EDES-ACM: Enigma Diagonal Encryption Standard Access Control Model for Data Security in Cloud Environment

Sameer[1]
Ph.D Scholar
Department of Computer Science and Applications
Chaudhary Devi Lal University, Sirsa-125055(India)

Dr. Harish Rohil[2]
Associate Professor
Department of Computer Science and Applications
Chaudhary Devi Lal University, Sirsa-125055(India)

***Abstract*—The data management across the different domains is the foremost requirement for many organizations universally. The organization establishes the cloud computing paradigm to handle the data effectively due to its robust scaling at a low cost. In recent times the usage of cloud and its data is increasing with the multiuser environments. This resulted in the issue of ensuring the security of data in the cloud environment uploaded by the owners. The cloud service providers and researchers implemented several schemes to ensure data security. However, the task of providing security with multiuser remains tedious with data leakage. A novel Enigmatic Diagonal Encryption Standard (EDES) algorithm to provide access control over the cloud is proposed. The framework with the proposed algorithm is named as EDES-ACM. The Inverse Decisional Diffie Hellman (IDDH) technique is used for generating the signature of the group. The data is encrypted with the EDES algorithm by the data owner. The encrypted data is provided to the user and is accessed by the EDES based private key. The group manager monitors the cloud and provides the activity report to owners based on which the revocation is performed. The framework is validated for its performance on security parameters and compared with the existing models on computation cost. The EDES-ACM framework is effective with low computation cost. The future notion for the proposed framework is to include the block chain technology that may improve the security and better accumulation of data.**

Keywords—Cloud; security; multiuser; EDES-ACM; computation cost

I. INTRODUCTION

Cloud computing (CC) has emerged in the various platforms to provide services at flexible time and place with internet connection [1]. Many organizations and enterprises establish cloud as the effective solution with low cost, rapid scaling. The only concern for the data owners is that the cloud service providers have to guarantee the privacy and security of data to remain secure and confidential among the dynamic cloud environment [2]. Most of the CSP's rely on the third-party operation in storing the data that are case sensitive. Henceforth the cloud user must trust the CSP or employ the effective system in the cloud infrastructure to improve the security of data in the cloud [3]. Several standards for cloud security are developed and suggested by standard bodies like the National Institute for Standards and Technology (NIST) [4]. However, the Multi-user cloud environment demands distribution and sharing with integrating applications that are available either internally or externally. These aspects pose a critical challenge over the integrity, authenticity of cloud data [5].

Many novel algorithms are proposed for securing the data in the multi-user cloud environment to confirm the data integrity with privacy preserving approaches [6] and several other approaches. One among the effective approach is to provide either the symmetric or asymmetric group key. Using the keys, the data owners can encrypt the data and store it in the cloud. The user decrypts the data after downloading to access it. In symmetric keys, both cryptic keys are similar and it is dissimilar in unsymmetrical keys [7]. Even with cryptic keys, the data security is under threat with possible key leakage and cyber-attacks in a multi-user cloud environment [8]. The role-based access approach that is established with the ciphertext policy and attribute-based encryption are subjectable to data leakage with some access permissions [9].

For secure data management in the cloud environment, a novel Enigma Diagonal Encryption Standard Access Control Model (EDES-ACM) is proposed. The model of EDES-ACM is implemented to examine the environmental data in the effective manner and providing a better Unbreakable Secure Data Sharing Environment in Cloud Computing. The proposed EDES algorithm is the improved form of symmetric Advanced Encryption standards with enigmatic diagonal based key generation. The proposed model secures the cloud data effectively by ensuring data security with proper revocation mechanism.

The following contributions are provided to secure the cloud data through the proposed EDES-ACM model:

1) The data security is achieved through very fine-grained access control in Multiuser sharing in a cloud environment.

2) The new mathematical approach for EDES-ACM Cryptographic System is proposed to secure the data.

3) The proposed model is provided with the effective revocation mechanism for revoking the user who performs any unauthorized activities.

4) The proposed cloud set up is protected from the Dictionary Attack, Brute force Attack, and many more.

The present paper is structured in the following order as: Work related to data security in the cloud is discussed in Section 2. The preliminaries for the EDES-ACM frameworks are deliberated in Section 3. The architecture of the EDES-ACM framework with the system and security model in Section 4. Section 5 deliberates the security framework in the EDES-ACM system. Section 6 provides the algorithm and Section 7 details the implementation for the system prototype and its performance and the final section concludes the proposed work with the future proposal.

II. Related Works

A survey on the performance of some security algorithms in providing security to the cloud is discussed. The work deliberated various clouds that includes the private, community and hybrid cloud. Some research works are selected and related to the encryption mechanism and security of clouds. The comparative studies showed that the performance of AES is better than that of RSA [10]. A chaos-based hybrid AES encryption algorithm was proposed for secure cloud data. An assessment of hybrid algorithms was developed previously revealed that only some portions of the algorithm is employed for chaotic systems. However, in the proposed system many parts of the AES algorithm were involved in chaos structuring [11]. The AES area optimization was accomplished by establishing the mapping among the path hardware of lower data and transformations through the architecture of the iterative loop. The outcomes obtained showed that the proposed architecture of AES is appropriate for its usage in resource constrained systems [12]. An AES algorithm is modified and proposed with an increase in the number of rounds (16) and key size (320 bits) with Polybius square. The main benefit was increased security in high speed data transmission and its drawback was more computational time [13].

An assignment scheme with a hierarchical key was recently proposed [14]. Contrasting with some established schemes that generally encloses a single secret key and few public information to process the decryption process, the proposed system did not share any public information as it is based on access policy chain partitions. A system was developed with a large attribute universe-based access control with the unconstrained flexible attributes of system and space that outsourced cloud decryption. The outcome showed that the developed scheme enhanced the backward secrecy through an effective revocation mechanism but lacked performance in the cryptic mechanism [15]. With decryption outsourcing, a new multi-authority ciphertext policy ABE (MA-CP-ABE) scheme was developed. The implemented outcomes showed that the scheme was efficient, scalable and securable. The scheme was supportable and adaptive for monotone linear secret sharing scheme access policy [16]. A group management system based on lazy-revocation was designed to produce effectual activities of a group that had to endure attacks of collusion when increasing computational costs considerably. The outcome demonstrated an effective achievement towards secure auditing [7].

The combined AES and blowfish algorithm is proposed to secure the cloud with short message service that provides confidentiality, verification and authentication for data. The proposed scheme provided the security for cloud data without a cloud service provider. The main drawback is that the proposed scheme is applicable only for text data [17]. A third-party auditor is employed for enhancing the security of the cloud through implementation of the AES algorithm. The auditor controls the data access of the user whereas the AES encryption technique protects the data during transfer. The AES algorithm in the proposed model ensures the availability of cloud during the storage of huge data in it [18].

From the literature study, it was observed that the issue of fine-grainedness, security and data confidentiality for sharing the cloud data still remained unresolved in multiuser clouds. Another issue is proper method to consider direct attribute / user revocation in data sharing for resource limited users in cloud computing. The frameworks with AES provided a more secure cloud environment than other cryptographic techniques.

III. Preliminaries

A. Bilinear Mapping

Bilinear Mapping is the most common technique employed in generation of security keys and digital signature in the cloud for securing it against any attacks or data infringement [19]. Consider the additive group G_k and a multiplicative cyclic group of Prime Orders, G_p, then the bilinear map that exists between G_k and G_l is given as,

1) Bilinear – c,d $\in Z_q^*$ and a,b $\in G_k$, e (ca,db) = e(a,b)cd for all

2) Non-degenerate-the existence is possible at only one point $(G_k, G_l) \neq 1$

3) Computable- to estimate e (c,d) for any c,d$\in G_k$

B. Digital Signature Generation

For generating the digital signature, the computational Diffie-Hellman technique is employed. Among the many variants, the Inverse Decisional Diffie-Hellman (IDDH) is implemented to generate the digital signature. From the large cyclic group G with the group P (prime order), the following two distribution are involved in signature generation.

1) IDDH triple- $g, g^s, g^{s^{-1}}$, where $s \in Z_q^*$.

2) Random triple- g, g^s, g^t, where s, t $\in Z_q^*$ (s and t are selected randomly form the uniform random).

C. Advanced Encryption Standard

AES does all its computations on bytes rather than bits. It is generally employed with three different key sizes that includes 128 bits, 192 bits and 256 bits with total rounds of 10, 12 and 14 rounds respectively. For encryption it uses byte substitution, shift rows, mix columns and add round key respectively. For decryption it the reverse of the encryption process is performed. The plain text is converted into the cipher-text through the number of round Nr specified for different bit keys. The steps of AES cryptography as in Fig. 1.

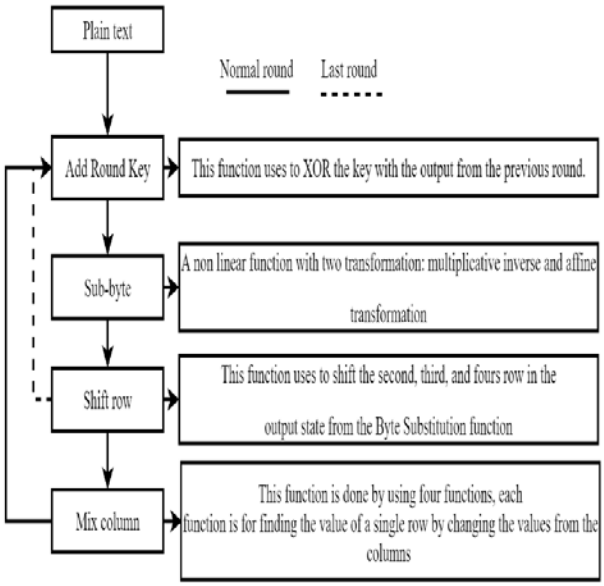

Fig. 1. Steps in AES Cryptology.

IV. Proposed EDES-ACM Cloud Architecture

The framework to secure the data in the cloud environment with the Enigma Diagonal Encryption Standard as given in Fig. 2. The proposed approach is established to ensure the security of the cloud through the effective access control mechanism. The control mechanism is established with effective group and data management in the proposed framework. The group management is established with the robust group signature with revocation scheme. The data security is achieved through the EDES algorithm in which the data is encrypted with the symmetrical key before storage into cloud. All the digital group signatures and EDES keys are stored in the key manager and is used to validate the user during the access into the cloud and data.

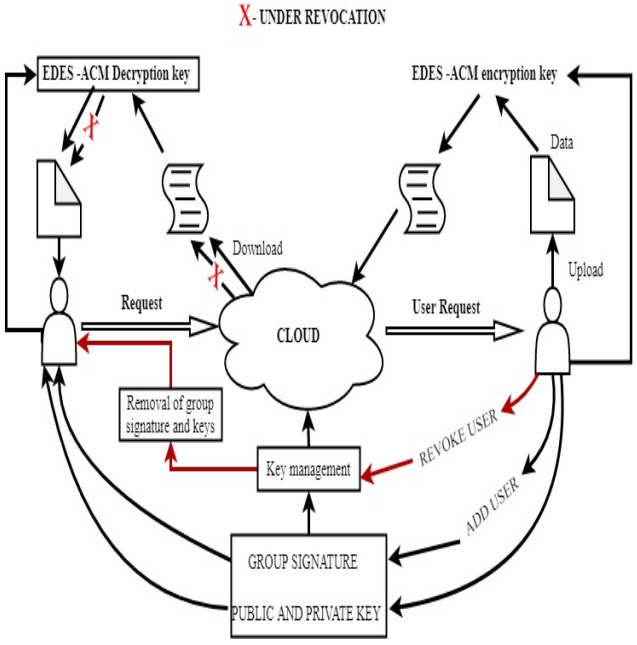

Fig. 2. Proposed EDES-ACM Framework.

Let us consider the user A and B with two different roles process the request to join the cloud environment in the organization. The cloud authority processes the user request and forward it to the data owners for approval. The data owner will generate the two distinct digital group signature and send them to the users through the cloud. Similarly, the generated group signature is stored in the cloud key management. The group owner uploads the data into the cloud and before storing it in the cloud the process of encryption is carried out on the data through the proposed EDES-algorithm. The EDES algorithm is the enhanced version of AES algorithm based symmetric key with 512-byte size that has a total of 10 rounds. After the termination of AES algorithm. The obtained key matrix is subjected to the enigmatic diagonal formulation in which the key is generated with diagonal elements predominantly either in direct order (first to last element) or in reverse order randomly. The final key obtained is shared with the users in the cloud. The users can access the cloud any time, at any place through their distinct digital group signature and private key to access the data.

V. Security Model in Proposed EDES-ACM

The main goal of the proposed EDES-ACM framework is to secure the data in the cloud environment in an effective way. Let us again consider the two users A and B who are added to the cloud with different roles. The user's activity is continuously monitored in the cloud environment with the group manager. The group manager reports the activity of the user to the data owner over each session. When user A has involved in any unauthorized activity like tampering the data or any perform any activity that are not defined in the role, the group manager tracks it and reports the owner. The data owner revokes the digital group signature for the user A and the key data management is updated. If user A tries to access the cloud again, the signature is invalid and hence the data is secured in the cloud with improved confidentiality.

In other case, when there is an attack from the user end like DDoS attack, the data in the cloud is under severe threat. In the proposed model, the data is effectively encrypted with the EDES algorithm. Even if the attacker gets the data from the cloud, the decryption is not possible without the EDES key. This results in invalidation of the attacker and the signature through which the access performed is revoked from the key management. It ensures the security of the data over its integrity and privacy preservation.

VI. System Algorithm

The system algorithm to secure the data in the cloud environment:

- **Setup (1^{λ}, N)**: The cloud environment is set up is established with the security parameter λ and the maximum receiver capacity of size N. Using the security parameter, the public and the master key are generated in the cloud and are designated as PU and MA respectively.
- **AccUser (IU, IG)**: Every user in the cloud initially process the request for adding them in the cloud. The group manager GM obtains the identity of the user IU

and list it in the group with identity IG based on the role list and its parameter (RL and RLP).

- **GSgen (IU, MA):** Based on the user identity IU, the cloud authority employs the master key MA to generate the digital group signature (DGS) with the validating message V.
- **RM (MA, RUH, S):** Every user in the cloud is provided with some role which follows some hierarchy RUH in the role set S for securing the secrecy of the group through Public parameters set PS.
- **ReUser (IU, IG, DGS):** When the user is tracked for any unauthorized activities, the user identity IU is obtained along with the group identity and digital signature. The RL and RLP of the user are retrieved and digital signature is removed from the key management and it is updated.
- **KeyGen (MA, IU, AP, MK):** The access policy AP of every user is defined in the cloud and it is used along with the MA and IU. The Key matrix MK is obtained through the EDES algorithm with a random diagonal prioritization technique. The final private key PR is provided to the user. Let the final matrix after 10 rounds of AES is given in Fig. 3.

	0		1		2		3
A		B		C		D	
	4		5		6		7
E		F		G		H	
	8		9		10		11
I		J		K		L	
	12		13		14		15
M		N		O		P	

Fig. 3. Enigmatic Diagonal Technique.

The forward or reverse order is selected randomly and its sample keys are given in Table I.

TABLE I. ORDER OF TWISTING

Forward Order	0,5,10,15,1,2,3,4,6,7,8,9, 11,12,13,14	AFKPBCDEGHIJL MNO
Reverse order	15,10,5,0,14,13,12,11,9,8, 7,6,4,3,2,1	PKFAONMLJIHGE DCB

- **EC (M, SU, AP):** The data owner employs the EDES algorithm along with the Access policy AP and the user group set SU to encrypt the data with message M to get EnD.
- **DC (IU, PR, EnD):** Once the user downloads the data with the IU, the PR is provided to decrypt the encrypted data EnD to get the message M.

Algorithm 1: Digital Group Signature and user control

Input: λ,N,IU, IG,
Output: Digital group signature (DGS)
1: Execute the set-up algorithm with λ and N
2: Generate the master key MA, PU
3: When the user processes the request
4: Get S from Z_q^*
5: generate the DGS
6: Distribute the DGS to the user
7: Add the user with IU based on IG
8: Track the activities of user
9: When the user performs unauthorized activity
10: revoke the user DGS
11: user signature is invalid
12: end

Algorithm 2: Key generation and Cryptic mechanism

Input: MA, IU, AP, M, SU, 4x4 matrix, sbox-4x4 matrix,KM, constant matrix – CM, rejandael scheduler RS,
Output : private key. EnD, DnD
1: get A
2: $A \leftarrow Sub\_Bytes(KM, S_{Box})$
3: $A(i,j) \leftarrow S_{Box}(p,q)$
4: $A \leftarrow Shiftrows(A)$
5:if i=1 or j=1or i=j
6: A (i,j) ← A (i,j)
7: else If i<j
8: A (i,j) ←A (i+1,j-1)
9: else if i > j
10: A(i,j) ←A(i-1,j+1)
11: $A \leftarrow Mix\_Column(A, CM)$
12: for i → 1 to 4
13: $A(:,i) \leftarrow CM$ x $A(:,i)$
14: $A \leftarrow Add\_Round\_Key(A, KM)$
15: $A(:,i) \leftarrow A(:,i) \oplus KM(:,i)$
16: Random (forward, backward)
17: Get the private key PR
18: Using PR encrypt the data (EnD) and upload to the cloud
19: Download the data and decrypt it (DnD)
20: end

VII. RESULTS 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 on 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 a memory of 16 GB at 2.45 GHz with a disk of 1TB capacity.

A. Digital Group Signature

Whenever the user processes the request to join the group in the cloud, they are provided with the digital group signature is provided to thee. In the proposed model, the Inverse Decisional Diffie Hellman (IDDH) technique is employed to generate the signature that is provided to the user and stored along with the user identity in the cloud key management. The verification is carried out when the user attempts to access the cloud.so in general there are two parametric that are involved in analyzing the group signature generation i.e. generation time and proofing time as in Fig. 4.

B. Uploading and Encryption

Every data owner in the cloud upload the data into the after encrypting it with the proposed EDES algorithm. Bothe the uploading time and the encryption time increases with the increase in the file size. The time taken for uploading is less compared to that of the encryption time. Hence the cost involved in encrypting the file is given as the **(RL+1) M**. the time taken for uploading and encryption of data through the EDES algorithm is given in Table II and the corresponding plots are given in Fig. 5 and 6.

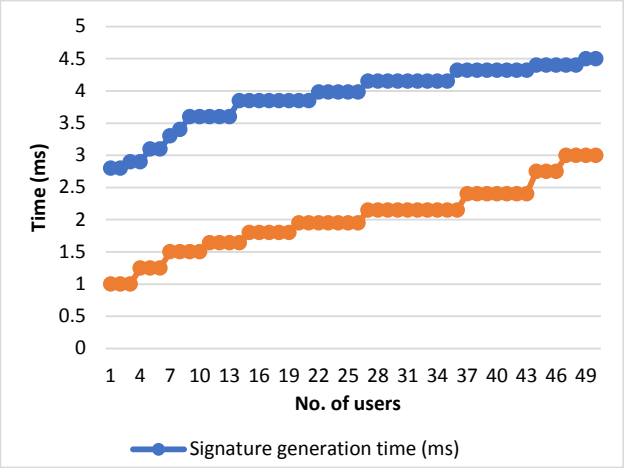

Fig. 4. Generation Time and Proofing Rime of the IDDH.

TABLE II. UPLOADING AND ENCRYPTION TIME FOR DIFFERENT FILES

File size (kb)	Upload time (ms)	Encryption time (ms)
10	1	75
20	1.2	80
30	1.3	87
40	1.6	100
50	1.6	115
60	1.95	135
70	2.5	160
80	2.5	190
90	2.5	190
100	3.1	235
500	3.15	280
1024	3.5	335
2048	3.5	380

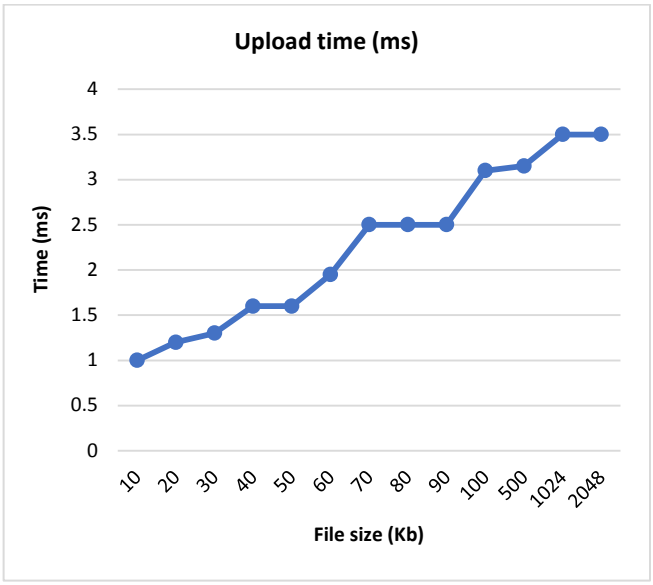

Fig. 5. Uploading of Data through the EDES Algorithm.

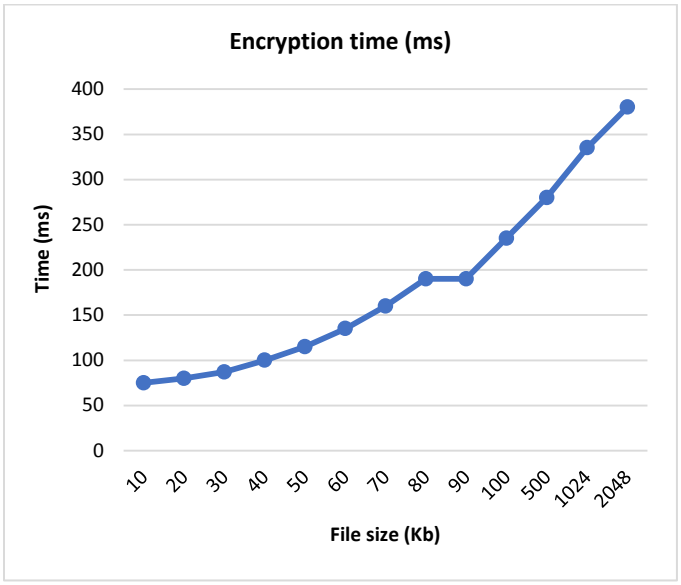

Fig. 6. Encryption of Data through the EDES Algorithm.

C. Decryption and Download Time

The encrypted data in the cloud is downloaded to the user based on their request. The user employs the decryption key to access the information from the downloaded data. But unlike uploading the downloading time of encrypted data take more time than that involved in decrypting it. The cost involved in decrypting the file 2k(P+E) +3M where P and E are the pairing and exponential operators and M is the multiplicative operator. The value of K defines the complexity of the access mechanism to access the data in the cloud. The time taken for downloading and decrypting the file is given in Table III and its corresponding plot are given in Fig. 7 and 8.

The comparison between the existing and the proposed model is given in Table IV.

TABLE III. DOWNLOADING AND DECRYPTION TIME FOR DIFFERENT FILES

File size (kb)	Decryption time(ms)	Download time (ms)
10	620	950
20	620	950
30	635	950
40	635	985
50	635	985
60	665	985
70	680	1020
80	680	1020
90	705	1065
100	705	1065
500	750	1108
1024	750	1108
2048	800	1139

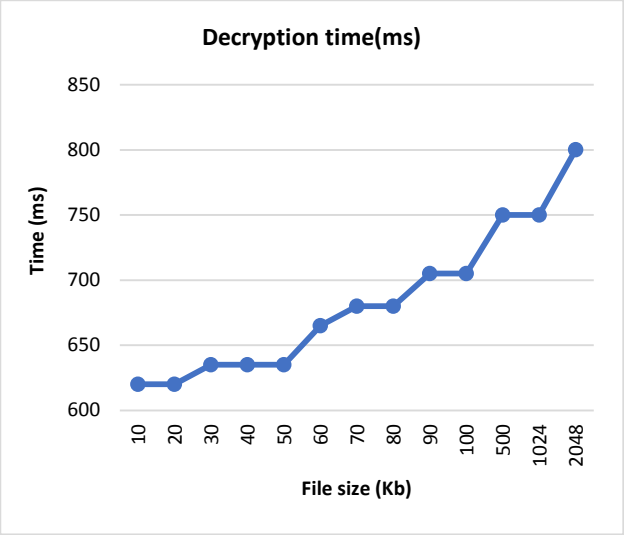

Fig. 7. Time for Decrypting the File.

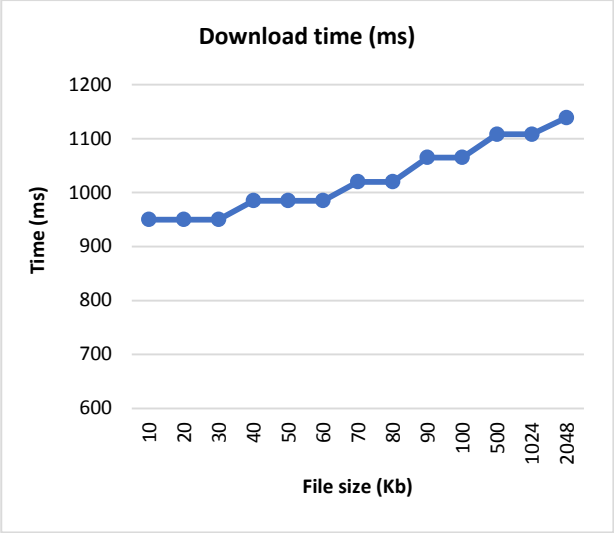

Fig. 8. Time for Downloading the File.

TABLE IV. COMPARISON ON COST AND PARAMETER SIZE

Parameter/ frameworks	HW [20]	ADBS [21]	Proposed EDES-ACM
Encryption cost	(l_a+ 1) M	(l_a+ 2) M	(RL+1) M
Decryption cost	3kP + 2kE + 3kM	3kP + 2kE + 3kM	2k(P + E) +3M
Parameter size	(3k+1)$l_G + l_{G_T}$	(3k+2)l_G + l_{G_T}	(3k+3)l_G + l_{G_T}

Where l_a is the attribute list, LR is the role list, k is the access structure complexity, l_G *and* l_{G_T} represent the size of element G and G_T. M, P and E are the multiplication, exponential, and pairing operators.

The proposed EDES-ACM framework is effective with reduced cost for both encrypting and decrypting the files than the existing models of HW [20] and ADBS [21]. The size of parameters involved in the study is larger in the proposed EDES-ACM framework than in the existing models. This showed that the proposed framework is effective with reduced computational cost with large parameter size.

VIII. CONCLUSION

The novel framework of EDES-ACM is proposed to secure the cloud environment and its data. The proposed scheme employed the improved version of the AES algorithm to ensure the security of the data. Similarly, the group signature is generated through the IDDH technique and is provided to the user. The key matrix obtained at the end of the AES round is subjected to the enigmatic diagonal technique with either forward or backward approach that are selected randomly for multiusers. Initially, the cloud is organized by the cloud authority with the public key and the master key which are placed in the cloud key management along with the private keys and signatures. The data owner encrypts the data with the EDES encryption key. The data user decrypts with the private key after the validation. The group manager monitors the activity of the user and generates the report on user activities to the data owner. The data owner can revoke the user under any suspicious activity in the cloud environment. The proposed EDES-ACM framework is evaluated on the security metrics that involves the time and cost-based analysis. The results from the analysis showed that the time of signature generation and proofing increase with users and the time for cryptic mechanism increases with file size. The computation cost and parametric size is found to be effective compared with the existing models.

In future the proposed framework can be enhanced with dual encryption techniques with blockchain technology to ensure the security and accumulation of data in effective manner. Aside parallel computation can be performed over the segmented data to reduce the time and cost involved proposed framework. The signature in the proposed framework can involve some secondary operation to make it further more robust.

REFERENCES

[1] Shen, Yaosheng, Ding Wang, and Ping Wang. "Revisiting Anonymous Two-Factor Authentication Schemes for Cloud Computing." In

International Conference on Cloud Computing and Security, Springer, Cham, 2018 pp. 134-146.

[2] Kalaiprasath, R., R. Elankavi, and Dr R. Udayakumar. "Cloud. security and compliance-A semantic approach in end to end security." International Journal Of Mechanical Engineering And Technology (Ijmet) 8, no. 5 2017: 987-994.

[3] Hoeppner, Joseph A. "A Comparison of Cloud Computing Database Security Algorithms." (2015).

[4] Sandhu, Rajinder, and Inderver Chana. "Cloud Computing Standardization Initiatives: State of Play." International Journal of Cloud Computing and Services Science (IJ-CLOSER) 2, no. 5,2013: 351.

[5] Wegberg, Gregor, Hubert Ritzdorf, and Srdjan Capkun. Multi-User Secure Deletion on Agnostic Cloud Storage. ETH Zurich, 2017.

[6] Yu, Yong, Man Ho Au, Giuseppe Ateniese, Xinyi Huang, Willy Susilo, Yuanshun Dai, and Geyong Min. "Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage." IEEE Transactions on Information Forensics and Security 12, no. 4 2016: 767-778.

[7] Tian, Hui, Fulin Nan, Chin-Chen Chang, Yongfeng Huang, Jing Lu, and Yongqian Du. "Privacy-preserving public auditing for secure data storage in fog-to-cloud computing." Journal of Network and Computer Applications 127,2019: 59-69.

[8] Wang, Zhiwei. "Provably secure key-aggregate cryptosystems with auxiliary inputs for data sharing on the cloud." Future Generation Computer Systems 93, 2019: 770-776.

[9] Mao, Xianping, Xuefeng Li, Xiaochuan Wu, Chuansheng Wang, and Junzuo Lai. "Anonymous attribute-based conditional proxy re-encryption." In International Conference on Network and System Security, Springer, Cham, 2018, pp. 95-110.

[10] Kanthale, Akash, and S. P. Potdar. "Survey on Cloud Computing Security Algorithms." vol 5: 2015-2017.

[11] Zeghid, Medien, Mohsen Machhout, Lazhar Khriji, Adel Baganne, and Rached Tourki. "A modified AES based algorithm for image encryption." International Journal of Computer Science and Engineering 1, no. 1 2007: 70-75.

[12] Shaji, Neenu, and P. L. Bonifus. "Design of AES architecture with area and speed tradeoff." Procedia Technology 24 2016: 1135-1140.

[13] Rao, B. Nageswara, D. Tejaswi, K. Amrutha Varshini, K. Phani Shankar, and B. Prasanth. "Design of modified AES algorithm for data security." International Journal For Technological Research In Engineering 4, no. 8, 2017: 1289-1292.

[14] Crampton, Jason, Naomi Farley, Gregory Gutin, Mark Jones, and Bertram Poettering. "Cryptographic enforcement of information flow policies without public information via tree partitions 1." Journal of Computer Security 25, no. 6, 2017: 511-535.

[15] Fu, Xingbing, Xuyun Nie, Ting Wu, and Fagen Li. "Large universe attribute based access control with efficient decryption in cloud storage system." Journal of Systems and Software 135, 2018: 157-164.

[16] Li, Qi, Jianfeng Ma, Rui Li, Ximeng Liu, Jinbo Xiong, and Danwei Chen. "Secure, efficient and revocable multi-authority access control system in cloud storage." Computers & Security 59, 2016: 45-59.

[17] Akhil, K. M., M. Praveen Kumar, and B. R. Pushpa. "Enhanced cloud data security using AES algorithm." In 2017 International Conference on Intelligent Computing and Control (I2C2), IEEE, 2017.pp. 1-5.

[18] PIUS, U.T., ONYEBUCHI, E.C., CHINASA, O.P., and ADOBA, E.F. “A Cloud-Based Data Security System Using Advanced Encryption (AES) and Blowfish Algorithms” Journal of Scientific and Engineering Research, 5 (6) 2018, (pp. 59-66).

[19] Huang, Qinlong, Yixian Yang, and Jingyi Fu. "Secure data group sharing and dissemination with attribute and time conditions in public cloud." IEEE Transactions on Services Computing (2018).

[20] Hohenberger, Susan, and Brent Waters. "Online/offline attribute-based encryption." In International workshop on public key cryptography, Springer, Berlin, Heidelberg, 2014.pp. 293-310.

[21] Li, Jin, Yinghui Zhang, Xiaofeng Chen, and Yang Xiang. "Secure attribute-based data sharing for resource-limited users in cloud computing." Computers & Security 72 2018: 1-12.