Computer Systems Science & Engineering
DOI:10.32604/csse.2022.022467
Article

Tech Science Press

User Centric Block-Level Attribute Based Encryption in Cloud Using Blockchains

S. Godfrey Winster[1], A. Siva Kumar[2,*] and R. Ramesh[3]

[1]Department of Computer Science and Engineering, School of Computing, College of Engineering and Technology, SRM Institute of Science and Technology, Chengalpattu, 603203, India
[2]Department of Information Technology, Sri Sai Ram Engineering College, Chennai, 600044, India
[3]Department of Electronics and Communication Engineering, Saveetha Engineering College, Chennai, 602105, India
*Corresponding Author: A. Siva Kumar. Email: siva.aaru53@gmail.com
Received: 08 August 2021; Accepted: 10 September 2021

Abstract: Cloud computing is a collection of distributed storage Network which can provide various services and store the data in the efficient manner. The advantages of cloud computing is its remote access where data can accessed in real time using Remote Method Innovation (RMI). The problem of data security in cloud environment is a major concern since the data can be accessed by any time by any user. Due to the lack of providing the efficient security the cloud computing they fail to achieve higher performance in providing the efficient service. To improve the performance in data security, the block chains are used for securing the data in the cloud environment. However, the traditional block chain technique are not suitable to provide efficient security to the cloud data stored in the cloud. In this paper, an efficient user centric block level Attribute Based Encryption (UCBL-ABE) scheme is presented to provide the efficient security of cloud data in cloud environment. The proposed approach performs data transaction by employing the block chain. The proposed system provides efficient privacy with access control to the user access according to the behavior of cloud user using Data Level Access Trust (DLAT). Based on DLAT, the user access has been restricted in the cloud environment. The proposed protocol is implemented in real time using Java programming language and uses IBM cloud. The implementation results justifies that the proposed system can able to provide efficient security to the data present in and cloud and also enhances the cloud performance.

Keywords: Cloud; blockchain; data security; ABE; block-level

1 Introduction

The growing size of organizational has challenged the organizations to maintain their data in a centralized server. Since due to the computational cost, the organizations are not able to afford a huge amount to purchase high complex data servers to store their data. The revolution and boom of the cloud environment have become a sophisticated solution for their storage problem where they can maintain their data in the cloud and can avail the services of the cloud at nominal cost. The organization has the

responsibility to maintain data integrity and provide efficient security to the customer data which has been stored in the cloud.

To ensure the integrity and privacy of the data stored in the cloud, the different access policies and privacy methods should be designed effectively. The users of the cloud are restricted based on their level namely: service level, data level, and attribute level. By maintaining the access profile based on the data, attribute, and service, the access restriction is obtained to ensure the integrity and privacy of the user's data stored in the cloud.

The blockchain is one of the modern security standards which has been used for data security in a variety of environments. The blockchain comes with several blocks and each block has three parts namely the data part, hash code, and reference part.

Fig. 1 shows the sample blockchain used in the cloud environment. The blockchain consists of three blocks and each block contains the data part, hash code, and reference part. The data part consists of the user's data which are stored in the cloud. The reference part is used to identify the next block of data. The hash code block is used to encrypt the data from the block.

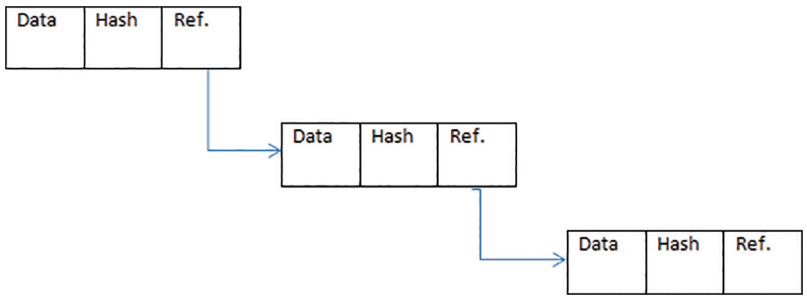

Figure 1: Sample blockchain

Fig. 2, gives the blockchain model used for the cloud data security, where the user's access is verified and data accessed is encrypted with blockchain encryption and decrypted mechanism with the hash code available in each block.

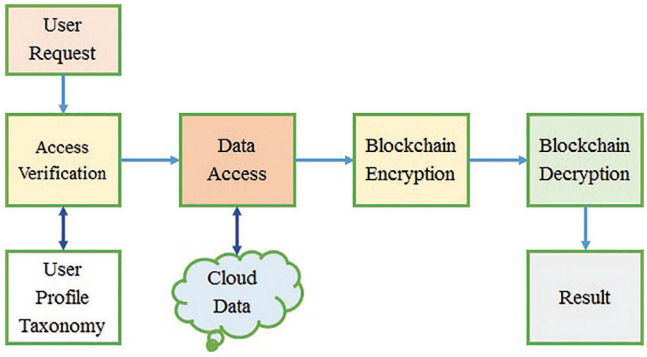

Figure 2: Example cloud blackchain model

The proposed model restricts the user access based on Data Level Access Trust (DLAT) and data security is provided using the User-Centric Block Level Attribute-Based Encryption (UCBL-ABE) scheme. Attribute-based access control scheme for cloud frameworks enormously works on the access management. We use Blockchain innovation to record the appropriation of attributes to stay away from

single point failure and information altering. The entrance control measure has likewise been enhanced to address the issue of high efficiency and lightweight calculation for cloud security. Security and performance analysis show that our plan could successfully oppose multiple attacks and be efficiently carried out in frameworks. Where as trust level based data storage and trust level based information access control arrangement which changes the control interaction of data storage and information access. The introduced course of action enables straightforward data dealing with subject to given out trust levels to limit game plans in a distributed data storage environment and the arranged affectability level of the data to be taken care. The rest of the manuscript is organized as follows.

Section 2, discusses the details of the proposed UCBL-ABE scheme and Section 3 provides the evaluation results on the proposed UCBL-ABE. Finally, Section 4 provides the conclusion and future work.

Motivated from all these observations in this paper an efficient user-centric block-level Attribute-Based Encryption (UCBL-ABE) scheme is proposed to provide the efficient security of cloud data in the cloud environment. The observations of this literature survey are that most of the existing systems have suffered to achieve higher performance in terms of security and energy-efficient in nature. Motivated from all these observations in this paper an efficient user-centric block-level Attribute-Based Encryption (UCBL-ABE) scheme is proposed to provide the efficient security of cloud data in the cloud environment. Moreover, the proposed system provides efficient privacy with access control to the user access according to the behavior of cloud users using Data Level Access Trust (DLAT).

2 Related Works

Various approaches have been proposed for providing efficient cloud data security using the Blockchain technique. Some of the techniques are discussed as follows.

The new robust key pre-distribution [1] scheme has been proposed to provide cloud security to the user's data stored in the cloud environment. Their proposed system provides better security during data communication without compromising network security. The square matrix of a pool of keys is generated based on eigenvalue and eigenvectors. Their simulation results justify that the proposed system significantly reduces the overhead and provides secure data communication to the nodes of WSN.

ETARP [2] has been proposed to provide security with better energy optimization in WSN and this routing protocol is mainly used in unfriendly environments such as a battlefield. The route selection in the proposed routing protocol is carried out based on the utility theory. The key idea of this routing protocol is it selects the optimized route based on the maximum utility. The advantage of this routing protocol is it provides energy-efficient trust-based secure routing in the network. The limitations of this protocol are it has more overhead when it is compared to other state of art protocols in WSN.

In [3] authors have proposed a system that can improve the network efficiency and precision in WSN by using a two-phase distributed PSO algorithm to solve the flip ambiguity problem. In the proposed system, by using the boundary box method, the initial search space is defined. The main role of the refinement phase is to carry out error corrections that occur due to flip ambiguity.

In [4] authors employ a multi-objective particle swarm optimization localization algorithm (MOPSOLA) to identify the localization in WSN. The proposed algorithm uses the space distance constraint and the geometric topology as multi-objective functions. The advantage of this system is its localization accuracy. The limitations are its computation overhead.

In this system [5] authors use Blockchain technology to award the nodes who stores more data in WSN. The proposed system has two Blockchains. The first Blockchain is used for data storage and another one is used for access control. The advantage of this system is it provides efficient access control for the nodes of WSN.

A Blockchain-based Contractual routing (BCR) [6] has been designed for IoT devices to provide efficient distributed authentication. The proposed system discovers an optimal route to transmit the data to the destination node. The advantages of this system are its route reliability and limitations are its occurrence of computational overhead.

A survey [7] has been carried out by the authors to shows how Blockchain technology has improved the security of IoT devices. In this survey, the various challenges of IoT are addressed.

A novel trust-based secured routing [8] is proposed by the authors for energy-efficient routing in WSN using Blockchain technology. In the proposed scheme, the routing information is obtained from the Blockchain which is available in the network by using reinforcement learning to identify the most efficient links in the network.

The author proposed UC protocol [9] where he has employed Blockchain technology to provide security to IoT-based cloud systems. The advantages of their approach are their security to the IoT devices and the limitations are their computational and communication overhead.

In [10] author proposed edge computing-based peer-to-peer Blockchain technology to provide efficient security to the devices in IoT. The proposed Blockchain technology provides data integrity by using anonymous user authentication. The limitations are it is not lightweight in nature.

In [11] author has proposed a security mechanism in the Blockchain that can provide security to the bit coins in the IoT environment. The advantages of their system are their energy efficiency and limitations are it is vulnerable to various types of attacks in IoT-based Blockchain technology.

In [12] author has proposed stochastic models to detect and verify the probabilities of occurrence of errors in the IoT-based Blockchain network. The advantage of this system is its accurate error detection which is occurred in the network. The limitations are its overhead involved during the error detection in the network.

In [13] author has proposed a system that can able to detect malicious nodes in the network by using Blockchain Trust Model (BTM). The proposed system constructs a Blockchain data structure to identify and detect malicious nodes. The advantages of their system are better detection accuracy of malicious nodes and limitations are its overhead involved in communication and computation

The author proposed cryptographic checksums signatures [14] mechanism to detect and recover the attacks in WSN. The proposed system provides data integrity with efficient anonymous user authentication to detect the malicious nodes in the network. The limitations are the malicious nodes detection is not accurate and it has overhead in terms of computation.

In [15] authors have proposed a signcryption mechanism based on offline/online methods to provide efficient authentication to the devices in the IoT environment. The advantages system is secure data transmission to the medical server and efficient data access by using the remote method. The limitations are its overhead due to computation and communication.

In [16], the author presents a nonlinear cooperative control algorithm based on game theory and Blockchain. Here, a new model is proposed for the automatic processing and management of data in heterogeneous distributed wireless sensor networks stored in a Blockchain. The advantage of this model it provides interoperability with better security in WSNs. The limitations are its overhead in terms of computation and communication.

In [17] author has proposed the system which can able to detect malicious nodes attack by using Proof of Authority (PoA) in the network. The advantage of this system is it provides efficient node authentication. The limitations are the malicious node detection is not accurate.

In [18–22] authors have provided security by designing Blockchain-based distributed collocation storage architecture in WSN. They have used an asymmetric signature and trust [23–26] for providing efficient security in WSN. The advantages are its better security and the limitations are its both computational and computational overhead.

In [27–30] authors proposed a trust model based on fuzzy logic for proving trust-based security in WSN. The advantage of this system is the accurate detection of malicious nodes in the network. The limitations are less accuracy of malicious node detection and it has overhead in terms of communication and computation [31–35].

The observations of this literature survey are that most of the existing systems have suffered to achieve higher performance in terms of security and energy-efficient in nature [36–40]. Motivated from all these observations in this paper an efficient user-centric block-level Attribute-Based Encryption (UCBL-ABE) scheme is proposed to provide the efficient security of cloud data in the cloud environment [41,42]. Moreover, the proposed system provides efficient privacy with access control to the user access according to the behavior of cloud users using Data Level Access Trust (DLAT).

3 Dynamic User Centric Block Level ABE Model

The proposed security model in the cloud computing environment maintains profiles of users in form of taxonomy. Attribute-based encryption (ABE) calculation acknowledges adaptable and fine-grained admittance control, countless clients buy in or withdraw the various administrations habitually in the cloud, which takes a huge expense for membership management. The taxonomy contains information related to the access constraints of various users and the users are classified under various groups based on the different taxonomy. According to the taxonomy, the user's request is processed towards access control and data encryption with blockchain. Fig. 3 gives the architecture of the Proposed UCBL-ABE Scheme in a detailed manner. It consists of four phases namely DLAT Access Restriction, BlockChain Generation phase, Hash Code Generation, Dynamic Block-Level Encryption.

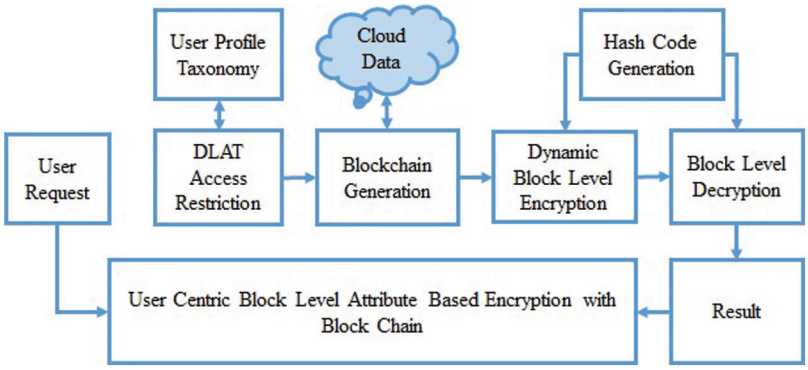

Figure 3: Architecture of proposed dynamic user centric block level scheme

4 DLAT Access Restriction

The cloud environment has the number of users who can access the service and data present in the cloud. Consider, there exists K number of data points and each has N number of attributes. Similarly, if there exists S number of users in the environment, then not all the users of the set S have access to all the data points and attributes present in the cloud. The cloud will have various data belongs to different users and customers. It is necessary to restrict the users from accessing the other data which have no access for them. It can be enforced by the DLAT (Data Level Access Trust) based access restriction. According to this, whenever a user requests

access to the specific data, then the profile taxonomy can be used in verifying the access privilege for the user based on all the attributes required. Similarly, the behavior of the user in accessing the data has been used in measuring the DLAT measure. According to the value of DLAT, the access restriction is performed.

Consider the data requested is D, then the features present in the data D has been identified using the below equation.

$$\text{Feature List Fl} = \sum Features \in D \tag{1}$$

Now according to the profile taxonomy PT, the number of attributes to which the user has access is identified as follows:

$$\text{Access Feature List AFl} = \int_{i=1}^{size(PT)} \int_{i=1}^{size(Fl)} Fl(j) \in PT(i).User == U \tag{2}$$

where, U is the User id

Now, the trust of user in accessing the data is measured by measuring the earlier access.

$$\text{Previous Access Trust PAT} = \frac{\sum_{i=1}^{size(Trace)} Trace(i).User == U \;\&\&\; Trace(i).Access = Complete}{\sum_{i=1}^{size(Trace)} Trace(i).User == U} \tag{3}$$

Now the value of DLAT is measured as follows:

$$\text{DLAT} = \frac{size(AFL)}{Size(FL)} \times PAT \tag{4}$$

Based on DLAT the access restriction is performed. If DLAT value is high, then the users have been granted permission to access the data in the cloud else, the users are not given the privilege to access the data in the cloud. The Pseudo Code of DLAT Access Restriction is given in Algorithm 1.

Algorithm 1: Pseudo Code of DLAT Access Restriction:

Input: Trace T, Request R, Profile Taxonomy PT

Output: Boolean

Begin

Read T, R, PT. // where Trace T, Request R, Profile Taxonomy PT

Identify data requested D = $\int Data \in R$ // give interval function

Identify features required in Fl using the expression: Feature List Fl = $\sum Features \in D$

Identify features to which access available using the expression: Access Feature List AFl = $\int_{i=1}^{size(PT)} \int_{i=1}^{size(Fl)} Fl(j) \in PT(i).User == U$

Compute previous access trust PAT value using equation: Previous Access Trust PAT = $\frac{\sum_{i=1}^{size(Trace)} Trace(i).User == U \;\&\&\; Trace(i).Access = Complete}{\sum_{i=1}^{size(Trace)} Trace(i).User == U}$

Compute DLAT measure using equation: DLAT = $\frac{size(AFL)}{Size(FL)} \times PAT$

(continued)

Algorithm 1: (continued)

If DLAT > Th then

Return true.

Else

Return false.

End

Stop

The access restriction with DLAT algorithm is performed according to the DLAT measure which is computed for the user request given. Based on the value of DLAT, the method performs access restriction for the user.

5 Block Chain Generation

The Blockchain generation scheme is executed when the data required has been extracted by accessing the cloud. When user access is granted, the method accesses the data and obtains the required data. From the data, the method extracts the attributes to which the user has access. Now, using the attribute taxonomy AT, the method selects a unique encryption scheme and key from the scheme and key sets. According to with encryption scheme and key generated, the data attributes are encrypted. Moreover, the method generates a random number R from the group Z*P, which represents the number of blocks to be generated in the chain. According to the value of R, the method generates the block chain and split the data into R number of blocks. Generated Blockchain and data blocks are used to perform dynamic block-level encryption and decryption. The algorithm for the Blockchain generation is given in algorithm 2.

Algorithm 2: Pseudo Code of Block Chain Generation:

Input: Data D, Access Feature List Afl, Attribute Taxonomy AT

Output: Block Chain BC, Data blocks Dbl

Begin

Read D, AFL, AT. // Data D, Access Feature List Afl, Attribute Taxonomy AT

$$\text{Extract Features Fes} = \int_{i=1}^{size(D)} \sum D(i) \in Afl \tag{5}$$

For each feature f of fes

DO

$$\text{Select Encryption Scheme Es} = \int_{i=1}^{size(AT)} Random(AT(i).F == F,\ AT(i).Schemes) \tag{6}$$

$$\text{Select encryption key Ek} = \int_{i=1}^{size(AT)} Random(AT(i).F == F,\ AT(i).Kes) \tag{7}$$

(continued)

Algorithm 2: (continued)

Fes = Encrypt(f, Es, Ek)

End For

Encrypted data (Ed) = Merge (Fes).

$$\text{Random R} = \int Random(3,\ 10) \tag{8}$$

$$\text{Data list Dbl} = \int Split(Ed,\ R) \tag{9}$$

Initialize Block Chain (BC).

Generate Dl (NB) // where NB is Number of Blocks in the block chain.

$$\text{BC} = \int_{i=1}^{size(Dl)} \sum(Blocks \in BC) \cup GenerateBlock \tag{10}$$

END

The Algorithm 2 represents how the block chain is generated. The method encrypts each attribute with different encryption scheme and key. Further, the data has been split into number of blocks. According to the number of block a block chain is generated.

6 Hash Code Generation

Blockchain hash every exchange prior to packaging them together into blocks. Hash pointers connect each block to its predecessor, by holding a hash of the information in the past block. Since each block connects to its predecessor, information in the Blockchain is changeless. The hashing function implies that an adjustment of any exchange will deliver a completely unique hash, which will change the hashes of every single ensuing blocks. Each block of the chain contains data and hash code concerning the next block. From the hash code, the receiver can obtain the code to identify the encryption key used. By identifying the key, the receiver can decrypt the cipher text to get the original data. In the proposed system it uses a key set that contains the number of keys which has been used for data encryption. The selection of keys is performed according to the prime and polynomial scheme. The method uses a character set that has several alphabets and characters. The key set and character set are distributed to the user in the initial stage itself. Now, first, the method generates a random number according to the size of the character set used. Now consider, the character set Cs is used which has N number of characters then, the hash character is generated as follows:

Hash character Hc = $\int Random(1,\ size(Cs))$

Tthe character set Cs is defined as follows

Cs = {x, b, c, d, u, v, w, y, z, a, e, f, I, h, j, l, m, o, p, q, n, r, s, t, k, Z, H, J, K, M, R, P, Q, S, T, U, L, M, O, N, A, B, C, D, E, F, I, G, V, W, X, Y, @, #, $, %, ∧, &, ! , *}

Now, the random number of generated is 8, then the hash character is y, then the method computes the ascii value of the character. Say if the ascii value of y is 36, then the method verify the prime factor of the value y. now the hash code is generated as follows:

R = generate random number upto the size of key set.

Hash code = y+R

If the value of R is 12 then the hash code is as follows:

Hash code = y12.

The algorithm for the hash code generation is explained in the Algorithm 3.

Algorithm 3: Pseudo Code of Hash Code Generation:

```
Input: Character set Cs, Key set Ks, Data D
Output: Hash Code Hc, Encoded Text ET
Begin
    Read Cs, Ks, D. // Cs, Key set Ks, Data D
    R1 = ∫ Random(1, size(Cs)) // add limit
    Character y = Cs(R1)
    If y (prime)
   then
      Generate Hash code = y + Random (size (keyset))
     Encrypted data ET = Encrypt (Keyset (Ascii (y)+ Random(size(keyset))
   Else
     Hash code = Ascii(y) + Random(size(keyset))
     Encrypted data ET = Encrypt (Keyset(Ascii(y) − Random(size(keyset))
   End
END
```

The Generated hash code is added to the block considered and encrypted data is added to the block. According to the hash code the user can identify which key should be used to decrypt the text to obtain original data.

6.1 Dynamic Block Level Encryption

The block-level encryption is performed when the algorithm is given with the data blocks generated. For each data block, the method generates a hash code and encrypts the data with the key identified in the hash code generation phase. The encrypted text is generated in the hash code generation phase added to the block and reference is generated to the next block of data. Generated blockchain with data has been populated as result to the user. The algorithm for the dynamic block-level encryption is given in Algorithm 4.

Algorithm 4: Pseudo Code of Block Level Encryption:

```
Input: Data blocks Dbl, Block Chain BC
Output: BC
Begin
    Read Dbl, BC.
```

(continued)

Algorithm 4: (continued)

For each (block bl)

Do

BC = $\int_{i=1}^{size(BC)} BC(i) = HashCodeGeneration(bl)$

End

END

The pseudo code of algorithm 4 provides how the block level encryption is performed in IoT based block chain for the cloud environment.

6.2 Dynamic Block Level Decryption

The decryption of data to obtain the original data from the blockchain is performed in this stage. The method is given with the blockchain which contains the number of blocks and each has data, hash code, and reference unit. First, the method reads the blockchain and for each block, the hash code is identified and the encoded text is taken. The hash code is split with character and numeric. Now according to the character, the ASCII value is generated and identified for prime value. According to the status of the prime factor, the method computes the index of the key to be selected. Based on the key identified, the data has been decrypted to obtain the original text. Algorithm 5 gives the Pseudo Code of Block Level Encryption.

Algorithm 5: Pseudo Code of Block Level Encryption:

Input: Data blocks Dbl, Block Chain BC

Output: Decrypted Data Dd

Begin

Read Dbl, BC.

For each block bl

Hash Code Hc = $\int hashcode \in bl$

Character C = $\int Substring(Hc,\ 1)$

Characters C1 = $\int Substring(Hc,\ 2,\ length(hc))$

P = Ascii©

If P is Prime

Then

Index = p+value(C1)

Dd = Decrypt(bl.Data, Keyset(index))

Else

Index = p-value(C1)

Dd = Decrypt(bl.Data, Keyset(index))

End

End

END

Algorithm 5 gives pseudo code that represent the working of block level decryption algorithm which decode the hash code and identify the key index to be used for decrypt the data to obtain original data.

7 Experimental Results

The proposed role-based class level access trust block chain algorithm has been implemented and evaluated for its performance. The proposed CLAT algorithm is hardcoded in advanced java. The simulation parameters used in the proposed system is given in Tab. 1.

Table 1: Details of simulation

Parameter	Value
Tool used	Advanced Java, IBM Cloud
Number of users	200
No of classes	5
No of features	60

Fig. 4 gives the performance in security has been measured for the proposed UCBL-ABE algorithm under varying number of users and compared with the values of other methods. The proposed UCBL-ABE algorithms have achieved higher performance in terms of security compared to other methods.

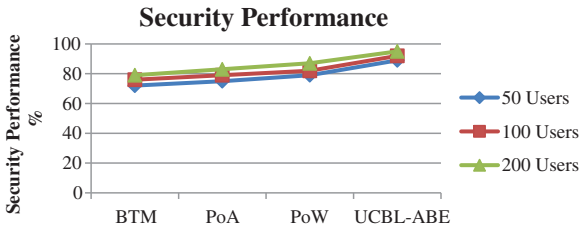

Figure 4: Performance in security *vs.* no of users

Fig. 5 gives the achievement in terms of the throughput performance has been measured at varying number of users and compared with the result of other methods. The proposed UCBL-ABE algorithms have achieved higher throughput performance compare to other methods.

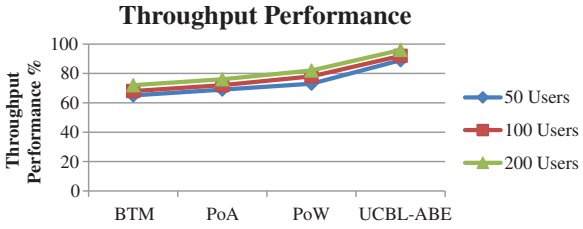

Figure 5: Performance on throughput achievement *vs.* no of users

Fig. 6 gives the performance in encryption and decryption has been measured at different number of users and compared with the values of other methods. The proposed UCBL-ABE algorithms have produced higher performance than other methods.

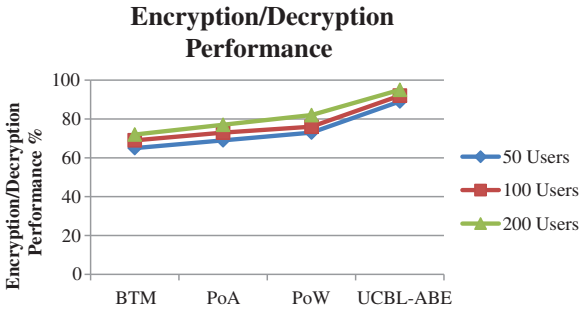

Figure 6: Performance in encryption/decryption *vs.* no of users

Performance in time complexity has been measured at varying number of users and presented in Fig. 7. The proposed UCBL-ABE algorithms have produced less time complexity than other methods.Through intensive examination conveyed and the outcomes acquired for each model, Compared to different models, this proposed UCBL-ABE model gives higher throughput and performance.

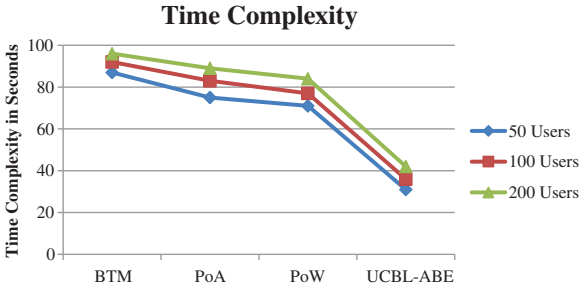

Figure 7: Performance in time complexity *vs.* no of users

8 Conclusion and Future Work

This paper proposes a novel user-centric block-level attribute-based encryption scheme with a Blockchain towards cloud data security. The execution results justifies that the proposed framework can ready to give efficient security to the data present in and cloud and furthermore improves the cloud execution. The proposed technique works on the performance of information encryption and decoding. Additionally, the technique works on the performance of data security. The method maintains the number of data and taxonomy for the users and attributes. In the proposed system, whenever a user requests the data, the user has been measured for Data level access Trust (DLAT) based on which the user access has been restricted. Moreover, the data extracted from the cloud has been encrypted with block-level encryption and added to the block of the chain according to the hash code generation. The hash code generation is performed according to the index of the key in the key set and the character selected from the character set. Encoded data and hash code generated are added to the block of the chain. Similarly, at the decryption, the prime value of the character present in the hash code of the block is used to find the index of the key to performing data decryption. The proposed method improves the performance of data encryption and decryption. Also, the method improves the performance of data security.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] Z. Zheng, S. Xie, H. N. Dai, X. Chen and H. Wang, "Blockchain challenges and opportunities: A survey," *International Journal of Web and Grid Services*, vol. 14, no. 4, pp. 352–375, 2018.

[2] P. Gong, T. M. Chen and Q. Xu, "ETARP: An energy efficient trust-aware routing protocol for wireless sensor networks," *Journal of Sensors*, vol. 2015, pp. 1–5, 2015.

[3] N. Binti, M. Ahmad, Z. Mahmoud and R. M. Mehmood, "A pursuit of sustainable privacy protection in big data environment by an optimized clustered-purpose based algorithm," *Intelligent Automation & Soft Computing*, vol. 26, no. 6, pp. 1217–1231, 2020.

[4] Z. Sun, L. Tao, X. Wang and Z. Zhou, "Localization algorithm in wireless sensor networks based on multiobjective particle swarm optimization," *International Journal of Distributed Sensor Networks*, vol. 2015, pp. 1–9, 2015.

[5] R. Yongjun, L. Yepeng, J. Sai, S. Arun Kumar and W. Jin, "Incentive mechanism of data storage based on blockchain for wireless sensor networks," *Mobile Information Systems*, vol. 2018, pp. 1–10, 2018.

[6] Y. Yu, Y. Li, J. Tian and J. Liu, "Blockchain-based solutions to security and privacy issues in the internet of things," *IEEE Wireless Communications*, vol. 25, no. 6, pp. 12–18, 2018.

[7] N. Islam, F. Farhin, I. Sultana, M. S. Kaiser, M. S. Rahman *et al.,* "Towards machine learning based intrusion detection in iot networks," *Computers, Materials & Continua*, vol. 69, no. 2, pp. 1801–1821, 2021.

[8] B. Mi, Y. Weng, D. Huang, Y. Liu and Y. Gan, "A novel PoW scheme implemented by probabilistic signature for blockchain," *Computer Systems Science and Engineering*, vol. 39, no. 2, pp. 265–274, 2021.

[9] D. Cao, B. Zheng, B. F. Ji, Z. B. Lei and C. F. Feng, "A robust distance-based relay selection for message dissemination in vehicular network," *Wireless Networks*, vol. 26, no. 3, pp. 1755–1771, 2020.

[10] R. Qiao, S. Dong, Q. Wei and Q. Wang, "Blockchain based secure storage scheme of dynamic data," *Computer Science*, vol. 45, pp. 57–62, 2018.

[11] J. Wang, Y. Q. Yang, T. Wang, R. S. Sherratt and J. Y. Zhang, "Big data service architecture: A survey," *Journal of Internet Technology*, vol. 21, no. 2, pp. 393–405, 2020.

[12] L. Gong, B. Yang, T. Xue, J. Chen and W. Wang, "Secure rational numbers equivalence test based on threshold cryptosystem with rational numbers," *Information Sciences*, vol. 466, pp. 44–54, 2018.

[13] F. Li, R. Xie, Z. Wang and L. Guo, "Online distributed IoT security monitoring with multidimensional streaming big data," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4387–4394, 2020.

[14] J. Y. Zhang, S. Q. Zhong, T. Wang, H. C. Chao and J. Wang, "Blockchain-based systems and applications: A survey," *Journal of Internet Technology*, vol. 21, no. 1, pp. 1–14, 2020.

[15] J. Iqbal, A. I. Umar, N. Amin and A. Waheed, "Efficient and secure attribute-based heterogeneous online/offline signcryption for body sensor networks based on blockchain," *International Journal of Distributed Sensor Networks*, vol. 15, no. 9, pp. 1–23, 2019.

[16] A. S. Kumar, S. G. Winster and R. Ramesh, "Efficient sensitivity orient blockchain encryption for improved data security in cloud," *Concurrent Engineering*, vol. 29, no. 3, pp. 249–257, 2021.

[17] J. Gubbi, R. Buyya, S. Marusic and M. Palaniswami, "Internet of things (IoT): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, 2013.

[18] Y. Zhou, T. Liu, F. Tang and M. Tinashe, "An unlinkable authentication scheme for distributed IoT application," *IEEE Access*, vol. 7, pp. 14757–14766, 2019.

[19] Z. Q. Xia, J. J. Tan, J. Wang, R. L. Zhu, H. G. Xiao and A. K. Sangaiah, "Research on fair trading mechanism of surplus power based on blockchain," *Journal of Universal Computer Science*, vol. 25, no. 10, pp. 1240–1260, 2019.

[20] Y. S. Zhou, X. W. Long, L. J. Chen and Z. Yang, "Conditional privacy-preserving authentication and key agreement scheme for roaming services in VANETs," *Journal of Information Security and Applications*, vol. 47, pp. 295–301, 2019.

[21] B. Varghese and R. Buyya, "Next generation cloud computing: New trends and research directions," *Future Generation Computer Systems*, vol. 79, pp. 849–861, 2018.

[22] V. R. Prabha and P. Latha, "Fuzzy trust protocol for malicious node detection in wireless sensor networks," *Wireless Personal Communications*, vol. 94, no. 4, pp. 2549–2559, 2017.

[23] W. Zhang, S. Zhu, J. Tang and N. Xiong, "A novel trust management scheme based on dempster–Shafer evidence theory for malicious nodes detection in wireless sensor networks," *Journal of Supercomputing*, vol. 74, no. 4, pp. 1779–1801, 2018.

[24] T. G. Rodrigues, K. Suto, H. Nishiyama and N. Kato, "Hybrid method for minimizing service delay in edge cloud computing through VM migration and transmission power control," *IEEE Transactions on Computers*, vol. 66, no. 5, pp. 810–819, 2017.

[25] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen and B. C. Ooi, "Untangling blockchain: A data processing view of blockchain systems," *IEEE Transactions on Knowledge and Data Engineering*, vol. 30, no. 7, pp. 1366–1385, 2018.

[26] X. F. Wang, L. Wang, Y. H. Zheng and J. Wang, "An event-driven plan recognition algorithm based on intuitionistic fuzzy theory," *Journal of Supercomputing*, vol. 74, no. 12, pp. 6923–6938, 2018.

[27] Y. Jiang, M. H. Zhao, C. Q. Hu, L. L. He, H. T. Bai and J. Wang, "A parallel Fp-growth algorithm mining world ocean atlas data using multi-core CPU," *Journal of Supercomputing*, vol. 75, no. 2, pp. 732–745, 2019.

[28] R. Roman, J. Lopez and M. Mambo, "Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges," *Future Generation Computer Systems*, vol. 78, pp. 680–698, 2018.

[29] S. Choy, B. Wong, G. Simon and C. Rosenberg, "A hybrid edge-cloud architecture for reducing on-demand gaming latency," *Multimedia Systems*, vol. 20, no. 5, pp. 503–519, 2014.

[30] J. Xu, Y. J. Zhang, K. Y. Fu and S. Peng, "SGX-Based secure indexing system," *IEEE Access*, vol. 7, pp. 77923–77931, 2019.

[31] S. Wei, J. Wang, R. Yin and J. Yuan, "Trade-off between security and performance in block ciphered systems with erroneous ciphertexts," *IEEE Transactions on Information Forensics & Security*, vol. 8, no. 4, pp. 636–645, 2013.

[32] Y. S. Khiabani, S. Wei, J. Yuan and J. Wang, "Enhancement of secrecy of block ciphered systems by deliberate noise," *IEEE Transactions on Information Forensics & Security*, vol. 7, no. 5, pp. 1604–1613, 2012.

[33] M. Suresh and M. Neema, "Hardware implementation of blowfish algorithm for the secure data transmission in internet of things," *Procedia Technology*, vol. 25, pp. 248–255, 2016.

[34] J. Kim and S. Nepal, "A cryptographically enforced access control with a flexible user revocation on untrusted cloud storage," *Data Science and Engineering*, vol. 1, no. 3, pp. 149–160, 2016.

[35] O. A. Mahdi, Y. R. B. Al-Mayouf, A. B. Ghazi, A. W. A. Wahab and M. Y. I. B. Idris, "An energy-aware and load-balancing routing scheme for wireless sensor networks," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 12, no. 3, pp. 1312–1319, 2018.

[36] C. Gong, J. Liu, Q. Zhang, H. Chen and Z. Gong, "The characteristics of cloud computing," in *Proc. of the Int. Conf. on Parallel Processing Workshops*, San Diego, CA, USA, pp. 275–279, 2010.

[37] M. Humayun, M. Niazi, N. Z. Jhanjhi, M. Alshayeb and S. Mahmood, "Cyber security threats and vulnerabilities: A systematic mapping study," *Arabian Journal for Science and Engineering*, vol. 45, no. 1, pp. 3171–3189, 2020.

[38] A. Ostad, H. Arshad, M. Nikooghadam and D. Abbasinezhad-Mood, "Three party secure data transmission in IoT networks through design of a lightweight authenticated key agreement scheme," *Future Generation Computer Systems*, vol. 100, pp. 882–892, 2019.

[39] Z. I. Saleh, H. Refai and A. Mashhour, "Proposed framework for security risk assessment," *Journal of Information Security*, vol. 2, no. 2, pp. 85–90, 2011.

[40] K. Sahu and R. Shree, "Software security: A risk taxonomy," *International Journal of Computer Science and Engineering Technology*, vol. 7, no. 3, pp. 36–41, 2015.

[41] S. Y. Lim, P. T. Fotsing, A. Almasri, O. Musa, M. L. M. Kiah *et al.*, "Blockchain technology the identity management and authentication service disruptor: A survey," *International Journal on Advanced Science, Engineering and Information Technology*, vol. 8, no. 4–2, pp. 1735–1745, 2018.

[42] 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.