STE-AMM: Secret Twist Encryption Standard Access Mechanism Model in Cloud Environment

Sameer and Harish Rohil
Department of Computer Science & Applications, Chaudhary Devi Lal University, Sirsa-125055, India
Email: {asameer1982; harishrohil2}@gmail.com.

Abstract —The advent of the cloud computing has provided the opportunity for various organizations and enterprises to store the data effectively at low cost. With the advancement, the cloud environment manages to have mutli-users to access the data in the cloud based on their request. The requests and the activities of users are monitored and controlled by the group manager based on the roles of them. However due to the dynamic nature of the multi -user clouds result in challenges for ensuring the security of the cloud. Additionally, the revocation of existing users often results in increased overheads. A novel framework of Secret Twisted Encryption based access mechanism model (STE-AMM) is proposed to resolve these issues with two modules. The Square Decisional Diffie-Hellman (SDDH) technique is employed to generate the digital signature for users and used to govern the user in group module. The secret keys to secure the data is generated with the STE algorithm which is the improved Advanced Encryption Standard (AES) and used in the data module. The proposed STE-AMM framework is implemented and evaluated with the metrics of time and cost. The obtained results showed that the performance of the proposed framework is effective than the existing models for securing the data in the cloud. The proposed framework may be enhanced with random size for signature and security key.

Index Terms—Cloud computing, Multi-users, STE-AMM, SDDH, group module, data module

I. Introduction

Cloud Computing is the most significant technology that are established to store and supply the resources over the request through internet. The cloud computing is providing major benefits of scalability and accessibility for effective resource management [1]. Cloud computing provides much more effective computing by centralized memory, processing, storage, and bandwidth. Cloud computing is a term to describe a technology that distributes computer services away from a local client [2]. In general, three different types of cloud setups that involves third party based public cloud, organization based private cloud and the integrated hybrid cloud [3]. Each types of cloud serve their distinct purposes to support its clients. The major barriers for adapting the cloud computing is its security issues. Cloud service providers have been concerned of the non-adequate security measures and aspects like data integrity, control, audit, confidentiality, availability should be added [4]. Practitioners of cloud technologies from around the world indicated that the biggest challenges of using cloud computing technology within their organizations were related to security. Around 83 percent of respondents found security to be a significant challenge or somewhat of a challenge.

Encryption is used as a data confidentiality assurance measure, the management of cryptographic keys is a critical and challenging security management function, especially in large enterprise data centers, due to sheer volume and data distribution and the consequent number of cryptographic keys [5]. The loss of encryption key or privileged access code will bring serious problems to the cloud service users. Accordingly, lack of cryptographic management information such as encryption keys, authentication codes and access privilege will heavily lead sensitive damages on data loss and unexpected leakage to outside [6]. Especially in the multi-user cloud environment, the prevention on data through key leakage is inevitable. Moreover, there is some development on preventing the attacks against the data stored in clouds and maintaining its integrity [7]. Even though the cipher text policy (CP) and attribute-based encryption provide some enhance security it is found to be some attributes result in leakage of sensitive data [8].

For ensuring the security of the data in the cloud, a novel framework of Secret Twist Encryption Standard Access Mechanism Model (STE-AMM) id proposed. The proposed framework includes the three different layers for securing the data over the confidentiality, integrity and privacy issues. The proposed framework is provided with effective access control with resource allocation for the users. The proposed framework also provides revocation of user in the cloud environment.

The major goal of the proposed framework is to secure the data in the cloud effectively to ensure the better user control mechanism. The following contributions are performed to achieve the paper goals.

- We achieve the fine-grained-ness, high efficiency on the data owner’s side, and standard the data confidentiality, data privacy, data integrity of secure cloud data sharing.
- We achieve the user revocation in data sharing for resource limited users in cloud computing.
- We prevent from Brute force Attack, Dictionary Attack, SQL Injection Attack, collusion Attacks, and Side Channel Attacks.

Manuscript received August 12, 2020; revised February 8, 2021.
doi:10.12720/jcm.16.3.111-117

- We perform New Mathematical STE-AMM Cryptographic System to Secure the Cloud Environment.

The present paper is structured in the following order as: work related to data security in cloud is discussed in Section 2. The preliminaries for the proposed frameworks are deliberated in Section 3. The architecture of the proposed framework with the system and security model in Section 4. Section 5 deliberates the algorithms in the system. Section 6 provides the implementation details for the system prototype and its performance and the final section concludes the proposed work with the future proposal.

II. Related Works

In [9] proposed a model of protecting the privacy of the user to generate signatures by using third-party medium (TPM). The TPM is employed to develop a simple model for auditing integrity remotely. The TPM has an expiration time for authorization with a valid period. In [10] introduced a scheme of user revocation without affecting the blocks held by the revoked user. Instead of focusing on the verifiers of the revoked user the model focused on updating the non-revoked group keys. The scheme is made on ID cryptography it does not need certificate management as needed in Public Key Infrastructure (PKI) systems. a scheme was introduced with critical information hiding. It is a remote auditing scheme that uses a cleanser to mask critical information on the blocks while enabling remote integrity auditing. The scheme is based on ID cryptography [11].

The AES algorithm along with the verifiable key block cipher is employed in the cloud environment to protect the cache from time-based attacks. It was a collaborative solution that provides data integrity and prevent the attacks effectively [12]. Another AES algorithm-based framework to secure the data in the cloud is proposed with Pretty Good Privacy (PGP) algorithm and Secure Socket Layer (SSL). The proposed algorithms supported the cloud server and the network channel with greater security. The security was ensured with distinct secret key for both encryption and decryption other than public key. The framework provided better confidentiality for data in the cloud [13]. Similarly using SSL and PGP based framework for securing the data is proposed with triple AES algorithm. It has better performance than the earlier model, but the time consumption is high with lot of key generators in the system [14].

A third-party auditor is employed for enhancing the security of cloud through implementation of the AES algorithm. The auditor controls the data access of the user whereas the AES encryption technique protect the data during transfer. The AES algorithm in the proposed model ensures the availability of cloud during the storage of huge data in it [15].

A lightweight public auditability scheme with TPA is formulated to support the dynamics of data and public verifiability to secure the data in the cloud. This scheme provided the user some permission to carry out initialization with low computational overhead. The proposed framework supports the batch auditing with effective storage [16]. An AES based encryption scheme was proposed with hybrid steganography and SHA-2 to protect the image data in the cloud. The proposed framework was observed to be reliable and highly secure with effective security analysis [17]. The combined AES And blowfish algorithm is proposed to secure the cloud with short message service that provide confidentiality, verification and authentication for data. The proposed scheme provided the security for cloud data without cloud service provider. The main drawback is that the proposed scheme is applicable only for text data [18]

The CPABPRE system was employed to tackle the CCA problem in the existing models with selective access structure and chosen-ciphertext along with the encryption of sharing cloud data. The model was proved under the assumption of the decisional q-parallel Bilinear Diffie Hellman Exponent. The entire framework was implemented through the Random Oracle model only [19]. An efficient revocation of the user was achieved through the implementation of the secure scheme for data sharing, Mona. This scheme was established with the formation of the revocation list, and there was no key updation for remaining users, and there was no variation in the storage overhead and computation cost [20].

III. Preliminaries

A. Bilinear Mapping

Bilinear Mapping was employed extensively in the cryptography and signature generation in securing the data in the cloud environment [21]. Let Ga, Gb be an additive group and a Prime Orders multiplicative cyclic group respectively, then the bilinear map that exist between Ga and Gb is given based on the following theories as,

a) Bilinear – and x,y Ga, e (lx,my) = e(x,y)lm for all

b) Non-degenerate- it will exist only at a point where e (Ga, Gb) $\neq$ 1

c) Computable- to estimate e (l,m) for any l,m Ga

B. Mechanism for Signature Generation

The signature generation in the proposed framework is carried out through the square based decisional Diffie-Hellman algorithm (SDDH). For the given large cyclic group of G over the prime order group q, there are two different distribution for signature generation as follows:

a) SDDH triple-, where

b) Random triple- where m, l

In the above distributions both m and l are selected randomly form the uniform random.

c) Advanced encryption standards

The AES is the one of the standard symmetrical cryptography that are employed to encrypt and decrypt the data in the cloud environment. In general, the AES algorithm operates with the 4X4 matrix and involves for steps for both encryption and decryption of data.

Sub bytes – This form the first step in AES, a value among the 16 inputs in the matrix is replaced with the value of another matrix. It can be achieved through multiplicative inverse followed by affine transformation

Permutation - The next step in the AES is the shifting of the rows of input matrix into column. It is performed over the all the rows except the first row. It is generally achieved through shift left. Mixing- In this step the shifted matrix is generally multiplied with the common polynomial. This process will yield the new matrix with 16 different input values.

Add Round key- It is the final step of AES; it involves the bitwise XOR function over the two sub keys in the similar state.

IV. System Architecture and Security Model

Let us consider the users X, Y, Z and they provide the request to the cloud administrator to access the cloud. The cloud administration performs the registration process for the requested user and provide the computed digital signature for the user to access the cloud (See Fig. 1).

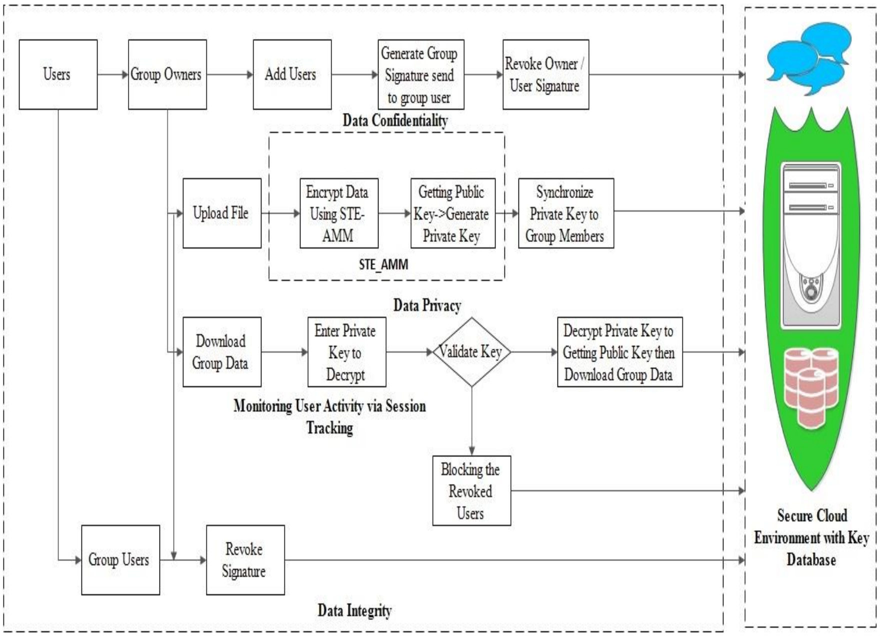
Users
Group Owners
Add Users
Generate Group Signature send to group user
Revoke Owner / User Signature
Data Confidentiality
Upload File
Encrypt Data Using STE-AMM
Getting Public Key->Generate Private Key
Synchronize Private Key to Group Members
STE_AMM
Data Privacy
Download Group Data
Enter Private Key to Decrypt
Validate Key
Decrypt Private Key to Getting Public Key then Download Group Data
Monitoring User Activity via Session Tracking
Blocking the Revoked Users
Group Users
Revoke Signature
Data Integrity
Secure Cloud Environment with Key Database

Fig. 1. Proposed system architecture and security model

When the user request for the data access they are provided with the public key and private key based on the roles by the data owners in the cloud environment. The keys are generated with the secret twists over the generated key matrix in AES. There are two order of key generation over with values of 1 and -1. The orders are assumed randomly by the cloud administrator. The digital signature and the cryptography keys are stored into the key database. The cloud administrator verifies the digital signature and security keys before allowing the user to access the cloud. The cloud administrator monitors the user activity and provides the report to eth data owner in the frequent manner. The data owner audits the user activity. When the user tries to manipulate or perform any unauthenticated activity, the data owner may revoke the signature of the users. This result in removal of signature and keys through the updation of key database.

In the proposed model, the security for the given data in the cloud is established through the two modules. They provided the security through the following aspects:

Data confidentiality- Each user in the cloud environment is provided with the distinct group signature at the time of registration to access the cloud. The cloud administrator approves the user to either access the cloud only after the verification of the digital signature. The group signature generated through the SDDH ensure that only authenticated person can access the cloud and it ensure the confidentiality of data in the cloud environment.

Data privacy- Similar to the digital signature, each user is provided with the common public key to access the data in the cloud. The distinct secret key for both encryption and decryption are generated through the proposed STE algorithm. Any user can access the cloud data only through their private key. This validates the privacy of data in the proposed architecture. Additionally, when the user is revoked using the digital signature, the keys are eliminated from eth key database and no other user can employ those keys to access the data.

Data integrity- The integrity of the data is to protect it from any manipulation from any user in the cloud. The proposed framework monitors the user activity and revoke the user who involves in the unauthorized activity. This provides the required data integrity to the data in the cloud environment.

V. System Algorithms

The proposed security architecture involves the following process:

Setup (1P, N): Let P be the security parameter for the with the maximum set size of receiver (N). with both the security P and N, the public and master key is obtained a and are designated as PK and MK through the cloud auditor

INUser (UID, IDG): The user with their identity UID is added to the group with the identity IDG and is performed through group manager GM. The inclusion of user defines the role parameter RP and listed role LR of user in the organized cloud

SignGen (UID, MK): the generated master key MK along with the UID is employed to generate the user digital signature UDS along with verifying message VM.

RoleManage (MK, UHR, RS): The master key MK along with the hierarchical role of user UHR with role set RS that maintain the group secrecy provide the Public parameters set PPS for the cloud user.

EXUser (UID, IDG, UDS): The user identity UID that are listed in the group with identity IDG can be revoked using the removal of the User Digital Signature UDS result in the elimination of the RP and LR of user and the cloud key database is updated.

KeyGen (MK, UID, AP, KM): Using the generated master key MK and the identity of the user with the access policy AP and the obtained key matrix KM. The twisting process with the value of +1 and -1 is performed randomly to generate the private key PrK.

En (M, UIS, AP): With the message M along with the access policy AP over the user identity set UIS, the data is encrypted EcD

De(UID, PrK, EcD): The encrypted data EcD is downloaded from the cloud with the user identity UID along with the private key PrK, it is decrypted to obtain the data (DcD)

A. Construction of Algorithm

Initial setup: The cloud administrator initiates this algorithm and obtain the security parameter P from along with the receiver set N. Using the bilinear technique, the public key PK and the master key MK for the cloud data is generated.

Include of User: Once the user sent their request to the cloud administrator using the user identity UID and group identity IDG, the group manager designate the role parameter and listed role to the user.

Digital signature generation: When the user is registered in the cloud, the data owner generate the digital signature for the each user in the group. The UID and MK are employed to generate the user digital signature (UDS) with the message VM.

Verify UDS, VM: The user is verified with the digital signature along with the verifying message and allowed to access the cloud

Group management: Since the cloud may have different hierarchical roles for the users, the role set is preserves to maintain the secrecy of the ancestral roles of the users to generate the public parameter PP with the role-based attributes.

Exclusion of user: The revocation is the reverse process of adding the user to the cloud. The user digital signature UDS is revoked along with the user and group identity. This result is removal of concerned user keys in the key database and updated.

Key generation

The key generation in the proposed method is carried out with the secret Twisted Encryption which is the improved version of Advanced encryption standards. In the proposed framework, a 512 byte AES is used with 10 rounds and are explained below.

Subbytes: The AEs is initiated with the matrix A and the sbox. The keys from The S box is used for replacing the values in the matrix A is given as in equation 1 and 2.

Matrix A

$$A = \begin{bmatrix} \mathrm{A} & \mathrm{B} & \mathrm{C} & \mathrm{D} \\ \mathrm{E} & \mathrm{F} & \mathrm{G} & \mathrm{H} \\ \mathrm{I} & \mathrm{J} & \mathrm{K} & \mathrm{L} \\ \mathrm{M} & \mathrm{N} & \mathrm{O} & \mathrm{P} \end{bmatrix} \tag{1}$$

Sbox

$$S_{box} = \begin{bmatrix} \mathrm{a} & \mathrm{b} & \mathrm{c} & \mathrm{d} \\ \mathrm{e} & \mathrm{f} & \mathrm{g} & \mathrm{h} \\ \mathrm{i} & \mathrm{j} & \mathrm{k} & \mathrm{l} \\ \mathrm{m} & \mathrm{n} & \mathrm{o} & \mathrm{p} \end{bmatrix} \tag{2}$$

Let us assume that there is a substitution of two inputs in the matrix A and it is specifically in the third row second column and second row third column, then the final updated matrix A is obtained is given as in equation 3.

$$A = \begin{bmatrix} \mathrm{A} & \mathrm{B} & \mathrm{C} & \mathrm{D} \\ \mathrm{E} & \mathrm{F} & \mathrm{g} & \mathrm{H} \\ \mathrm{I} & \mathrm{j} & \mathrm{K} & \mathrm{L} \\ \mathrm{M} & \mathrm{N} & \mathrm{O} & \mathrm{P} \end{bmatrix} \tag{3}$$

Permutation operation

The next phase in the AES is the permutation of the rows 2,3 and 4 and the output matrix of these operation over A is given as in equation 4.

$$A = \begin{bmatrix} \mathrm{A} & \mathrm{B} & \mathrm{C} & \mathrm{D} \\ \mathrm{E} & \mathrm{F} & \mathrm{j} & \mathrm{H} \\ \mathrm{I} & \mathrm{g} & \mathrm{K} & \mathrm{L} \\ \mathrm{M} & \mathrm{N} & \mathrm{O} & \mathrm{P} \end{bmatrix} \tag{4}$$

Mixing operation

The obtained modified input matrix is again operated with the fixed polynomial f(x) over the same column along the column of both the matrix A and Sbox. In the present let column 3 be under the mixing operation, the element in both the matrix is subjected to the conditional XOR function to obtain the mixed column in both the matrices

Generation of round key

The round key is obtained through the XOR operation over the identically placed values in both the matrix and is added to the subkey matrix. Let us assume the following matrix as the sub key matrix with different values as in equation 5.

$$Round\ key = \begin{bmatrix} 0 & 1 & 2 & 3 \\ 4 & 5 & 6 & 7 \\ 8 & 9 & 10 & 11 \\ 12 & 13 & 14 & 15 \end{bmatrix} \qquad (5)$$

Twisting phase

Once the final sub key matrix is obtained, the cloud administrator can pick either the value of +1 or -1 randomly and based on it the secret key is generated in the specified sequence

For +1: 2 8 4 0 2 6 10 14 1 5 9 13 15 11 7 3

For -1:13 9 5 1 3 7 11 15 0 4 8 12 14 10 6 2

Encryption

EcD En (M, UIS, AP): The data uploaded to the cloud is encrypted with the details of user identity set (UIS) along with the access policy AP with the message M to yield the encrypted data EcD.

Decryption

DcD De (UID, PrK, EcD): the decryption over the encrypted data EcD is performed with the identity of the user and the corresponding private key PrK which is verified with the key database to obtain the decrypted data DcD.

VI. Result and Discussion

The proposed security framework over the data in the cloud is implemented using Java and the data are accumulated in the dropbox. The interfaces in the cloud are achieved through the JAX-WS web services hosted with Apache Tomcat. The SQL database is updated at the server side for storing the data. A Java supported internet browser forms the client side. The remaining basis configuration is to use the intel processor with memory of 16 GB at 2.45 GHz with a disk of 1TB capacity.

Performance of proposed Framework

A. *Digital Signature*

In the proposed framework each and every user in eth cloud is provided with the distinct digital signature that are generated and stored in the key data base. The cloud administrator verifies the signature of each user before allowing them to access the cloud. The signature generation in the proposed framework is carried out through the SDDH approach. The time consumed for generating the signature is observed to increase with eth number of users. Similar to the generation time the proofing time for signature increases with increase in number of users. The Fig. 2 shows the performance of the signature generation technique over increasing number of user in the proposed cloud environment.

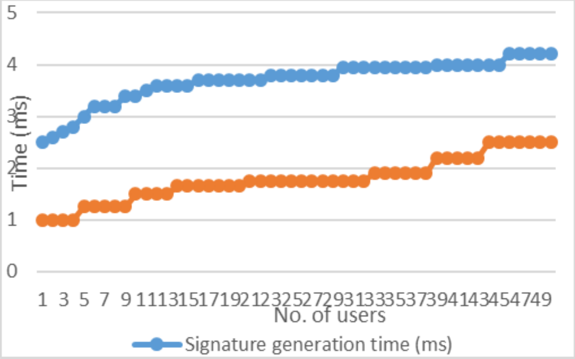

Fig. 2. Signature generation and proofing time

B. *Uploading and Encryption*

One of the major functions in any cloud environment is to upload the data in the cloud and for security purpose it requires to be encrypted. In the proposed framework, a novel STE algorithm is employed to perform the encryption of data in the cloud. The upload time for clouds over different file size in the proposed framework is given in Table I. The upload time increases slightly over increasing file size. The encryption time for the data in the cloud increases with file size to be encrypted. The computation cost for encrypting the size in the proposed framework is about the product of role list and the Bilinear based multiplication operation. The time involved in both uploading and encryption over different file sizes is plotted in Fig. 3.

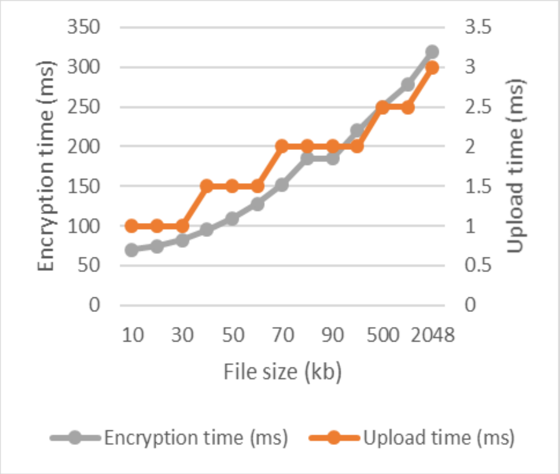

Fig. 3. Upload time and encryption time performance over different file size

C. *Downloading Decryption Performance*

The user required to download the encrypted data from the cloud and decrypt it to access the information in it. The download time for different size of file is given in Table I. Similar to the upload time, the download time for the encrypted data increase slightly with increase in file size. The decryption time for the file sizes are given in Table I. The decryption time for the data in the proposed framework is higher than the encryption time and it increases with increase in the file size. The decryption cost of the data in the proposed framework is twice the summed product of complexity with the operations of pairing, exponential and multiplication. The time for both the decryption and download of data is given in Fig. 4.

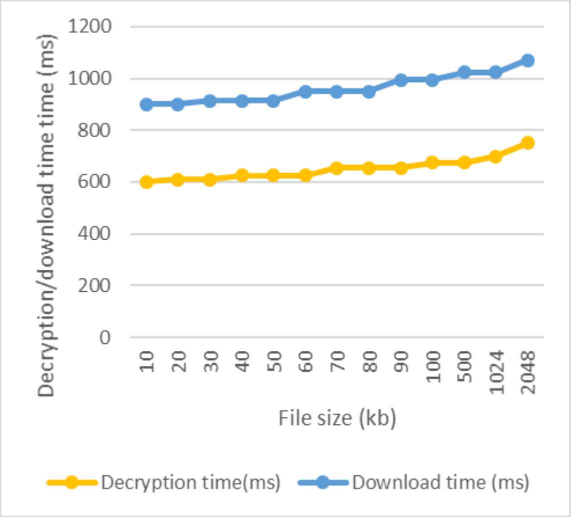

Fig. 4. Decryption and download time over different file size

D. Comparison with the Existing Framework

TABLE I. PERFORMANCE COMPARISON

Parameter/ frameworks	HW [22]	ADBS [23]	Proposed STE-AMM
Encryption cost	(l_a+ 1) M	(l_a+ 2) M	(LR) M
Decryption cost	3kP + 2kE + 3kM	3kP + 2kE + 3kM	2k (P + E + M)
Parameter size	(3k+1) $l_G + l_{G_T}$	(3k+2) $l_G + l_{G_T}$	(3k+4) $l_G + l_{G_T}$

where la is the attribute list, LR is the role list, k is the access structure complexity, represent the size of element G And. M, P and E are the multiplication, exponential, and pairing operators.

The proposed framework is analyzed with the existing HW [22] and ADBS [23] frameworks. The cost involved in both the encryption and decryption process is compared which showed that the proposed STE-AMM framework is effective with low cost than the existing frameworks. The parameter size in the proposed framework is bigger than the existing models.

VII. CONCLUSION

For securing the data in the multiuser cloud, a novel STE-AMM framework was proposed. The proposed framework employs the improved AES algorithm to secure the cloud data. The proposed framework provides all the assurances for secure data in the cloud environment. All the registered users are provided with the digital signature that is computed through the SDDH technique. The public key and the master keys of the users are generated through the cloud administrator. The data owner encrypts the data in the cloud using the STE algorithm and store it in the cloud. When the user wants to access the encrypted file, they must provide the appropriate secret key to decrypt the data. The activity of the user in the cloud is monitored continuously by the group manager. The framework is provided with the revocation policy through which any user can be revoked from the group for unauthorized activities. The proposed framework is evaluated for its performance through the time and cost-based analysis. The time taken for uploading, downloading, encrypting and decrypting of data increased steadily with increase in file size of the user. The signature generation and proofing time also increased gradually. The proposed framework is compared with the existing framework with the cost metrics and the size of parameter involve. From the comparison it is observed that the proposed STE-AMM is effective than the existing models. The future scope of the proposed framework is to employ randomized key size both for signature and keys for user which may improve the security of data to a higher-level

CONFLICT OF INTEREST

Conflict of interest the authors declare that they have no conflict of interest.

AUTHOR CONTRIBUTIONS

Sameer and Harish Rohil conceptualized and designed research. Sameer contributed in data collection, experimentation, interpretation and manuscript writing. Harish Rohil supervised the experimentation, analysis and in manuscript drafting. Both authors read and approved the manuscript

REFERENCES

[1] J. Li, W. Yao, Y. Zhang, H. Qian, and J. Han, "Flexible and fine-grained attribute-based data storage in cloud computing," *IEEE Transactions on Services Computing*, vol. 10, no. 5, pp. 785–796, Sep. 2017.

[2] L. Badger, Cloud Computing Synopsis and Recommendations : Recommendations of the National Insititute of ... Createspace, 2012.

[3] S. Tabassam, "Security and privacy issues in cloud computing environment," *Journal of Information Technology & Software Engineering*, vol. 07, no. 05, 2017.

[4] J. Sen, "Security and privacy issues in cloud computing," in *Cloud Technology: Concepts, Methodologies, Tools, and Applications*, 2015.

[5] R. Chandramouli, M. Iorga, and S. Chokhani, "Cryptographic key management issues and challenges in cloud services," *Secure Cloud Computing*, pp. 1–30, Dec. 2013.

[6] D. K. Malviya and U. K. Lilhore, "Survey on security threats in cloud computing," *International Journal of Trend in Scientific Research and Development*, vol. 3, no. 1, pp. 1222–1226, Dec. 2018.

[7] Z. Wang, “Provably secure key-aggregate cryptosystems with auxiliary inputs for data sharing on the cloud,” *Future Generation Computer Systems*, vol. 93, pp. 770–776, Apr. 2019.

[8] X. Mao, X. Li, X. Wu, C. Wang, and J. Lai, “Anonymous attribute-based conditional proxy re-encryption,” *Network and System Security*, pp. 95–110, 2018.

[9] W. Shen, J. Yu, H. Xia, H. Zhang, X. Lu, and R. Hao, “Light-weight and privacy-preserving secure cloud auditing scheme for group users via the third party medium,” *Journal of Network and Computer Applications*, vol. 82, pp. 56–64, Mar. 2017.

[10] Y. Zhang, J. Yu, R. Hao, C. Wang, and K. Ren, “Enabling efficient user revocation in identity-based cloud storage auditing for shared big data,” *IEEE Transactions on Dependable and Secure Computing*, pp. 1–1, 2018.

[11] W. Shen, J. Qin, J. Yu, R. Hao, and J. Hu, “Enabling identity-based integrity auditing and data sharing with sensitive information hiding for secure cloud storage,” *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 2, pp. 331–346, Feb. 2019.

[12] R. Saxena and S. Dey, “Data integrity verification: a novel approach for cloud computing,” *Sādhanā*, vol. 44, no. 3, Mar. 2019.

[13] K. Arul, *et al*. Efficient cloud computing with secure data storage using AES and PGP algorithm. [Online]. Available:http://ijcsit.com/docs/Volume%208/vol8issue6/ijcsit2017080601.pdf

[14] V. Sangeetha and D. Jagadeeshwari, “Enhancing the security of the cloud computing with triple Aes, Pgp Over Ssl algorithms,” *Rev. Res.*, vol. 7, no. 12, pp. 1–9, 2018.

[15] K. M. Akhil, M. P. Kumar, and B. R. Pushpa, “Enhanced cloud data security using AES algorithm,” in *Proc. International Conference on Intelligent Computing and Control*, 2017, pp. 1-5.

[16] A. Li, S. Tan, and Y. Jia, “A method for achieving provable data integrity in cloud computing,” *The Journal of Supercomputing*, vol. 75, no. 1, pp. 92–108, Jan. 2016.

[17] G. Mahmood, D. Huang, A. Baidaa, and Jaleel, “Achieving an effective, confidentiality and integrity of data in cloud computing,” *International Journal of Network Security*, vol. 21, no. 2, pp. 326–332, 2019.

[18] U. Pius, C. Onyebuchi, O. Chinasa, and E. Adoba, “A cloud-based data security system using Advanced Encryption (AES) and blowfish algorithms,” *Journal of Scientific and Engineering Research*, vol. 5, no. 6, pp. 59–66, 2018.

[19] K. Liang, *et al*., “A secure and efficient ciphertext-policy attribute-based proxy re-encryption for cloud data sharing,” *Future Generation Computer Systems*, vol. 52, pp. 95–108, Nov. 2015.

[20] X. Liu, Y. Zhang, B. Wang, and J. Yan, “Mona: Secure multi-owner data sharing for dynamic groups in the cloud,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 6, pp. 1182–1191, Jun. 2013..

[21] Q. Huang, Y. Yang, and J. Fu, “Secure data group sharing and dissemination with attribute and time conditions in public cloud,” *IEEE Transactions on Services Computing*, p. 1, 2018.

[22] S. Hohenberger and B. Waters, “Online/Offline attribute-based encryption,” Public-Key Cryptography – PKC 2014, pp. 293–310, 2014.

[23] J. Li, Y. Zhang, X. Chen, and Y. Xiang, “Secure attribute-based data sharing for resource-limited users in cloud computing,” *Computers & Security*, vol. 72, pp. 1–12, Jan. 2018.

Copyright © 2021 by the authors. This is an open access article distributed under the Creative Commons Attribution License (CC BY-NC-ND 4.0), which permits use, distribution and reproduction in any medium, provided that the article is properly cited, the use is non-commercial and no modifications or adaptations are made.

Dr. Harish Rohil presently working as Associate Professor in Dept. of CSE, Ch. Devi Lal University, Sirsa, Haryana (India) started his career as Asst. Professor in 2004. He has worked as officiating Registrar in addition to other charges of Dean, Faculty of Physical Sciences and Chairperson, Dept. of CSA in Ch. Ranbir Singh University, Jind (Haryana) in 2014-15. He obtained his Ph.D. from Department of Computer Sc. & Applications, Kurukshetra University, Kurukshetra in 2012 and his M.Tech. (CSE) from Guru Jambheshwar University of Sc. & Technology, Hisar in 2004. He has published 76 research papers in national and international journals. He has presented 45 research papers in conferences held in India and abroad. He was awarded Young Scientist Award in 2014. He has filed two patent applications under Govt. of India. His research interests include software reuse, data mining, data structure and operations research.

Email: harishrohil@gmail.com

Sameer presently working as an Assistant Professor in Dept of CSE, Shah Satnam Ji P.G Boys College, Sirsa, Haryana (India) and he started his career as Asst. Professor in 2014. He has worked before in various companies. He obtained his B.Tech (I.T). from Kurukshetra University, Kurukshetra in 2004 and his M.Tech. (I.T) from Guru Gobind Singh Indraprastha University in 2007. and now pursuing Ph.D form Chaudhary Devi Lal University, SIRSA, Haryana. He has published various research papers in national and international journals. His research interests include cloud computing, data mining etc.