = e(D_j, C_y) / e(D'_i, C'_y)$

Step 4- If i does not belong to S then

Step 5- $Decryptify(SK[USER], PK[AA], CT, x) = Null$

Step 6- When policy is satisfied by access tree then:

Step 7- $Decryptify(SK[USER], CT, z) = e(g, g)^{FS}$

Step 8- $C' = F \cdot e(g, g)^{aS}, e(C, D) = e(gaS, ga+n/b)$

Step 9- $M = C' / e(C, D)^{1/S}$

Step 10- Verify (M, DS, PUK)

Step 11- Compute $e(h(M), gx)$

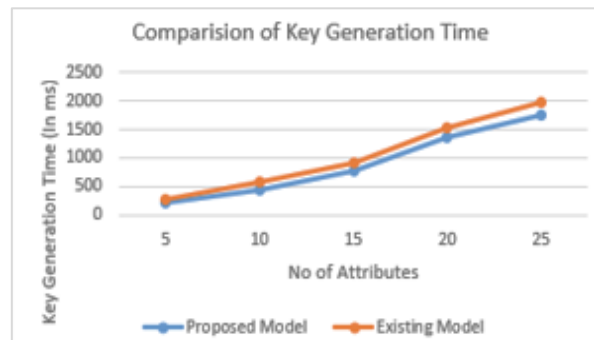
Step 11- Stop

3. RESULTS AND DISCUSSION

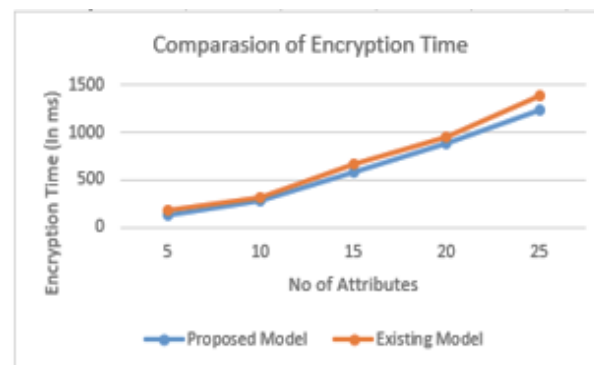
This environment has been set up on 64-bit windows 10 operating system (OS) having Intel (R) core (TM) i3, 2.20 GHz processor and 8 GB RAM. We are using CloudSim-3.0.3 framework, that is a simulation tool for the cloud storage environment. CloudSim is an open software that is used to provide the virtualization of cloud computing data center and also helps in virtualized cloud modelling and simulation. CloudSim framework provides the cloud computing component and behavioral modelling. This framework offers useful insights such as dynamic, distributed, and scalable environment. Eclipse 7.0 IDE has been used for implementing the proposed architecture with JDK 1.7. Also, external auxiliary java pairing-based cryptography is being used to implement the concept of bilinear pairing-based cryptography. Integration of java-based blockchain network with CloudSim-3.0.3 is done with the help of jar file CloudSim-3.0.3.jar. Available blockchain networks are not directly deployed, instead of that we are defining a minimized block header for maintaining user details.

From implementation point of view, we are creating different classes in java programming language for creation, storing, and validation of blocks and then this blockchain network is deployed with CP-ABE algorithm. Core functionalities such as generation of user keys and data owner keys, encryption, and decryption are provided by cloud storage services. Now according to the responses of user and data owner smart contract functions triggers automatically. Cloud storage service are also deployed by using the CloudSim tool.

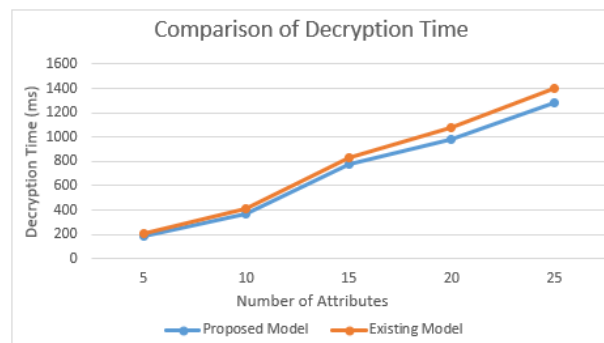
Performance of proposed system is analysed in terms of key generation time, encryption time, and decryption process. Here keys are generated for user and owner. It is the time required to generate keys either for user or owner after giving registration details. Encryption time is that is required to convert the plaintext to ciphertext. Decryption time is defined as the time that is required to get the plaintext from the ciphertext. We are using the data set that contains 6 access policies in the form of smart contracts, 25 attributes. Starting from 10 attributes, we are increasing the number of attributes and calculation the key generation time, encryption time, and decryption time of proposed system using org.cloudbus. CloudSim package of CloudSim simulator. Results obtained from this setup are calculated and the comparison between the existing model and proposed model is compared. In Figure 2, we have shown the results of various calculation performed to calculate the performance of proposed system. Figures 2(a) to (c) clearly show that key generation time, encryption time, and decryption time of proposed system is less as compare to the existing model though the complexity of system is increasing due to involvement of blockchain.



(a)



(b)



(c)

Figure 2. Comparison of (a) user key generation time, (b) encryption time, and (c) decryption time

4. CONCLUSION

As we know, the privacy and security of data kept on the BDaaS platform are challenging issues. In the proposed framework, we have designed the framework for secured data access in the BDaaS platform using blockchain technology in combination with the CP-ABE algorithm. The algorithm for secured access control has been designed according to the blockchain environment. The setup phase generates two algorithms which are for SK and MK generation of both data owner and attribute authority. Once the user registers on the blockchain network, the data owner, and attribute authority generate a secret key for that user. Both secret keys are passed through a two-party computation function to generate one common key for the user. Now the data encryption is performed and the digital signature of data is generated. The user decrypts the data using its secret key and also verifies the data. The existing model considered in this research was implemented without the involvement of blockchain technology. After implementing it with blockchain technology and compared the results on three parameters that are key generation time, encryption time, and decryption time. By analyzing the results, it is very clear that the performance of the proposed system has improved after putting one more layer of blockchain in the existing model of access control that is only with the CP-ABE algorithm. In the future, we are planning to try some modified versions of the CP-ABE algorithm and also the KP-ABE algorithm. Then we will compare the result with our proposed model and analyze the result.




REFERENCES

- [1] D. A. Pratap, "Review of dimensionality reduction techniques in data mining from big data," *International Journal for Research in Applied Science and Engineering Technology*, vol. 7, no. 5, pp. 2135–2144, May 2019, doi: 10.22214/ijraset.2019.5359.
- [2] S. K. Singh, P. K. Manjhi, and R. K. Tiwari, "Cloud computing security using blockchain technology," *Transforming Cybersecurity Solutions using Blockchain*, pp. 19–30, 2021, doi: 10.1007/978-981-33-6858-3_2.
- [3] H. Shekhawat, S. Sharma, and R. Koli, "Privacy-preserving techniques for big data analysis in cloud," in *2019 Second International Conference on Advanced Computational and Communication Paradigms (ICACCP)*, IEEE, Feb. 2019, pp. 1–6. doi: 10.1109/ICACCP.2019.8882922.
- [4] P. Chinnasamy, P. Deepalakshmi, A. K. Dutta, J. You, and G. P. Joshi, "Ciphertext-policy attribute-based encryption for cloud storage: toward data privacy and authentication in AI-enabled IoT system," *Mathematics*, vol. 10, no. 1, pp. 1–24, Dec. 2021, doi: 10.3390/math10010068.
- [5] N. Elisa, L. Yang, F. Chao, and Y. Cao, "A framework of blockchain-based secure and privacy-preserving E-government system," *Wireless Networks*, vol. 29, no. 3, pp. 1005–1015, Apr. 2023, doi: 10.1007/s11276-018-1883-0.
- [6] S. Khan, K. A. Shakil, S. A. Ali, and M. Alam, "On designing a generic framework for big data-as-a-service," in *2018 1st International Conference on Advanced Research in Engineering Sciences (ARES)*, IEEE, Jun. 2018, pp. 1–5. doi: 10.1109/ARES.2018.8723269.
- [7] T. Lee, H.-S. Moon, and J. Jang, "Data encryption method using CP-ABE with symmetric key algorithm in blockchain network," in *2021 International Conference on Information and Communication Technology Convergence (ICTC)*, IEEE, Oct. 2021, pp. 1371–1373. doi: 10.1109/ICTC52510.2021.9620889.
- [8] X. Wang, L. T. Yang, H. Liu, and M. J. Deen, "A big data-as-a-service framework: state-of-the-art and perspectives," *IEEE Transactions on Big Data*, vol. 4, no. 3, pp. 325–340, Sep. 2018, doi: 10.1109/TBDDATA.2017.2757942.
- [9] M. B. Taha, H. Ould-Slimane, and C. Talhi, "Smart offloading technique for CP-ABE encryption schemes in constrained devices," *SN Applied Sciences*, vol. 2, no. 2, pp. 1–19, Feb. 2020, doi: 10.1007/s42452-020-2074-z.
- [10] S. Agrawal and M. Chase, "FAME," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, New York, NY, USA: ACM, Oct. 2017, pp. 665–682. doi: 10.1145/3133956.3134014.
- [11] P. Sharma, R. Jindal, and M. D. Borah, "Blockchain technology for cloud storage," *ACM Computing Surveys*, vol. 53, no. 4, pp. 1–32, Jul. 2021, doi: 10.1145/3403954.
- [12] 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, Jul. 2019, doi: 10.1016/j.cose.2019.03.016.
- [13] J. Gong and N. J. Navimipour, "An in-depth and systematic literature review on the blockchain-based approaches for cloud computing," *Cluster Computing*, vol. 25, no. 1, pp. 383–400, 2022, doi: 10.1007/s10586-021-03412-2.
- [14] R. Kumar and R. Tripathi, "A secure and distributed framework for sharing COVID-19 patient reports using consortium blockchain and IPFS," in *2020 Sixth International Conference on Parallel, Distributed, and Grid Computing (PDGC)*, IEEE, Nov. 2020, pp. 231–236. doi: 10.1109/PDGC50313.2020.9315755.
- [15] L. Tan, N. Shi, C. Yang, and K. Yu, "A blockchain-based access control framework for cyber-physical-social system big data," *IEEE Access*, vol. 8, pp. 77215–77226, 2020, doi: 10.1109/ACCESS.2020.2988951.
- [16] A. Saini, Q. Zhu, N. Singh, Y. Xiang, L. Gao, and Y. Zhang, "A smart-contract-based access control framework for cloud smart healthcare system," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5914–5925, Apr. 2021, doi: 10.1109/JIOT.2020.3032997.
- [17] P. Sharma, R. Jindal, and M. D. Borah, "Blockchain-based cloud storage system with CP-ABE-based access control and revocation process," *The Journal of Supercomputing*, vol. 78, no. 6, pp. 7700–7728, Apr. 2022, doi: 10.1007/s11227-021-04179-4.
- [18] H. Zheng, J. Shao, and G. Wei, "Attribute-based encryption with outsourced decryption in blockchain," *Peer-to-Peer Networking and Applications*, vol. 13, no. 5, pp. 1643–1655, Sep. 2020, doi: 10.1007/s12083-020-00918-1.
- [19] Q. Su, R. Zhang, R. Xue, and P. Li, "Revocable attribute-based signature for blockchain-based healthcare system," *IEEE Access*, vol. 8, pp. 127884–127896, 2020, doi: 10.1109/ACCESS.2020.3007691.
- [20] Y. Yu, Y. Zhao, Y. Li, X. Du, L. Wang, and M. Guizani, "Blockchain-based anonymous authentication with selective revocation for smart industrial applications," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 5, pp. 3290–3300, May 2020, doi: 10.1109/TH.2019.2944678.
- [21] S. K. Sharma, A. Pratap, and H. Dev, "Challenges against big data as a service a survey," *International Journal of Computer Sciences and Engineering*, vol. 7, no. 12, pp. 74–78, Dec. 2019, doi: 10.26438/ijcse/v7i12.7478.
- [22] L. Xiong, F. Li, S. Zeng, T. Peng, and Z. Liu, "A blockchain-based privacy-awareness authentication scheme with efficient revocation for multi-server architectures," *IEEE Access*, vol. 7, pp. 125840–125853, 2019, doi: 10.1109/ACCESS.2019.2939368.




- [23] S. Wang, X. Wang, and Y. Zhang, "A secure cloud storage framework with access control based on blockchain," *IEEE Access*, vol. 7, pp. 112713–112725, 2019, doi: 10.1109/ACCESS.2019.2929205.
- [24] M. Muniswamaiah, T. Agerwala, and C. Tappert, "Big data in cloud computing review and opportunities," *International Journal of Computer Science and Information Technology*, vol. 11, no. 4, pp. 43–57, Aug. 2019, doi: 10.5121/ijcsit.2019.11404.
- [25] L. Zhang, Y. Cui, and Y. Mu, "Improving security and privacy attribute based data sharing in cloud computing," *IEEE Systems Journal*, vol. 14, no. 1, pp. 387–397, Mar. 2020, doi: 10.1109/JSYST.2019.2911391.

BIOGRAPHIES OF AUTHORS






Santosh Kumar Sharma    completed master of computer application from Uttar Pradesh Technical University, Lucknow, then received his M.Tech. degree in computer science from Graphic Era University, Dehradun. He is pursuing Ph.D. from Amity University, Lucknow. He is now full-time assistant professor in Department of Computer Application at Pranveer Singh Institute of Technology, College of Higher Education, Kanpur, India. He has 12 years of teaching experience. His research areas are big data, cloud computing, and big data as a service. He can be contacted at email: santosh.sharma.ddn@gmail.com.



Dr. Ajay Pratap    completed his masters in year 2006 and Ph.D. in year 2013 from Babasaheb Bhimrao Ambedkar Central University Lucknow. He is holding the position of Member Secretary-Research Cell, Amity Institute of Information Technology, Amity University Uttar Pradesh, Lucknow, India. He worked as an associate professor and head-computer application at Pranveer Singh Institute of Technology, Kanpur, India. He has supervised over 40 master thesis and 04 research scholars are pursuing Ph.D. under his guidance. He has also authored and coauthored over 15 conference papers and 15 research papers in various journals. His current research interests include database systems, data analysis, cloud computing, blockchain, quantum computing, and cyber security. He has chaired various technical session in different national and international conferences and received several prizes for the acknowledgment of his outstanding research and teaching performance. He can be contacted at email: chitrvasi.ajay@gmail.com.



Dr. Harsh Dev    is a professor in Department of Computer Science and Engineering, he is also holding a position of Dean Research at Pranveer Singh Institute of technology, Kanpur, India. He got his M.Sc. degree in 1995 from Lucknow University, India and Ph.D. degree in computer science in 2005 from Babasaheb Bhimrao Ambedkar University, Lucknow, India. He has 27 years of teaching experience and 21 years of research experience in the field of computer graphics, machine learning, deep learning, blockchain technologies, cryptography, software engineering, and data mining. He has published more than 66 international and national publications. Ten students have been awarded Ph.D. degree in computer science under his guidance. He is a member of editorial board of reputed journal. He is a member of Computer Society of India, Indian Science Congress. He can be contacted at email: drharshdev@gmail.com.