

Flexible and secure continues data transmission among multiple users in cloud environment

Ezhilarasan Elumalai, Dinakaran Muruganandam

School of Information Technology and Engineering, Vellore Institute of Technology, Vellore, India

Article Info

Article history:

Received Sep 7, 2022

Revised Jan 13, 2023

Accepted Jan 16, 2023

Keywords:

Broadcasting encryptions

Cloud computing

Data transmission microgrid

Decryption time

Encryption time

Flexible and secure continues

ABSTRACT

Cloud computing is an internet based computing where the sharable information, software and resources are provided based on demand devices. Where, the rapid development and pervasive growth of unavoidable sending of message advances, there are expanding requests of adaptable cryptographic natives to protected group data transactions and computing platforms in cloud. Group key agreement (GKA) protocol enables a group to share a standard encryption key across an open network so that only members of the group may decode the ciphertexts encoded using the secret encryption key that has been released. However, a sender cannot deny any specific member from decryptions the ciphertexts in cloud. However, before sending a message to a group, a user must join the group and follow the GKA protocol to provide the intended members access to a secret key. To find a better solution for the above-mentioned issues, flexible and secure continues data transmission (FSCDT) algorithm is proposed to offer dynamic and secure data transfer broadcasting without full trust of key authority in unreliable cloud environment. It provides compete security proof, outlines the requirements of the aggregatability of the secret attribute based FSCDT building block. Based on experimental evaluations, FSCDT algorithm minimizes encryption time, decryption time and communication cost.

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



Corresponding Author:

Dinakaran Muruganandam

School of Information Technology and Engineering, Vellore Institute of Technology

Vellore, Tamil Nadu, India

Email: dinakaran.m@vit.ac.in

1. INTRODUCTION

Cloud computing is a web-oriented computing systems where the sharable data, programming and assets are given dependent on request devices [1]. The surfacing of cloud has essentially mutilated the overall view of infrastructure development, programming system and advancement models. This in the end lead to a steep change from centralized storage server to client-server execution models, which thus moves forward to assign cloud computing [2]. These current trends on cloud platform consider instant-messaging tools, collaborative computing, and social network [3]. The issue of applying the broadcast encryption system to cloud storage server discussed about a few security and protection challenges. To overcome the above-mentioned issues, flexible and secure continues data transmission (FSCDT) algorithm is proposed to offer dynamic and secure data transfer broadcasting without full trust of key authority in cloud environments. It defines the requirement for the aggregatability of the basic attribute-based FSCDT building block and provides complete security confirmations. The paper contribution is as follows:

- To develop the FSCDT algorithm for to provide dynamic and secure data transmission broadcasting without relying entirely on key authorities in unreliable cloud environments.

- To set up the FSCDT algorithm with a public group encryption key to provide an effective and dependable encryption and decryption procedure for shared data in cloud environments.
- To build system that has been rigorously demonstrated to be reliable and collusion-resistant under the accepted privacy-preserving paradigm.
- To enable scalable key management in an unstable cloud environment between data owners, data users, and cloud service providers.
- To design a robust framework for identifying and preventing the malicious activities in un-trusted cloud environments. To reduce encryption and decryption times as well as communication cost (CC) for speed up FSCDT in un-trusted cloud environments in comparison to existing approaches.

A technique based on attribute-based broadcast encryption is provided in [4] to secure group information exchange using attribute-based broadcast encryption. Cloud computing system included the internet of things as a foundational event for big data [5]. In order to increase security concerns, it also made an effort to develop an architectural handing-off on the organization's security. YRL scheme attack was discussed, and it was demonstrated that unauthorized receivers could also decode broadcast messages [6]. In the selected cipher text configuration, it obtains anonymity and semantic security under adaptive corruptions. A smart medical care city using a multi-agent system (MAS) with a three-layered design is detailed in [7], [8]. The method ensures that sensitive health information about residents is protected, with group key arrangement (GKA) serving as the cornerstone for safely exchanging medical information across healthcare partners. Described group key agreement mechanism based on attribute authentication and privacy protection in [9]. Privacy protection is a specific concept in several applications and it assists users in comprehending how each privacy pattern is created and how it contributes to data privacy protection [11]. A cloud-based privacy-preserving multi-receiver certificate-less broadcast encryption method with de-duplication (PMCBED) that relies on anonymous broadcast encryption and certificate-less cryptography is described in [12]. It can satiate semantic security considerations of receiver anonymity and information categorization. Anonymous broadcast encryption for its merits with reference to communication expense and overburden [13]. The technique advances an efficient identity-based broadcast encryption development and applies it to the cloud services' information access control component. The flexible, secure cross-cloud information collaboration strategy in [14] used proxy re-encryption (PRE) and identity-based cryptography (IBC) techniques. Several cryptographic approaches used for query authentication and dispersed information base security [15].

The state-of-the-art method on secure and protection safeguarding clinical information sharing of the previous decade with an emphasis on blockchain-based methodologies [16]. SKY, a cryptographic access control expansion designed to provide privacy and obscurity guarantees while expertly scaling to large associations [17]. To combat the complexity of anonymous broadcast encryption (ANOBE) systems, A-SKY uses trusted execution environments, achieving computation time and more constrained ciphertexts. Several important concerns relating to the security and preservation of EHRs [18]. The data storage lock algorithm (DSL) provides secure information storage in cloud computing is described in [19]. A configurable identity-based proxy re-encryption scheme with an external equality test (IBPRE-ET) was investigated [20]. Revocable hierarchical identity-based broadcast encryption (RHIBBE) allows for rejection of the HIBBE, was established [21]. Ciphertext is designed to be resistant to the bounded revocable identity-vector-set and chosen-plaintext attack on prime-request bilinear groupings, usage renunciation. Two layers dynamic broadcasting encryption to deal with tackle the issue [22]. The decentralized unique broadcasting encryption and subgroup key trade, a structure block use in development that might be of autonomous enthusiasm by designating [23] in cloud. However, there are many of the access control authorization obligations as could reasonably be expected to the Cloud while limiting the data introduction chances due to conspiring users and cloud [24]. The design that underpins various ways to deal with secure information collection in cloud [25].

2. METHOD

The section describes FSCDT algorithm proposes to offer dynamic and secure data transfer broadcasting without full trust of key authority in unreliable cloud environment. It offers full security confirmations, shows the need of the aggregatability of the basic attribute based FSCDT building block. Here, proposed algorithm execution procedure is divided into following phase namely: data owner, group authority, cloud storage server, data users, attacker and cloud server provider. Here proposed approach tackles the data transportation issues in cloud environment. In this technique provides freedom and full access to data owner to change cloud storage server without any privacy issues. This method is efficient in multiple cloud environments and as well effective to prevent external malicious attack during data transmission from one cloud to another cloud storage server in unreliable cloud environments.

2.1. Data owner

The data owner should be enrolled with client name, email and group, subsequent to enlisting user's needs to login by utilizing substantial client name and secret password. The data owner peruses and transfers their information to the cloud server. For the security reason the information, data owner encrypts information (document, image and video) and afterward stores in cloud server. Data owner is responsible for characterizing (attribute based) access policy and upholding it on its own information by encoding the information under the arrangement prior to putting away it to the storage cloud server.

2.2. Key authority

The key authority is responsible for enrolling and login approval for the end clients in the event that they are in similar groups and furthermore see bunch clients, bunch signs and enlisted client. Where, key age measure produces people in public/private parameters for attribute-based encryptions. The key authority contains focal power and different neighborhood specialists. It expects that there are secure and dependable correspondence ways between a focal position and every neighborhood authority during the underlying key arrangement and age measure. Every closest authority oversees various ascribes and issues comparing characteristic mystery keys to information customers. Key authority grant differential access rights to individual clients dependent on the user's attributes.

2.3. Cloud storage server

The Storage worker is liable for information stockpiling and record approval for data user and data owner. The information (document, image and video) file will be put away in cloud server with their labels, for example, owner, record name, secret key, and private key, can likewise see the enlisted owners and data consumer in the cloud storage server. The information file will send dependent on the advantages. On the off chance that the advantage is right, at that point the information will be sent to the comparing information consumer and furthermore will check the record name, end username and secret key.

2.4. Data user

The data user will ask for getting data information from the comparing cloud storage servers. If the document name and secret key, access authorization like search and download is right then the end is getting the record reply from the cloud storage server to data user. In the event that a data user has a bunch of keys for fulfilling the access policy of the encoded information characterized by the data owner, and is not revoked in any of the traits, at that point he/she will have the option to decode the cipher text and recover the information from cloud.

2.5. Attacker

Attacker is one who is attempting to get records by giving secret key to get the information from cloud storage server. The assailant might be inside a group or from outside of the group. In the event that Attacker r is from inside the group, at that point those assailants are called as internal attackers. In the event that the assailant is from outside the groups, at that point those aggressors are called as external attackers.

2.6. Flexible and secure continues data transmission algorithms

FSCDT algorithm is designed to offer dynamic and secure data transfer broadcasting without full trust of key authority in unreliable cloud environment. Proposed method is utilized to make sure about information shared among data owner and data user by means of secure key about the protection of their information imparted to their data users in unreliable cloud. The proposed solution formalizes settlement blockage by posing an attacker who can completely seize control of everyone outside of the intended recipients but is unable to distinguish valuable data from cipher text on a cloud storage server. Simply the accumulated decoding keys of a single individual are valid unscrambling keys when compared to the combined public keys of the hidden encryption. The proposed device is used to impervious classified content and is utilized globally for credential data encryption and decryptions. The specific round of keys is deployed. Each group consists of steps, which have a substitution, transposition, and mixing of plain content. Then, the right content is exchanged into encoded content. Proposed technique develops encryption conspire firmly demonstrated to be completely agreement safe under standard privacy preserving model. The proposed technique offers productive encryption/decryption and short ciphertexts. In this case, setting up the proposed architecture and creating the public group encryption key just require one cycle. The capacity value of the owner and the group authority after the framework configuration is $O(n)$. Where, the range of group authority contributions during setup is denoted by the number n . The proposed solution bridges the gap between the online presentation and the multidimensional setup. The variant has $O(n^2=3)$ unpredictable correspondence, processing, and storage in a cloud environment after a tradeoff. This is equal to standard proposed method have $O(n^1=2)$ unpredictability

in comparable execution measurements. The technique access policy need not be sent alongside the cipher text, by which we can protect the security of the encryptor. The method scrambled information can be kept secret regardless of whether the cloud storage server is untrusted; in addition, proposed techniques are secure against agreement assaults. When, the original cipher text is produced for a set of users who have highlighted a certain unique characteristic for instance. When a portion of the receivers is rejected, if the character information about them isn't guaranteed, the unique attribute held by the full recipients will be made public by the revoked user. It also consists of the stages that follow.

Setup: Given a **protection** boundary, the **association** calculation arbitrarily **selections** a bilinear gathering $B_G = (G, GT, e, p)$ with generator $P \in G$. It picks $s \in \mathbb{Z}_p$ and units $P_{pub} = sP$.

Then At that **factor** it **preferences** cryptographic hash **features**: $\{0, 1\}^* \rightarrow G$.

The **group** public key and the Master secret key are $mpk = (BG, P, P_{pub}, H), msk = s$:

KeyGen (mpk, msk, Ik): Given the master key pair (mpk; msk) and a **person traits** $Ik \in \{0, 1\}^*$ key generation **strategies** restores a user private key as $dID = sH(Ik)$:

Encrypt (mpk; M; S): Given the master public key mpk, a message $M \in G$ and an **characteristics** s set $S = (Ik_1, Ik_2, \dots, Ik_n)$, the encryption algorithm **options** a specious user signified as $Ik_0 \notin S$ and proceeds as follows;

1. Randomly pick **out** an encryption key $K \in G$ and arbitrary numbers $r_1 \in \mathbb{Z}_p$, calculate $C_0 = K + M, C_1 = r_1P$
2. For each $i = [0, n]$, calculate $x_i = H_1(eH(ID_i), P_{pub}, ID_i)$
At that factor it assembles polynomial functions as (1).

$$f_i(x) = \prod_{j=0, j \neq i}^n \frac{x - x_j}{x_i - x_j} \sum_{j=0}^n a_{i,j} x^j \text{ mod } p \tag{1}$$

It estimates

$$Q_i = \sum_{j=0}^n a_{j,i} A_j, U_i = \sum_{j=0}^n a_{i,j} B_j \tag{2}$$

The output cipher text is $CT = (C_0, C_1, C_2, C_3, r_1, [Q_i, U_i]_{i=0}^n)$

Revoke (mpk, CT, R): Given a cipher text CT which is parsed as the master public key $CT = (C_0, C_1, C_2, C_3, r_1, [Q_i, U_i]_{i=0}^n)$ the master public key mpk and a forsake character set $R = (ID_1, ID_2, \dots, ID_t)$ where $t < n$. If $R = \emptyset$, the revocation technique **units** the new cipher text $CT' = CT$. Randomly pick out $K_2 \in G$ and tactics $C_0' = K_2 + C_0$.

For every $ID_i \in R$, method $x_i = H(e(H(ID_i), P_{pub})^{r_1}, ID_i)$ and construct.

$$g(x) = \prod_{i=1}^t (x - x_i) = \sum_{i=0}^t b_i x^i \text{ mod } p \tag{3}$$

For $i = 0, 1, 2, \dots, t$ process.

$$Q_i'' = Q_i + b_i K_2$$

What's more, set the new ciphertext as a

$$CT' = (C_0', C_1, b_0, b_1, \dots, b_{t-1}, q_0', q_1', \dots, q_{t+1}', \dots, q_n, u_0, \dots, u_n)$$

Decrypt (mpk, CT', dID): Given a cipher text parsed CT' which is parsed as

$$CT' = (C_0', C_1, b_0, b_1, \dots, b_{t-1}, q_0', q_1', \dots, q_{t+1}', \dots, q_n, u_0, \dots, u_n)$$

The master public key mpk, identification ID and the consequent private key dID, the decryption method executes as follows;

Compute $x_i = H(e(C_1, dID_i), ID_i)$

$$g(x_i) = \sum_{i=0}^t b_j x_i^j + x_i^t \text{ mod } p \tag{4}$$

If $g(x_i) = 0$, it **in advance** ends, else, it schedules

$$U = U_0 + x_1 U_1 + x_2 U_2 + \dots + x_n U_n,$$

$$q = q'_0 + x_1 q'_1 + x_2 q'_2 + \dots + x_t q'_t + x_{t+1} q'_{t+1} + x_n U_n$$

Use the private key dID_i to **get well** the encryption keys **with the aid of** computations

$$K'_1 = U - H(e(C_3, d_{ID_i}), Id_i)$$

$$K'_2 = g(x_i)^{-1}(q - H(e(C_2, d_{ID_i}), Id_i))$$

Furthermore, collect the message $M' = C'_0 - K'_1 - K'_2$. If $ID_i \in S \setminus R$, we have $K'_1 = K_1$, $K'_2 = K_2$ and can **accumulate** the message M effectively.

In addition to the requirement that the message and the user be protected from the public by the cipher text CT_0 , the message must also be unexpected from CT and CT must safeguard the recipient's privacy from outsiders. The proposed approach offers more than just content privacy. To protect origin identification and semi-anonymity, it also includes privacy identification and decentralizes the central authority. Therefore, the technology completely conceals the identity and aids in achieving complete anonymity. In this context, there are four different types of attributes: Group authorities (abbreviated as Group A), specifically cloud server, data owners, and data user. In a single session, a data user may also be both a data owner and a data user. In a single session, a data user may also be both a data owner and a data user. Encrypted data files are uploaded to the cloud server by the data owner. Proposed system prefers encryption for forwarding the token & secret keys for authorizes them to function the operations. In a system, the decryption of an encrypted data is solely one situation is accessible solely if the user secret key of the set of attributes fits the attributes of the cipher text then encrypted data will be transformed in plain text. A proposed approach is collusion-resistance; where, adversary holds multiple keys. It needs to be capable to get access to the data; if at least one particular key access approval. The keys are supplied via a system to users is used to operate the operations for having access to the file data from the cloud server.

3. RESULT AND DISCUSSION

3.1. Deployment setup

The proposed FSCDT algorithm is executed against standard approaches using a laptop running Windows 10 with an Intel i7Core CPU, 8 GB of RAM, and 500 GB of storage. Here, the proposed approach is implemented in a Java web application with the help of the NetBeans 8.0 IDE (integrated Development Environment), a JProfiler MySQL 5.7 database, and the Jelastic open-source cloud server for cloud deployment of the algorithm-integrated application. For proposed FSCDT approach evaluation, the experimental system utilized 5 kinds of users 200, 400, 600, 800, and 1,000 with 3 types of data namely documents, images and videos. For transmitting the owner data from data owner to data user and cloud storage server, Java based developed effective and secure data migration with reliable data transmissions model is used.

3.2. Simulation result

The proposed method represents mathematical expression that will increase the security of cloud storage servers. The privacy approach that is being works with data owner and data user. The content of the data owner will be safe throughout data transfer and retrieval in an unstable cloud environment even when cloud storage servers are no longer completely dependable on key authorities. Consider the proposed flexible and secure continues data transmission algorithm's scalability, decryption time, and communication costs.

3.3. Encryption time (ET)

In this section, proposed method for describing the mathematical model of encryption in (5). Data transfer or a message M , the public key PK , and a collection of attributes I are the inputs for this method. The cipher-text CT is carried out in the following manner:

$$CT = (I, CT\{CT_i\}_{i \in I}) \quad (5)$$

where $\tilde{CT} = MYs$, $CT_i = Asi$, and s is randomly chosen from Z_p .

3.4. Decryption time (DT)

In this section, proposed method denotes the mathematical model of decryption time in (6). The attribute set I is received by this method and entered as cipher-text CT encrypted information the user's public key PK and secret key SK for accessing tree a . It carries out the decryption process in (6).

$$CT(CT_i, ski) = CT(g, g)^{pi(0)s} \tag{6}$$

Where CT=Chiper-text and ski=user secret key issue for attribute I leaf nodes. The polynomial interpolation approach is then used to sequentially integrate the paired results. Last but not least, it improves the blind item $Y_s = CT(g, g)^s$ and displays the message M only if I is satisfied A.

3.5. Communication cost (CC)

The CC is calculation of complete quantity of data transportation in unreliable cloud environment. The proposed FSCDT algorithm elaborates a mathematical expression in (7) to consider the communication cost in %. The CC is evaluated with recognition of data transfer rate with data sizes.

$$CC = \frac{DR_{transfer}}{D_{consize}} \times 100 \tag{7}$$

Where, $DR_{transfer}$ is data transfer rate, and $D_{consize}$ is the total size of data.

Table 1 displays the communication cost (%), encryption time (Milliseconds), and decryption time (Milliseconds) for 200, 400, 600, 800, and 1,000 Users. The PPIBE scheme, the AIBE approach, the EDABE scheme, and the EAIBE existing methodologies are all compared to the proposed FSCDT algorithm. When it comes to communications costs and correspondence overload, the [23] is defined with its positive examples. The process applies a broadcast encryption technique based on anonymous identification to the data access control system in a cloud storage server [24]. However, because the key data is not updated immediately, it may cause a bottleneck in the rekeying system or security corruption [25]. The sender is permitted by the proposed approach to prevent some people from reading the ciphertexts. The proposed FSCDT method formalizes collusion resistance by defining an aggressor who can fully control every group member outside of the expected receivers but who is unable to extract useful information from the encrypted text [26]. The proposed FSCDT method assesses communication cost in (%), encryption time (in sec), and decryption time (in sec). Where, it noticed that proposed FSCDT algorithm indicates better outcomes compare other than current methodologies alongside with common values for respective parameter. Table 1 shows the minimized 0.88 encryption time (seconds), 0.68 decryption time (seconds) and communication cost 31.6% for 200, 400, 600, 800, and 1,000 users rather than existing methodologies along with average values for respective parameter. transmission (FSCDT) algorithm is the best approach in unreliable cloud environment.

Table 1. Encryption time (ET) in milliseconds, decryption time (DT) in milliseconds and communication cost (CC) in % for 200, 400, 600, 800, and 1,000 users

User	200			400			600			800			1,000		
Technique	ET	DT	CC	ET	DT	CC	ET	DT	CC	ET	DT	CC	ET	DT	CC
PPIBE	2.5	2	199	4.3	3	190	5.2	3.5	101	7	4.6	80	9	5	60
AIBE	7.5	9	498	14	16	488	21	24	241	31	34	186	36	40	126
EDABE	4	1.5	211	5	2.2	195	3.8	2.7	92	5.5	3.3	71	7	4.5	51
EAIBE	1.6	0.95	201	2.7	2.0	180	3.0	2.3	98	4.2	3.0	66	5.3	4	54
FSCDT	0.95	0.42	121	2.2	0.92	115	1.5	1.8	95	3.95	2.5	70	3.8	3.2	40

According to proposed FSCDT algorithm evaluation result in Figure 1, Figure 2, and Figure 3 for 200, 400, 600, 800, and 1,000 Users. Where, it observed that proposed flexible and secure continues data behalf of encryption time, decryption time and communication cost, proposed FSCDT algorithm display that it always yields the best performance in both all graphical and tabular result. PPIBE discussed against an active attacker and consumed less storage and communication cost for data embedding during broadcasting the message. Where, it secures the protection of recipients of broadcasted messages by concealing the personalities of receivers in storages [27].

But the method failed to provide user protection and organization security during data transmissions. AIBE scheme explained about decoded text and secret keys which are undefined for the various beneficiaries set in cloud. However, it would possibly convey about bottleneck for the duration of rekeying system or privacy error due to the data of the windows weakness if the previous private key is not refreshed EDABE scheme adopted lagrange interpolation polynomial. Where, privacy recreation defined, the adversary is forbidden to trouble decryption queries. However, the scheme did not gain safety towards adaptive chosen-cipher text attack (CCA2) adversaries.

EDABE described with its favorable situations in the regards of communication cost and correspondence over-burden. Neither traditional symmetric GKA nor the recently expressed GKA permit the sender to unilaterally exclude a specific member from perusing the plaintext. Proposed framework attributes

are utilized to give an explanation for a client's accreditations, and a group encoding data decides a strategy for who can decrypt in cloud environments.

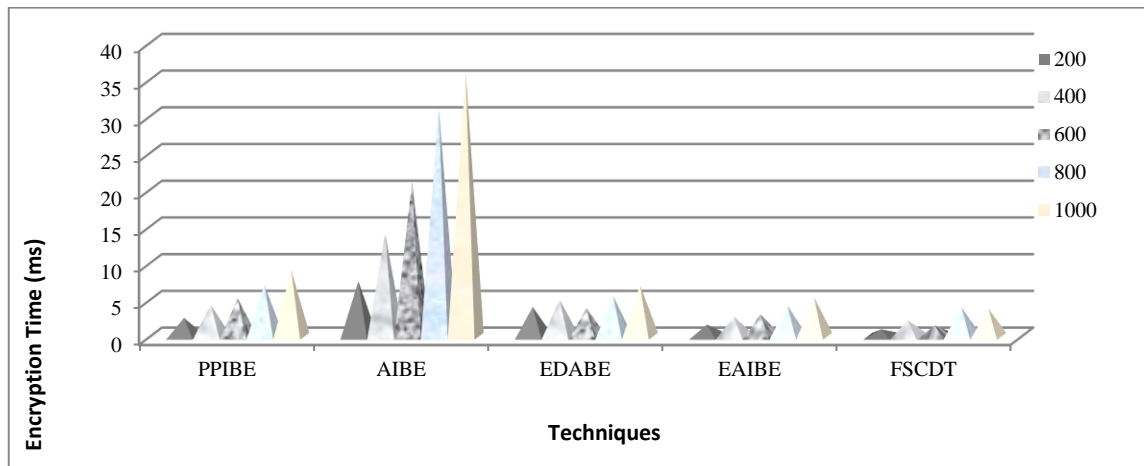


Figure 1. Encryption time (Milliseconds) for 200, 400, 600, 800, and 1,000 users

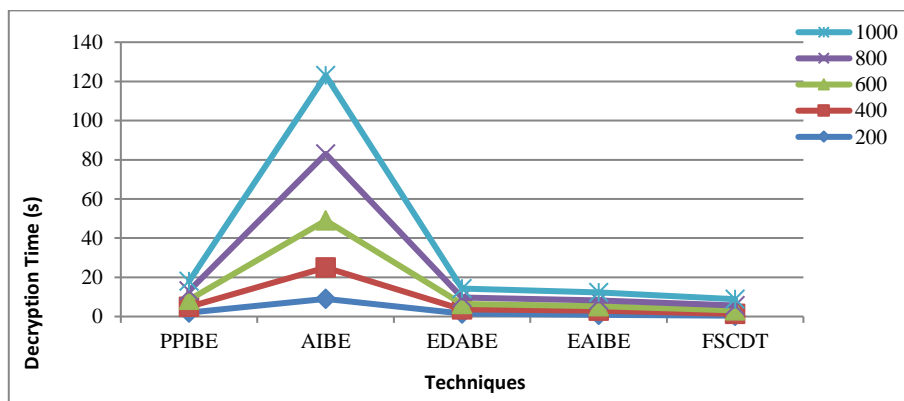


Figure 2. Decryption time (seconds) for 200, 400, 600, 800, and 1,000 Users

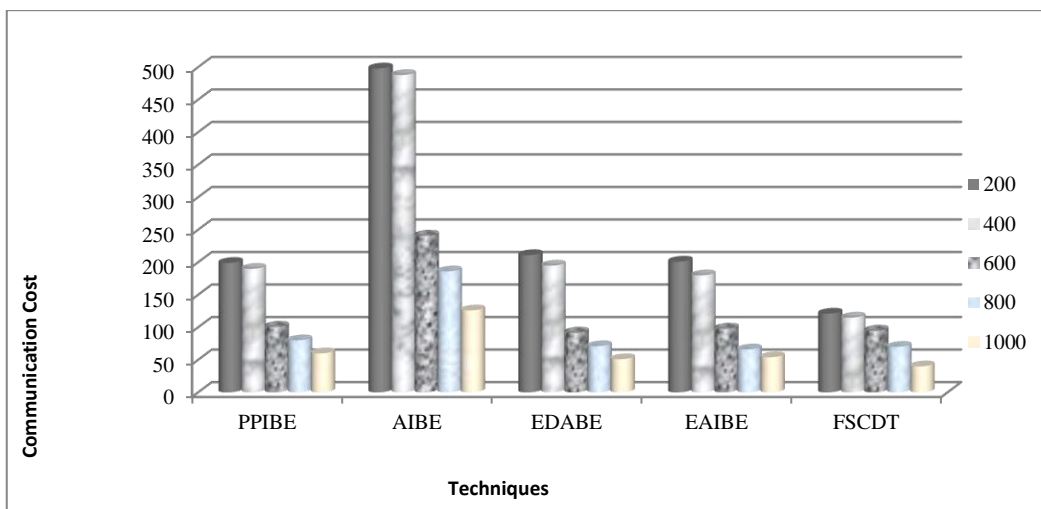


Figure 3. Communication cost for 200, 400, 600, 800, and 1,000 users

To operate unscrambling effectively, the revoked user character data ought to be joined as an aspect of cipher text and regarded publicly, which probably would not be desired in certain applications. The authorized user may easily and safely safeguard the encoded message. Proposed technique reduces 0.88 encryption time, 0.68 decryption time and 31.6% Communication value for 200, 400, 600, 800, and 1,000 Users. Hence, it can be stated that proposed FSCDT algorithm performs properly on every contrast parameter and respective compare than existing methodologies.

4. CONCLUSION

In order to enable dynamic and secure data transmission broadcasting in addition to complete confidence in key authority in an unstable cloud environment, the paper introduces the FSCDT method. In the cloud storage server, the proposed scheme's privacy has been shown to be semantically impenetrable. It represents the need for the aggregatability of the hidden attribute-based FSCDT building component and offers complete security assurances. The encoded message can be safely ensured and permitted which user can obtain with details. The revocation process does not produce any data on the content of the message or the personalities of the beneficiaries. The proposed system's security is demonstrated by the fact that it is semantically impermeable in the cloud storage server. For 200, 400, 600, 800, and 1,000 Users, the proposed approach decreases 0.88 seconds of encryption time, 0.68 seconds of decryption time, and 31.6% of communication costs. Thus, it implies that the suggested FSCDT algorithm outperforms traditional FSCDT algorithm can be prolonged in enterprise network of cloud services. Where, multiple types of user from various type of cloud types and different locations of data consumer as well datacenter.





REFERENCES

- [1] M. Sohal and S. Sharma, "BDNA-A DNA inspired symmetric key cryptographic technique to secure cloud computing," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 1, pp. 1417–1425, Jan. 2022, doi: 10.1016/j.jksuci.2018.09.024.
- [2] Y. Wu, Y. Wu, H. Cimen, J. C. Vasquez, and J. M. Guerrero, "P2P energy trading: Blockchain-enabled P2P energy society with multi-scale flexibility services," *Energy Reports*, vol. 8, pp. 3614–3628, Nov. 2022, doi: 10.1016/j.egy.2022.02.074.
- [3] N. Mohammed, L. R. Sultan, and S. Lomte, "Privacy preserving outsourcing algorithm for two-point linear boundary value problems," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 16, no. 2, p. 1065, Nov. 2019, doi: 10.11591/ijeecs.v16.i2.pp1065-1069.
- [4] S. Ouhamme and Y. Hadi, "Enhancement in resource allocation system for cloud environment using modified grey wolf technique," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 20, no. 3, pp. 1530–1537, Dec. 2020, doi: 10.11591/ijeecs.v20.i3.pp1530-1537.
- [5] E. Poornima, N. Kasiviswanath, and C. S. Bindu, "Secured data sharing in groups using attribute-based broadcast encryption in hybrid cloud," in *Advances in Intelligent Systems and Computing*, vol. 841, 2019, pp. 707–718.
- [6] C. Stergiou, K. E. Psannis, B. B. Gupta, and Y. Ishibashi, "Security, privacy & efficiency of sustainable cloud computing for big data & IoT," *Sustainable Computing: Informatics and Systems*, vol. 19, pp. 174–184, Sep. 2018, doi: 10.1016/j.suscom.2018.06.003.
- [7] R. Rabaninejad, M. H. Ameri, M. Delavar, and J. Mohajeri, "An attribute-based anonymous broadcast encryption scheme with adaptive security in the standard model," *Scientia Iranica*, vol. 26, no. 3 D, pp. 0–0, Oct. 2017, doi: 10.24200/sci.2017.4517.
- [8] V. S. Nares, M. M. Nasralla, S. Reddi, and I. Garcia-Magariño, "Quantum Diffie-Hellman extended to dynamic quantum group key agreement for e-healthcare multi-agent systems in smart cities," *Sensors*, vol. 20, no. 14, p. 3940, Jul. 2020, doi: 10.3390/s20143940.
- [9] S. Murugan, G. Babu, and C. Srinivasan, "Underwater object recognition using KNN classifier," *International Journal of MC Square Scientific Research*, vol. 9, no. 3, p. 48, Dec. 2017, doi: 10.20894/IJMSR.117.009.003.007.
- [10] Z. Qikun, L. Yongjiao, G. Yong, Z. Chuanyang, L. Xiangyang, and Z. Jun, "Group key agreement protocol based on privacy protection and attribute authentication," *IEEE Access*, vol. 7, pp. 87085–87096, 2019, doi: 10.1109/ACCESS.2019.2926404.
- [11] L. Alkharji, N. Alhirabi, M. N. Alraja, M. Barhamgi, O. Rana, and C. Perera, "Synthesising privacy by design knowledge toward explainable internet of things application designing in healthcare," *ACM Transactions on Multimedia Computing, Communications, and Applications*, vol. 17, no. 2s, pp. 1–29, Jun. 2021, doi: 10.1145/3434186.
- [12] M. M. Ismail, M. Subbiah, and S. Chelliah, "Design of pipelined Radix-2, 4 and 8 based multipath delay commutator (MDC) FFT," *Indian Journal of Public Health Research & Development*, vol. 9, no. 3, p. 765, 2018, doi: 10.5958/0976-5506.2018.00380.7.
- [13] J. Zhang and P. Ou, "Privacy-preserving multi-receiver certificateless broadcast encryption scheme with de-duplication," *Sensors*, vol. 19, no. 15, p. 3370, Jul. 2019, doi: 10.3390/s19153370.
- [14] L. Chen, J. Li, and Y. Zhang, "Adaptively secure anonymous identity-based broadcast encryption for data access control in cloud storage service," *KSII Transactions on Internet and Information Systems*, vol. 13, no. 3, pp. 1523–1545, Mar. 2019, doi: 10.3837/tiis.2019.03.023.
- [15] Q. Huang, Y. He, W. Yue, and Y. Yang, "Adaptive secure cross-cloud data collaboration with identity-based cryptography and conditional proxy re-encryption," *Security and Communication Networks*, vol. 2018, pp. 1–12, Oct. 2018, doi: 10.1155/2018/8932325.
- [16] M. Rady, T. Abdelkader, and R. Ismail, "Integrity and confidentiality in cloud outsourced data," *Ain Shams Engineering Journal*, vol. 10, no. 2, pp. 275–285, Jun. 2019, doi: 10.1016/j.asej.2019.03.002.
- [17] H. Jin, Y. Luo, P. Li, and J. Mathew, "A review of secure and privacy-preserving medical data sharing," *IEEE Access*, vol. 7, pp. 61656–61669, 2019, doi: 10.1109/ACCESS.2019.2916503.
- [18] S. Conti, S. Vaucher, R. Pires, M. Pasin, P. Felber, and L. Reveillere, "Anonymous and confidential file sharing over untrusted clouds," in *Proceedings of the IEEE Symposium on Reliable Distributed Systems*, Oct. 2019, pp. 21–31, doi: 10.1109/SRDS47363.2019.00013.





- [19] Z. Yang, W. Wang, Y. Huang, and X. Li, "Privacy-preserving public auditing scheme for data confidentiality and accountability in cloud storage," *Chinese Journal of Electronics*, vol. 28, no. 1, pp. 179–187, Jan. 2019, doi: 10.1049/cje.2018.02.017.
- [20] S. Chentharra, K. Ahmed, H. Wang, and F. Whittaker, "Security and privacy-preserving challenges of e-health solutions in cloud computing," *IEEE Access*, vol. 7, pp. 74361–74382, 2019, doi: 10.1109/ACCESS.2019.2919982.
- [21] K. Anitha and T. Gopalakrishnan, "Data storage lock algorithm with cryptographic techniques," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 9, no. 5, p. 3843, Oct. 2019, doi: 10.11591/ijece.v9i5.pp3843-3849.
- [22] J. Sun, H. Xiong, H. Zhang, and L. Peng, "Mobile access and flexible search over encrypted cloud data in heterogeneous systems," *Information Sciences*, vol. 507, pp. 1–15, Jan. 2020, doi: 10.1016/j.ins.2019.08.026.
- [23] D. Li, J. Liu, Z. Zhang, Q. Wu, and W. Liu, "Revocable hierarchical identity-based broadcast encryption," *Tsinghua Science and Technology*, vol. 23, no. 5, pp. 539–549, Oct. 2018, doi: 10.26599/TST.2018.9010023.
- [24] J. Harikumar and A. R. Gottimukkala, "Constrained preserve ABE with access control in mobile clouds," *International Journal For Technological Research In Engineering*, vol. 5, no. 7, pp. 3229–3233, 2018.
- [25] A. Unnikrishnan and V. Das, "Cooperative routing for improving the lifetime of wireless Ad-Hoc networks," *International Journal of Advances in Signal and Image Sciences*, vol. 8, no. 1, pp. 17–24, Jan. 2022, doi: 10.29284/ijasis.8.1.2022.17-24.
- [26] L. V. Silva, P. Barbosa, R. Marinho, and A. Brito, "Security and privacy aware data aggregation on cloud computing," *Journal of Internet Services and Applications*, vol. 9, no. 1, p. 6, Dec. 2018, doi: 10.1186/s13174-018-0078-3.

BIOGRAPHIES OF AUTHORS



Ezhilarasan Elumalai     is a Research scholar from school of Information Technology and Engineering at Vellore Institute of Technology, Vellore, India. He has received Masters in Computer Science Engineering at SCSVMV University in Kanchipuram, India. He has received his UG in Computer Science Engineering at Anna University Chennai, India. He has 4+Year of teaching and industrial experience in various organizations in TamilNadu, India. He published 4 articles in major indexing (Scopus and Web of Science) journals. He participated in many international/national Conferences, workshop seminar and guest lecturers among various institutions in India. His research interests in cloud security, mobile computing, cloud computing and mobile networks. He can be contacted at email: e.ezhilarasan2016@vitstudent.ac.in.



Dr. Dinakaran Muruganandam     is working as Professor at the School of Information Technology and Engineering, Vellore Institute of Technology, Vellore, India. He received his Ph.D award from Anna University Chennai and he received UG and PG degree in Vellore Institute of Technology, Vellore, India. He has over 14 years of academic experience in various institutions. He published 52 articles in major indexing (Scopus and Web of Science) journals. He participated in many international/national Conferences, workshop seminar and guest lecturers among various institutions in India. His research interests are in Mobile computing, cloud computing mobile networks, mobile IP, IPv6, mobile telephony. He can be contacted at email: dinakaran.m@vit.ac.in.