Rivista Italiana di Filosofia Analitica Junior Vol 14, No. 1 (2023)
ISSN: 2037-4445

Adaptive Attribute-Based Encryption on Blockchain with Enhanced Authentication Mechanism

Neeraj[1] (Research Scholar)
Computer science and engineering
Deenbandhu chhotu ram university of Science and Technology
Sonepat, India
neeraj.schcse@dcrustm.org

Anita Singhrova[2] (Professor)
Computer science and engineering
Deenbandhu chhotu ram university of Science and Technology
Sonepat, India
nidhianita@gmail.com

Abstract— Authentication is an essential component of a system since it serves in many circumstances as both the first and the last line of protection. Authentication makes it possible to stop users who are not approved from accessing the system. A novel Adaptve Attribute Based Encrytion (ABE) encryption using Threshold ABE, Multi Factor Authentication (MFA) and Revocation mechanism is utilized to add a layer of security to the authentication process as part of this plan. Proposed ABE encryption has been used to add a layer of security to the authentication process. Further, the simulation results of the proposed ABE are compared with ABE & Rivest Cipher 4 (RC4) in terms of cost of execution & transaction packet delivery rate & packet loss rate, and encryption & decryption execution.

Keywords—: ABE encryption scheme, Blockchain, Multi Factor Authentication, Revocation, Adaptive ABE

Introduction

User authentication has been a foundational component of information systems for the better part of three decades. The password-based method of user authentication is by far the most used and widespread practise in current computer systems. Nevertheless, the human cognitive ability to recall both the user ID and the password is a critical component of modern user authentication. The development of the Internet has forced users to generate several passwords for different systems, presenting them with the difficulty of remembering all of these passwords. This load is made worse by the fact that users are more likely to forget their passwords. Password-based user authentication has a number of problems, one of which is that it is susceptible to attacks that include cracking or leaking passwords. Authentication of identification at a consistent level is essential in order to address these limitations. Users of the system are given an easy and convenient approach to authenticate their identities whenever the system uses consistent identity authentication. Users are needed to provide a user ID and password in order to log in to a trusted authentication server, and then they must log in to any third parties that use a trusted authentication system. The difficulty is that technological failures and denial of service assaults, both of which can lead to inefficiency on the part of the trusted third party. The planning and execution of an authentication system that is friendly to users and does not rely on a third party to authenticate users is still a difficult task [1].

The proliferation of information technology results in the daily production of a massive amount of data, which is difficult for individuals to keep locally because to the complexity of the data involved. The use of cloud storage is widely regarded as the most cost-effective approach to resolving this issue. In spite of this, there is likely to be some sensitive data that needs to be uploaded, and there is no guarantee that the cloud servers can be trusted. Uploading the encrypted data to the cloud as a potential method to protect the user's privacy is therefore recommended. However, existing

encryption algorithms are not ideal for flexible data sharing or fine-grained access control. As a result, Sahai and Waters proposed a new cryptographic fundamental that they called attribute-based encryption (ABE). In this kind of system, the only person who has the correct key to decrypt the associated ciphertext is the one whose attribute set is the one that satisfies the access policy.
The classic ABE schemes, on the other hand, have an issue with efficiency. This means that the computational cost (especially the decryption cost) grows linearly with the complexity of the access policy. This makes it difficult to apply these schemes in practise, such as when they are implemented in devices with limited resources.
Blockchain is the type of system that may enable entities create trust relationships with one another even if they did not trust each other previously. As a result, it only makes sense to deploy blockchain technology to provide the desired level of verifiability. A verifiable outsourced computation protocol with timely delivery of results and equitable payment was considered. They accomplished this by making use of Bitcoin. The most important aspect of this protocol is that all participants should make initial deposits, which will be refunded to them if the verification procedure is successful.
In the proposed research, user authentication has been enhanced by using Adaptive ABE, an enhanced ABE algorithm using Multi Factor Authentication (MFA) and Revocation mechanism. This method enhances the security of the system because Multi-factor authentication is an extra security measure that prevents unauthorised users from gaining access to a blockchain by acting as a barrier between the blockchain and the user. The revocation mechanism allows the a user to revoke access to specific attributes of another user if necessary, increasing the system's flexibility.

Literature Review

ABE protocols are proposed as the basis for a unique privacy-preserving blockchain architecture [22]. It was the first way to combine new encryption with blockchains successfully. Because of its malleability and fine-grained design, the encryption makes it possible to exercise control over and use transaction information according to a wide range of criteria. The proposed model made changes so that the blockchain protocol works to conform to the ABE methodology without jeopardizing the essential security features of the Blockchain. The suggested model's privacy and security are assessed, and methods for mitigating specific threats discovered are devised. The research reveals that feature-dependent encryption would be beneficial to the blockchain in terms of achieving privacy while also reducing the amount of computational overhead. Using blockchain technology to enable secure data sharing across numerous distributed parties has the goal of the proposed architecture [22]. Those transformed the data sharing issue into machine learning (ML) by incorporating privacy-preserved federated knowledge.
Numerous user authentication systems have been presented in recent times [2-18]. In their proposal for key management and user authentication in e-health systems, Wong et al. [2] made use of the characteristics of hash functions.
However, Tseng et al. [3] demonstrated that their techniques were susceptible to assaults of replay, forgeries, and password guessing. In addition, Lee [4] discovered that the computational cost of Wong et al.'s method was excessively high, making it unsuitable for implementation on lightweight devices. Das [5] proposed a practical method of two-factor authentication for the internet of things that enhanced efficiency in terms of the amount of processing effort required. Unfortunately, Huang et al. [6] reported that Das's technique was incapable of fending against assaults such as password guessing, user impersonation, and other similar threats.
In addition, Das's plan does not make it possible for users to remain anonymous.
Following this, Yoo et al. [7] stated that the authentication technique proposed by Huang et al. was susceptible to insider and parallel session assaults, and that it was unable to accomplish mutual authentication. Subsequently, Das [8] further asserted that the system proposed by Li et al. [9] was unable to offer strong authentication during the authentication process and was unable to successfully conduct password updating locally. In the meantime, An [10] asserted that Das's [8] plan was riddled with security flaws, including a susceptibility to user impersonation attacks, server-masquerading attacks, insider assaults, and other such attacks. In addition to that, a [10] offered an improved

version of the technique. Unfortunately, Khan and Kumari [11] pointed out that impersonation assaults and password-guessing attacks could make this approach ineffective.

The goal of the novel key management and user authentication approach that Chang et al. [12] presented for e-health systems was to ensure the confidentiality of users. Every time authentication is carried out, this system has the capability of bringing a secret value that is stored on a smart card up to date. However, Das and Goswami [13] pointed out that their approach had security flaws, such as vulnerability to insider attacks and man-in-the-middle attacks, and did not provide adequate authentication. These flaws made their scheme susceptible to attacks. Arshad and Nikooghadam [14] suggested a method of anonymous authentication that uses three different factors. They asserted that the system may offer more reliable and secure authentication while also protecting the user's privacy. After that, Lu et al. [15] came up with the idea of enhancing Arshad et al.'s technique by utilising an elliptic curve cryptosystem as an additional security measure. An anonymous two-factor authentication technique based on ECC in a random oracle model was presented by Islam and Khan [16]. They provided evidence that their method was foolproof when subjected to the computational Diffie-Hellman dilemma. Sadly, Zhang and Zu [17], Feng et al. [18] indicated that Islam and Khan's [16] approach had security weaknesses such as vulnerability to server-spoofing attacks and off-line passwordguessing attacks. These faults made the technique susceptible to attacks.

Because the authentication of the aforementioned schemes relies primarily on flexible security models, and because these schemes are required in repeated contacts between users and medical service centres, this will be a significant barrier for mobile users to overcome in order to get efficient access to the data centre. In addition, each of these strategies is predicated on the idea that there is a reliable authority centre, which leaves the networks open to the possibility of suffering harm to the database that is kept and managed by the authority centre. Blockchain technology makes it possible to authenticate users across several data centres [18] and provides an effective means of maintaining data integrity.

The comparison of encryption algorithms is summarized in table 1. The comparison of functionalities is depicted in Table 2

TABLE I. COMPARISON OF ENCRYPTION ALGORITHMS

Author	**The technique used (Cryptography (C) or Steganography (S))**	**Algorithm used**	**Structure**	**Input Size (bit)**	**Key Length**	**Cipher Size (bit)**	**Char**	**Rounds**	**Security (Authentication (A), Integrity (I) & Confidentiality (C)**
Usman et al. [19]	C & S	Secure IoT	Substitution & Fiestel	64	64	64	1-100	5	A, I, C
Kumar et al. [20]	C	Dynamic Key	Diffusion & Shuffling	64	128	64	-	-	I
Patil et al. [21]	C	LiCi	X-Boxes & Fiestel	64	128	64	-	31	I
Das et al. [22]	C & S	MD5, AES/DES	LSB, S-Box, LSB-MSB	128	128	128	-	10	A, I, C
Hanin et al. [23]	C	LCA HASH-MAC	HASH, M.A.C., PSOCA	512	512	512	1-100	-	A, I
Bhapat	C & S	AES	LSB, S-	128	128	128	-	10	A, I, C

et al. [24]			Box						
Jang et al. [25]	C	SHA 128, AES	Hash-MAC	128	128	128	-	10	A
Aljawarneh et al. [26]	C	Fiestel, AES, and GA	S-Box, Fiestel	128	256	128	-	10	I
Indrayani et al. [27]	C & S	AES, MD5	S-Box, Homogenous Frame	128	128	128	audio	10	A, I, C
Bharathi et al. [28]	C & S	Chaos	Diffusion, Confusion, M.S.B., LSB	256	256	256	image	-	I, C
Patel et al. [29]	C & S	Dynamic Key	MSB PRN, LSB	128	128	128	image	-	I, C
Sarvabhatia et al. [30]	C	1-time Pad	Hash, OTP	-	-	-	-	-	A

TABLE II. COMPARISON OF FUNCTIONALITIES

Scheme	Attribute authority	Outsource decryption	Revocation	Blockchain	Hidden policy	Verification
[31]	Single	No	Yes	No	Yes	No
[32]	Single	No	No	No	Yes	No
[33]	Multiple	No	No	No	No	Yes
[34]	Multiple	No	No	Yes	Yes	No
[35]	Multiple	No	No	No	Yes	Yes

Methodology

A. Attribute-Based Encryption

Sahai and Waters [5] presented the FIBE in 2005, which views identities as a collection of descriptive characteristics. Because it employs fundamental and descriptive algorithms, this scheme is typically considered the fundamental ABE scheme.

1) The Assumption of Complexity: The assumptions of complexity are given below.

Definition 1 (decisional bilinear Diffie-Hellman (BDH) assumption). Let's say the challenger picks something at random. The decision BDH assumption will be the one in which there is no polynomial-time adversary that is capable from the tuple ($A=g^{a,}$ $B=g^{b}$, $C=g^{c}$, $Z=e(g,g)^{z}$) of distinguishing the tuple (by replacing z as ABC) with a not so important benefit. This is the case since the BDH algorithm can differentiate between the two tuples.

Definition 2 (decisional modified Bilinear Diffie-Hellman (M.BDH) assumption). Let's say the challenger picks something at random. The decisional M.BDH assumption is that there is no polynomial-time adversary that is capable of distinguishing the tuple ($A=g^{a,}$ $B=g^{b}$, $C=g^{c}$, $Z=e(g,g)^{ABC}$) from (by replacing ABC with z) with a negligible benefit. This assumption depends on the concept that the tuple has three elements.

2) Algorithm Model's Formal Definition: The FIBE was formally defined by Sahai and Waters [5], who authored the article. An ABE scheme typically contains an authority, the sender, and certain receivers as participants. Additionally, an ABE scheme has four core methods: generating the key, setting up, encrypting, and decrypting. The following outlines the four algorithms that comprise the ABE scheme's fundamental structure.

Setup. Setup is a randomized procedure a competent individual carries out to generate a brand-novel ABE program. The only input it accepts is the implicit security parameter, and it spits out a master key MK along with a public parameters PK set as output.

Key Generation. The authority carries out the necessary steps of this algorithm to produce a private key. It accepts PK, MK, and a set of attributes, as its inputs and produces a decryption key SK as its output.

Encryption. A sender who wishes to do encryption of a message will run this randomized algorithm together with PK and the characteristics set. The message will then be encrypted. It gives you the CT formatted ciphertext.

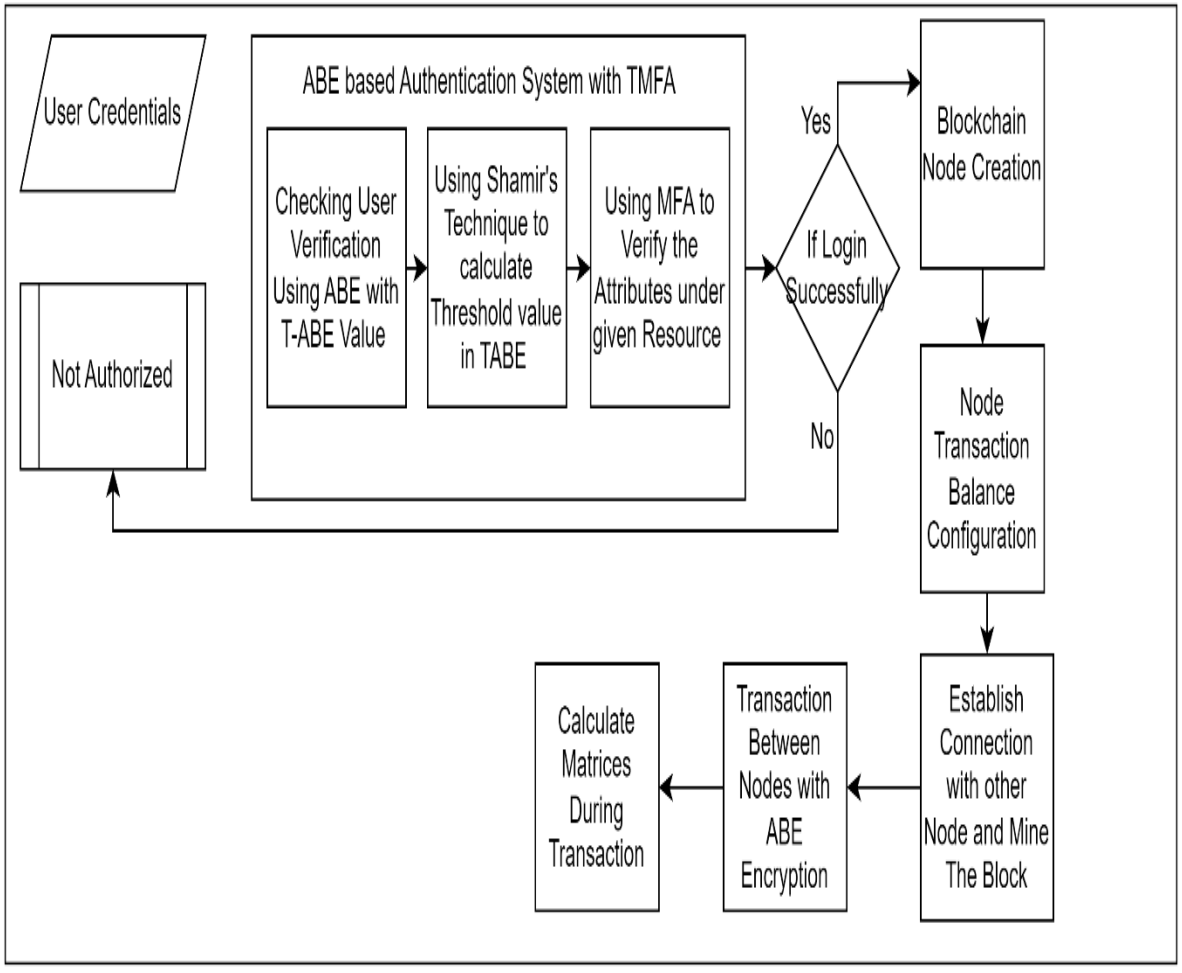

Fig. 1. Block diagram of the proposed methodology

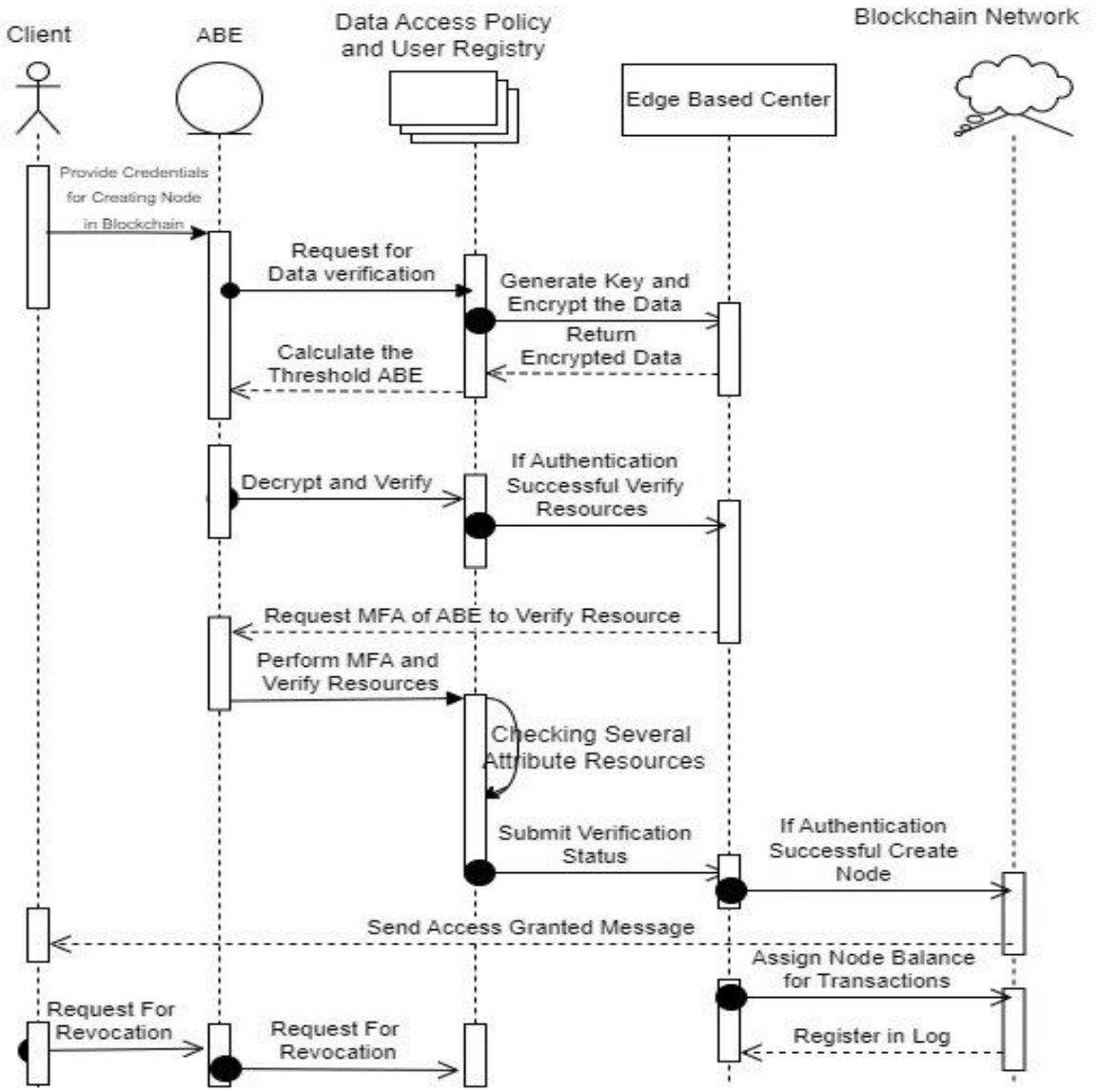

Fig. 2. Sequence diagram for the proposed research

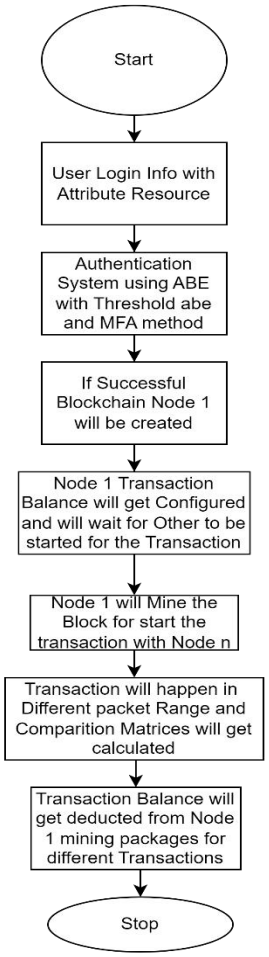

Fig..3. Flowchart of the proposed methodology

Decryption. This algorithm takes the ciphertext as input encrypted using PK, SK associated with, and the attributes ω' . These are the required inputs. The message is output if the condition $|\omega \cap \omega' \supseteq d|$ is met, and a threshold parameter is denoted by d. The ciphertext and the user's secret key have sets of descriptive properties attached to them when using the ABE scheme in its most basic form. Whether only there is at least one attribute overlap among the user's key and the attributes of the ciphertext, can a specific key be used to decrypt a particular ciphertext. The criterion for decryption in a KP-ABE or CP-ABE scheme is that the attribute set satisfies the access structure given in the ciphertext or secret key. This condition must be met for the procedure to be successful.

B. Steps used in the proposed research

In this research work, our distribution network is built on Blockchain with the help of the Web3 library. Each node in the network stands for a different user.

Created using LewkoWaters's algorithm, all transactions between nodes/blocks happen in the distributed network. However, data generated by the user session (genesis block) will be carefully checked for legitimacy by several nodes

(Hash block/supply block) in the blockchain network before it is in acceptance. The data access policy contains the list of all the network users. Most of the time, a ledger, a nonce, a hash, and a sample block are used in blockchain transactions between nodes. During the registration procedure, the details of the new user is given to the data access policy.

Fig. 1 represents the block diagram of the proposed research. Fig.2. Represents the sequence diagram of the proposed methodology. The system uses ABE to encrypt and decrypt resources and checks the user's attributes against access control policies stored on the blockchain.
The credentials are initially entered for blockchain node creation node 1. Once the request for data verification is given, the calculation for threshold ABE takes place using Shamir's technique. Encryption and decryption takes place using ABE at the same time. The Multi Factor Authentication (MFA) is enabled to verify if the resources requested by the user are registered by the user previously. Once the verification is successful, the block chain nodes are created and node balances are assigned for transactions. The revocation mechanism can be utilized by any user in the blockchain to revocate another user if required.
Since the basis ABE algorithm is inefficient and there is a lack of straightforward attribute revocation mechanism, the basic ABE system is improved by adding a revocation mechanism, multi-factor authentication (MFA), and threshold ABE to enhance the system's security and efficiency. The revocation mechanism allows another user to revoke access to specific attributes of a user if necessary, increasing the system's flexibility. The MFA adds an additional layer of security to the system by combining ABE with other authentication methods. If a user wants to access a resource but he is not allowed to use it, for that we are going to verify if this user is authorized to access this resource. The threshold ABE distributes the decryption key among multiple parties, making it more difficult for any single party to access the data on their own. Overall, the proposed implementation aims to provide a more secure and flexible authentication system that can better protect the data stored on the blockchain. Let there are numbers of participants as n participating in a system, denoted as P = {p1, p2, ...pn}. We consider the threshold value t for the system where $t \leq n$. We define a finite field K = GF(q), where identification of each participant in public is denoted as $\{(m1, m2, ...mn) \in GF(q) | \forall i,j\ (m1 \neq mj\ ; i \neq j)\}$. The threshold ABE is used to authenticate the user logging in using the login id and password.

The privileges and authorizations that a user has on a cloud application are used to determine the access class that user has on that application. In Multi Factor Authentication, the attributes that are given permission for a user is given authorization. In revocation process, any user can revoke the permissions of other user in the block chain. Fig. 3. represents the flowchart of proposed methodology.

Compared to AT (access tree) and AB (access-based) systems, the proposed ABE will improve the computational cost of decryption and encryption. Let us calculate the computation costs associated with incorporating the ABE scheme for blockchains. There are five distinct protocols in the ABE scheme. Nevertheless, the miners only during the decryption step participate in the computation, whereas the cluster chiefs participate in the encryption step. All three other protocols may be used in conjunction with the Internet. Thus, we will not be included them in our evaluation. The suggested concept modified the blockchain protocol mechanism only slightly to achieve attribute-based encryption without affecting the core security of the blockchain.

Pseudo code of ABE
Input: Al, Ks, D
Output: Null
Begin
Get Ks, Al, D
For every D and A
Find the chosen encryption key

$$K = \int_{i=1}^{size(Al)} Al(i) \equiv A \,\&\&\, \int_{j=1}^{size(Ks)} Ks(j).attr \equiv A$$

D(A) = Encryption (D(A), K)

End
Update cloud with D
Stop

We examined the proposed model's privacy and security and came up with strategies to lessen some frequent assaults. The sections on numerical analysis showed how attribute-based encryption might help blockchain become more private with less effort. Let A1 as the attribute list, Ks as the keyset, and D as the data point.

II. Results And Discussion

A. Dataset used

The shape of the dataset is (1000, 8). There are 1000 users who can be logged into the block chain. The user id for the users are user1, user2, …, user 1000. 6 attributes are considered, attribute 1, attribute 2, …, attribute 6. The sample dataset is given in Fig. 4.

	user_ID	user_key	attribute1	attribute2	attribute3
0	user1	a5sd5s4f6as	A	B	C
1	user2	vc1b59xc32c	A	B	C
2	user3	er8g4dxc5v2	A	B	C
3	user4	ebd4x35dv	A	B	C
4	user5	c1x8g5dfx	A	B	C

Fig. 4. Sample dataset

The dataset is next converted into Lists. This step in the implementation takes place because verification doesn't happen on datasets and the blockchain was not accepting the dataset as a whole, ABE process works on single data only and lists contains single data. Resource Attributes are calculated from the lists as represented in Fig. 5. The resource segments are calculated by classifying the attributes. Resources are sets of attributes. If someone checks for the attribute, it will check in the resource section and then connect to the user.

```
Resource: resource1
['A', 'B', 'C']

Resource: resource2
['Q', 'O', 'V']
['I', 'G', 'W']
['F', 'C', 'L']
['N', 'A', 'A']
['Y', 'Y', 'U']
['T', 'W', 'E']
['P', 'X', 'K']
['B', 'D', 'V']
['X', 'K', 'H']
['L', 'C', 'Q']
['M', 'X', 'W']
['E', 'W', 'B']
['T', 'B', 'J']
['Y', 'T', 'Q']
['W', 'C', 'E']
```

Fig. 5 : Resource Attributes Calculations

Attribute Checking in Resources takes place next. When the user is logging in and wants to acess any attributes, it will check in any one of the resources. It is used for verification of the attributes faster. Cypher User Table is represented in Fig. 6. It is basically an encrypted table using ABE. It will get transferred to Threshold ABE. Threshold ABE will decrypt the table and will verify the user id and password.

Next, Keys are being created for Encryption and decryption for ABE in general. Master Secret key (Private key), Master Public key and User key are generated for each user. Checking Keys for all users since every user have some keys. The secret key, public key and user key are used for all the users. User key is used for identifying user data. Each user has user key .

B. Checking Authentication of Users

Enter the user id and password for checking attributes of user 1 and then check for the required attributes. For checking User 1 Authentication, Keys are used and If User has Access to a Given Resources, Blockchain Node 1 Creation takes place. If Authentication is successful, MFA and Threshold ABE used. MFA resource verification takes place next. During the MFA verification process, the attributes that are given access to a user is verified.

Next for user 2, Enter the user id and password for checking attributes of user 2 and later check for the required attributes. For checking User 2 Authentication, Keys are used and If User has Access to a Given Resources, Blockchain Node 2 Creation takes place. If Authentication is successful, MFA and Threshold ABE used.

If the authentication is not successful, then an invalid user ID or password is generated and the user is not authorized to create a node block.

Revocation and Checking Authentication after Revocation takes place. One of the user is authorized for the access control. It has the authorization to revoke permission to any attribute of other user. Here the access of one the user has been revoked and then the authentication is checked after revocation. It is found out that the access is denied after revocation.

C. Transmission between two nodes using packets

Node Transaction balance is set up after two nodes, node 1 and node 2 are created. Block mining through Node 1 takes place and Node Transaction Communication is effected. For the transmission, 4 different packet sizes are considered, 5 kB, 10 kB, 20 kB and 50 kB. The threshold value of the Threshold ABE is set always to 2 for all the packet sizes. Table 4 gives the comparison of the performance matrics of the proposed adaptive ABE with ABE and RC4.

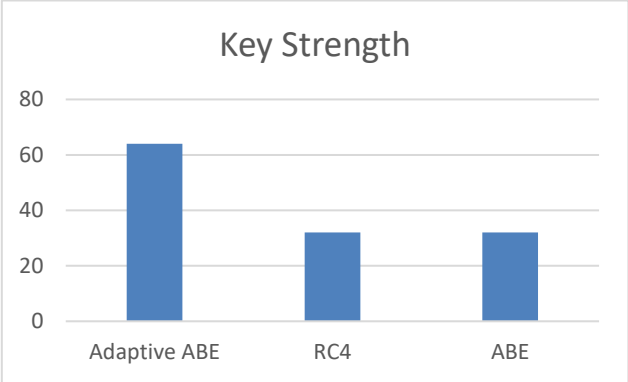

Fig. 6. Comparison of key strength

Fig. 6. gives the comparison of key strength of the proposed algorithm with RC4 and ABE. The integrity of a key can be evaluated using bits of security. After the bits of security for each individual key have been computed, the various types of keys (AES and RC4) will be able to have their respective strengths compared on a single scale.

Fig. 7. gives the comparison of encryption time complexity. In the encryption stage, the temporal complexity of the encryption method and the size of the generated ciphertext are defined not by the number of attributes that are present in access policies, but rather by the number of valid paths that are present. The ABE Time Complexity is given in Fig. 7.

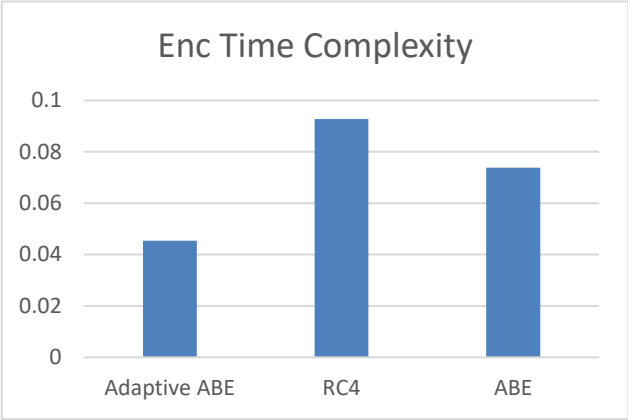

Fig. 7. Comparison of encryption time complexity

Fig. 8. gives the comparison of deccryption time complexity. In the encryption stage, the temporal complexity of the encryption method and the size of the generated ciphertext are defined not by the number of attributes that are present in access policies, but rather by the number of valid paths that are present.

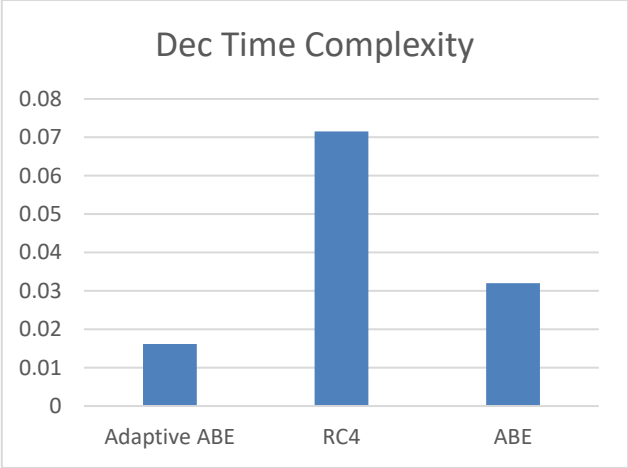

Fig. 8. Comparison of decryption time complexity

Fig. 9 shows the entire Program with proposed adaptive ABE execution time. It is observed that proposed adaptiveABE takes a minimum execution time. Throughout the process, the whole time cost for execution is execution cost and for transaction is transaction cost. Figure 10 gives the transaction cost comparison.

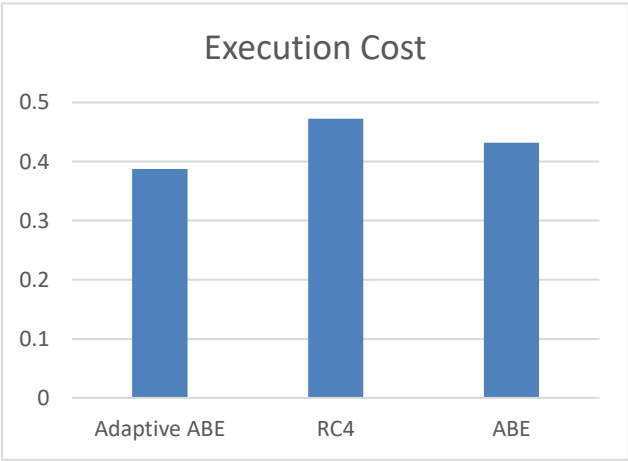

Fig. 9. Comparison of execution time

D. Comparison of the matrics for varied packet sizes

For the four packet sizes that are transferred the following graphs are compared for the proposed algorithm and RC4 and ABE.

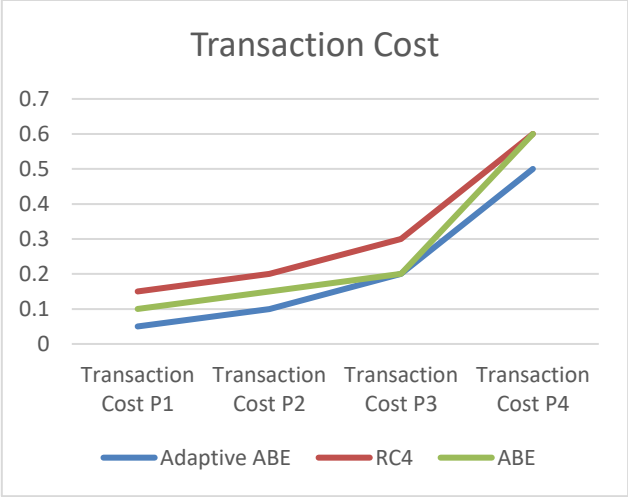

Fig. 10. Comparison of transaction cost

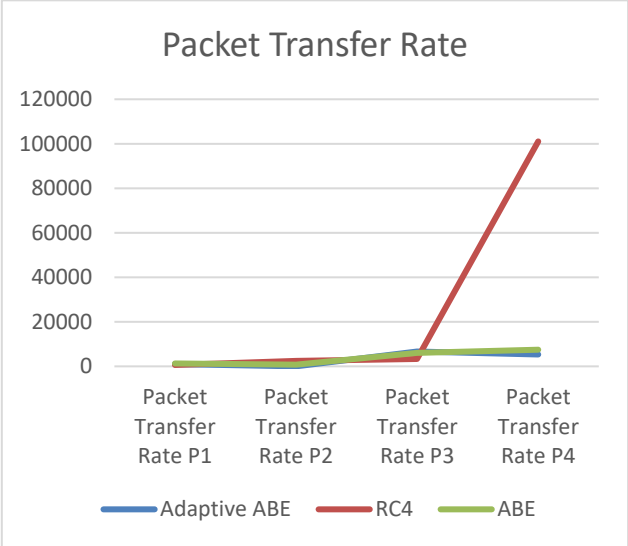

Fig. 11. Comparison of packet transfer rate

Fig. 11 gives the comparison of packet transfer rate. It gives the rate at which the packets have been transferred during the transmission process. Fig. 12. shows the Probability of how many encrypted message packets has been delivered and Fig. 13. gives the packet loss while transaction & verification. The term packet loss refers to the situation in which one or more data packets that are moving through a computer network do not arrive at their intended location. The packet ratio, is the ratio of the total number of packets delivered to the source node to the total number of packets sent to the destination node in the network.

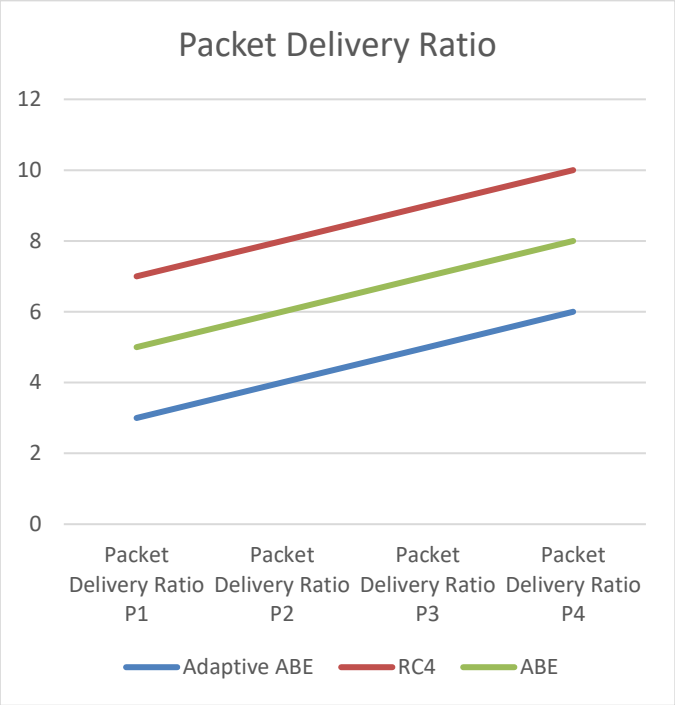

Fig. 12. Comparison of packet delivery ratio

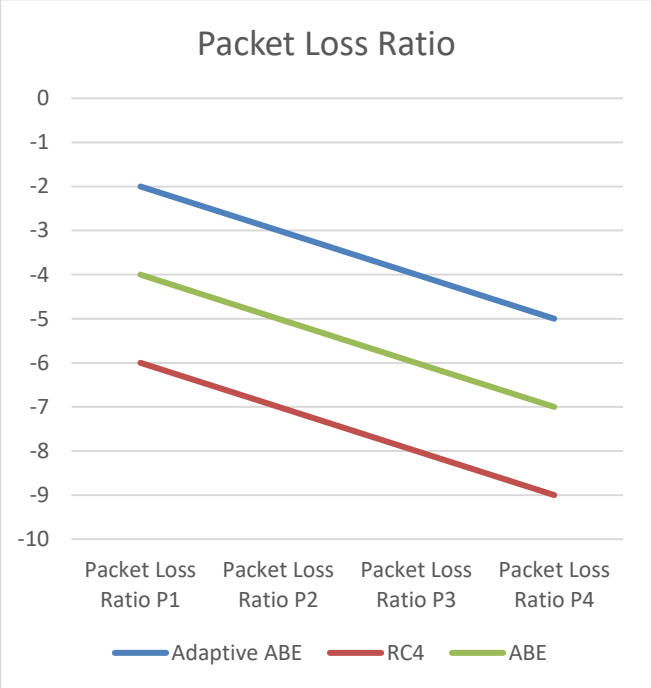

Fig. 13. Comparison of packet loss ratio

Fig. 14. shows the Encryption/Decryption Time of the Respective algorithm based on Message length and size. From the graphical results, it is observed that ABE consumes a minimum time for encryption and decryption as compared to the other two algorithms.

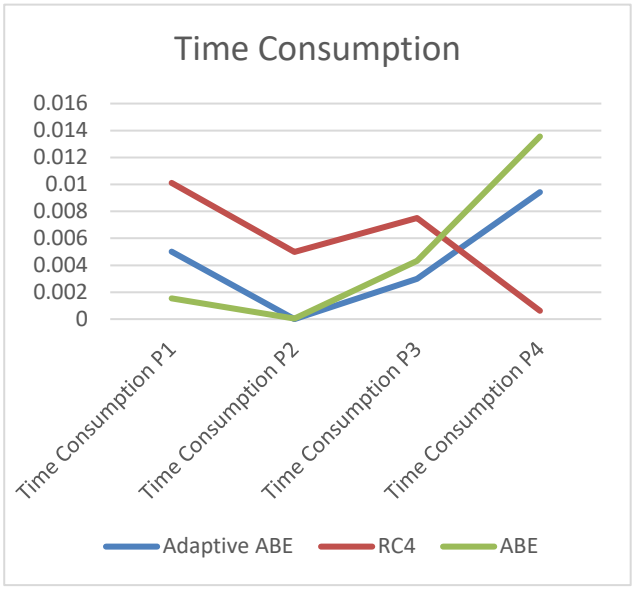

Fig. 14. Comparison of time consumption

TABLE III : COMPARISON OF PERFORMANCE MATRICS

Algorithm	Key Strength	Encryption Time Complexity	Decryption Time Complexity	Execution Cost
Adaptive ABE	64	0.045343161	0.016137123	0.38766328
RC4	32	0.092724657	0.071563862	0.472475529
ABE	32	0.073762452	0.0320153	0.43183264

V Conclusion

Authentication methods and protocols for users are being worked on in many different ways. But most existing works don't meet the required needs and requirements, like letting nodes move around, making sure they can scale through decentralized methods, and making adding new devices and services easy. The proposed technique enhances the authentication process for users, which is deemed more effective than the current methods. Our simulations show that the proposed adaptive ABE having threshold ABE, Multi Factor Authentication (MFA) and revocation mechanism is better than both ABE and RC4 with respect to cost of execution and transmission, packet delivery and loss, encryption execution time, and decryption execution time. Develop our plan for how to help manage permissions in future projects.

References

[1] A. Khan et al. IoT security: review, blockchain solutions and open challenges, FUtur. Gener. Comput. System (2018).

[2] K. Wong, Y. Zheng, J. Cao, and S. Wang, ‘‘A dynamic user authentication scheme for wireless sensor networks,’’ in *Proc. IEEE Int. Conf. Sensor Netw., Ubiquitous, Trustworthy Comput. (SUTC)*, Taichung, Taiwan, Jun. 2006, pp. 244–251.

[3] H.-R. Tseng, R.-H. Jan, and W. Yang, ‘‘An improved dynamic user authentication scheme for wireless sensor networks,’’ in *Proc. IEEE GLOBECOM-IEEE Global Telecommun. Conf.*, Washington, DC, USA, Nov. 2007, pp. 26–30.

[4] T. H. Lee, ‘‘Simple dynamic user authentication protocols for wireless sensor networks,’’ in *Proc. 2nd Int. Conf. Sensor Technol. Appl.*, Cap Esterel, France, Aug. 2008, pp. 657–660.

[5] M. L. Das, ‘‘Two-factor user authentication in wireless sensor networks,’’ *IEEE Trans. Wireless Commun.*, vol. 8, no. 3, pp. 1086–1090, Mar. 2009.

[6] H. F. Huang, Y. F. Chang, and C. H. Liu, ‘‘Enhancement of two-factor user authentication in wireless sensor networks,’’ in *Proc. 6th Int. Conf. Intell. Inf. Hiding Multimedia Signal Process. (IIH-MSP)*, Darmstadt, Germany, Oct. 2010, pp. 27–30.

[7] S. G. Yoo, K. Y. Park, and J. Kim, ‘‘A security-performance-balanced user authentication scheme for wireless sensor networks,’’ *Int. J. Distrib. Sensor Netw.*, vol. 8, no. 3, Mar. 2012, Art. no. 382810.

[8] A. K. Das, ‘‘Cryptanalysis and further improvement of a biometric-based remote user authentication scheme using smart cards,’’ *Int. J. Netw. Secur. Appl.*, vol. 3, no. 2, pp. 13–28, Mar. 2011.

[9] X. Li, J.-W. Niu, J. Ma, W.-D. Wang, and C.-L. Liu, ‘‘Cryptanalysis and improvement of a biometrics-based remote user authentication scheme using smart cards,’’ *J. Netw. Comput. Appl.*, vol. 34, no. 1, pp. 73–79, Jan. 2011.

[10] Y. An, ‘‘Security analysis and enhancements of an effective biometricbased remote user authentication scheme using smart cards,’’ *J. Biomed. Biotechnol.*, vol. 2012, pp. 1–6, Jul. 2012.

[11] M. K. Khan and S. Kumari, ‘‘An improved biometrics-based remote user authentication scheme with user anonymity,’’ *BioMed Res. Int.*, vol. 2013, pp. 1–9, Nov. 2013.

[12] Y. F. Chang, S. H. Yu, and D. R. Shiao, ‘‘A uniqueness and anonymitypreserving remote user authentication scheme for connected health care,’’ *J. Med. Syst.*, vol. 37, no. 2, pp. 9980–9988, 2013.

[13] A. K. Das and A. Goswami, ‘‘A secure and effificient uniqueness-andanonymity-preserving remote user authentication scheme for connected health care,’’ *J. Med. Syst.*, vol. 37, no. 3, p. 9948, Jun. 2013.

[14] H. Arshad and M. Nikooghadam, ‘‘Three-factor anonymous authentication and key agreement scheme for telecare medicine information systems,’’ *J. Med. Syst.*, vol. 38, no. 12, pp. 1–12, Dec. 2014.

[15] Y. Lu, L. Li, H. Peng, and Y. Yang, ‘‘An enhanced biometric-based authentication scheme for telecare medicine information systems using elliptic curve cryptosystem,’’ *J. Med. Syst.*, vol. 39, no. 3, pp. 1–8, Mar. 2015.

[16] S. H. Islam and M. K. Khan, ‘‘Cryptanalysis and improvement of authentication and key agreement protocols for telecare medicine information systems,’’ *J. Med. Syst.*, vol. 38, no. 10, pp. 135–142, Oct. 2014.

[17] L. Zhang and S. Zhu, ‘‘Robust ECC-based authenticated key agreement scheme with privacy protection for telecare medicine information systems,’’ *J. Med. Syst.*, vol. 39, no. 5, pp. 49–56, May 2015.

[18] Q. Feng, D. He, S. Zeadally, M. K. Khan, and N. Kumar, ‘‘A survey on privacy protection in blockchain system,’’ *J. Netw. Comput. Appl.*, vol. 126, pp. 45–58, Jan. 2019.

[19] Usman, M., Ahmed, I., Aslam, M. I., Khan, S., & Shah, U. A. (2017). SIT: A Lightweight Encryption Algorithm for Secure Internet of Things, 8(1).

[20] Kumar, M., Kumar, S., Budhiraja, R., Das, M. K., & Singh, S. (2017). Lightweight Data Security Model for IoT Applications: A Dynamic Key Approach. Proceedings - 2016 IEEE International Conference on Internet of Things; IEEE Green Computing and Communications; IEEE Cyber, Physical, and Social Computing; IEEE Smart Data, iThings-GreenCom-CPSCom-Smart Data 2016, (3), 424-428.

[21] Patil, J., Bansod, G., & Kant, K. S. "LiCi: A new ultra-lightweight block cipher," *in 2017 International Conference on Emerging Trends & Innovation in ICT (ICEI),* feb 2017, pp. 40-45.

[22] Das, R., & Das, I. (2017). Secure data transfer in IoT environment: Adopting both cryptography and steganography techniques. Proceedings - 2016 2nd IEEE International Conference on Research in Computational Intelligence and Communication Networks, ICRCICN 2016, 296-301.

[23] Echandouri, B., Hanin, C., Omary, F., & Elbernoussi, S. (n.d.). LCAHASH-MAC : A New lightweight Message Authentication code Using Cellular Automata for RFID. nov 2017, pp. 287-298.
[24] Bapat, C., Baleri, G., B, S. I., & Nimkar, A. V. (2017). Smart-Lock Security Re-engineered Using Cryptography and Steganography, Security in Computing and Communications, 325-336.
[25] Jang, S., Lim, D., Kang, J., & Joe, I. (2016). An Efficient Device Authentication Protocol Without Certification Authority for Internet of Things. Wireless Personal Communications, 91(4), 1681-1695.
[26] Aljawarneh, S., Yassein, M. B., & Talafha, W. A. (2017). A resource-efficient encryption algorithm for multimedia big data. Multimedia Tools and Applications, 76(21), 22703-22724.
[27] Indrayani, R., Nugroho, H. A., Hidayat, R., & Pratama, I. (2017). Increasing the security of MP3 steganography using AES Encryption and MD5 hash function. Proceedings - 2016 2nd International Conference on Science and Technology-Computer, ICST 2016, 129- 132.
[28] V, M. B., Manimegalai, M., & Sinduja, V. (2013). Enhancement of Image Security with New Methods of Cryptography and Steganography, 9(9), 59-64.
[29] Patel, N., & Meena, S. (n.d.). LSB Based Image Steganography Using Dynamic Key Cryptography. 2016 International Conference on Emerging Trends in Communication Technologies (ETCT),
[30] Sarvabhatla, M., Chandra, M. R. M., & Vorugunti, C. S. (2015). A secure and light weight authentication service in hadoop using one time pad. Procedia Computer Science, 50, 81-86.
[31] D. Han, N. Pan, K. Li, A traceable and revocable ciphertext-policy attribute-based encryption scheme based on privacy protection, IEEE Trans. Dependable Secure Comput., 19 (2020), 316–327.
[32] Q. Li, B. Xia, H. Huang, Y. Zhang, TRAC: traceable and revocable access control scheme for mHealth in 5G-enabled IIoT, IEEE Trans. Ind. Inf., 18 (2022), 3437–3448.
[33] S. J. De, S. Ruj, Decentralized access control on data in the cloud with fast encryption and outsourced decryption, in 2015 IEEE Global Communications Conference (GLOBECOM), (2015), 1–6.
[34] S. J. De, S. Ruj, Decentralized access control on data in the cloud with fast encryption and outsourced decryption, in 2015 IEEE Global Communications Conference (GLOBECOM), (2015), 1–6.
[35] K. Sethi, A. Pradhan, P. Bera, PMTER-ABE: a practical multi-authority CP-ABE with traceability, revocation and outsourcing decryption for secure access control in cloud systems, Cluster Comput., 24 (2021), 1525–1550