Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 32 No. 3 (2025)

A Study on Enhanced Elgamal Cryptosystem for Sharing Secret of Multi-User's

[1]Shivani Namala, [2]Dr. Rakesh Kumar Yadav

[1]Research Scholar, Department of Computer Science and Engineering, Maharishi School of Engineering and Technology, MUIT, Lucknow

shivaninamala1@gmail.com

[2]Associate Professor, Department of Computer Science and Engineering, Maharishi School of Engineering and Technology, MUIT, Lucknow

Article History:

Received: 12-01-2025

Revised: 15-02-2025

Accepted: 01-03-2025

Abstract:

Cloud computing is a predominant technology for education, health care, large-scale and small-scale industries, and all application sectors. However, securing data in the cloud from security breaches remains a challenge for Cloud Service Providers. Many academics believe that public key cryptosystems are commonly employed to secure the secrecy, authenticity, and non-repudiation of data belonging to a single owner. Data will be generated and stored in cloud by one user and shared among multiple users with the same privileges (i.e.) multi-user. Protecting the multi-user data against unauthorized access and providing key management solutions is still a challenging issue in the cloud. For securing the multi-user data, cryptographic techniques can be incorporated. The main aim of this study is to provide data confidentiality in Improved Secure Cloud Data Storage Framework for multi-user data incloud. In this paper Enhanced ElGamal cryptosystem is proposed to secure multi-user data storage &retrieval with key management in a secure cloud framework. The example of the proposed cryptosystems, the performance of the cryptosystems is explained in this research.

Keywords: Novel DNA cryptosystem, secure multi-user cloud data, enhanced elgamal, sharing Secret of multi-user's Cryptosystem

INTRODUCTION

Cloud has become a prominent technology for sharing data among users for business operations. Based on the business process, a group of users dynamically share the data as multi-user and work together for a while. It raises the organization's ultimate goal of protecting shared data from security breaches in order to achieve successful expansion. The objective of achieving data secrecy for multi-user data in the cloud remains, but there are several hurdles to overcome (Vinay Kumar Pant & Ashutosh Kumar 2016).

Cloud computing is dominated by three entities: Cloud Server (CS), Data Owner (DO), and Data User (DU). Storage services are provided by CS to application owners and dispersed users. DO is capable of creating, storing, and updating any type of data on cloud server. Through proper authentication, DU can access &change data stored in the cloud. If unauthorized users gain access to critical or secret data, DO and DU will be in big trouble. Data confidentiality is a critical component for data owners and users to safely store &retrieve shared cloud data. The lifetime of the group is considered less since the group has been created for a specific purpose.

For providing data confidentiality of shared data among the users, either symmetric cryptosystem or asymmetric cryptosystem can be utilized. a symmetric cryptosystem, DO and DU must share secret

key that is used forsboth encryption & decryption. DO & DU must produce public and private keys separately in asymmetric cryptosystems. Then, the DO and DU public keys must be exchanged across the group of users in order to accomplish encryption, and data will be decrypted using private key. The number of encryption &decryption keys differs between the two cryptosystems. Cloud service companies such Amazon, Microsoft, Google, &others employ symmetric cryptosystems to execute data encryption and asymmetric cryptosystems to handle key sharing among cloud users for rapid computation and safe data transport.

T. ElGamal developed a public key cryptosystem in 1985, which has recently attracted a lot of attention. The use of discrete logarithm problem is critical to cryptosystem. It is tough to solve a discrete logarithmic problem.

LITERATURE REVIEW

Inside keyword guessing attacks in cloud storage are identified by Rongmao Chen et al. (2016). To improve searchable encryption for safe cloud storage, the study offers dual server public key encryption with keyword search. Furthermore, homomorphic linear hash algorithms are suggested to validate the communication and cloud storage. When compared to existing systems, the suggested encryption scheme takes less time and has lower calculation costs.

Joseph K Liu et al. (2016) improve the cloud storage system's security by introducing a two-factor data security mechanism. Users can store and share the data with another user with a public key cryptosystem and security device. The sender encrypts data with the receiver's public key & stores it in the cloud. Cloud performs security operations based on security device data of receiver. The receiver using the private key and security device can decrypt received data from cloud. The data cannot be decrypted without any one factor at the receiver side. Besides, the sender need not worry about the receiver's security device information for encrypting and storing in the cloud. The security device can be changed at any particular time with the cloud server. However, the ciphertext again needs tobe processed in the cloud server according to the receiver's new security device.

Zheng Yan etal. (2016) proposed a scheme to address data confidentiality issues & duplicated data storage in the cloud. Attribute based encryption is used with a secure access control mechanism in the proposed scheme for securely accessing encrypted data. The encrypted data deduplicated for managing the storage space in the cloud server. AES cryptographic algorithmis used to encrypt data in the cloud. The data ownership verification, the effectiveness of the system performance, flexible solution for access control, and data deduplication are the proposed scheme concerns.

Hui Tianetal. (2017) suggested a public auditing approach based on dynamic hash tables for safe cloud storage. TPA keeps a dynamic hash table to deal with data block challenges from the data owner. TPA performs auditing via a homomorphic verifiable authenticator technique. The scheme also supports data dynamic operations. The research guides to design effective scheme all types of cloud data.

Yuan Zhang etal. (2017) introduced a public auditing scheme based on indistinguishability obfuscation. The scheme reduces computation overhead for TPA to perform auditing with cloud storage server. Data dynamics is performed with the proposed scheme. The research suggests focussing on resisting malicious TPA and reducing overhead at the cloud server.

Jian Shenetal. (2017) proposed a public auditing scheme with dynamic structures such as location array & doubly linked list info table. The auditing scheme is designed with a homomorphic verifiable authenticator. The scheme also supports data dynamics. The dynamic structures used in the scheme enhance the performance of the auditing process. The research guides to focus on efficient dynamic structures for reducing storage, communication, and computation costs.

Xingyuan Wangetal. (2018) suggested a DNA &CML-based picture encryption technique. Plaintext pictures were transformed to DNA matrices using DNA encoding principles. The cyclic shift operations are carried out on the DNA matrix's even rows and columns. The index-scrambling procedures were then conducted on the scrambled DNA matrix's odd rows. DNA sequence and calculation rules further disperse the matrix. Finally,the diffused matrix is decoded in order to produce an encrypted image.

Xuncai Zhang etal. (2018) recommended the image encryption method based on DNA encoding &Feistel network in permutation diffusion –scrambling structure. The proposed method resists statistical, differential, and plaintext attacks. The experimental results show that method is competent.

Manreet Sohal&Sandeep Sharma (2018) proposed a DNA-based symmetric key cryptography approach for cloud data security. Dynamic encoding tables are used to improve the cryptosystem's security. The suggested cryptosystem was compared to the cryptosystems DES, AES, and Blowfish.

Su Peng etal. (2019) proposed a multi-replica provable data possession scheme to avoid the problem of handling public keys by TPA. The scheme utilizes a compressed authentication array and homomorphic verification tag to perform multi-replica auditing and dynamic updates. The research suggests improving the performance of the scheme by reducing the computation &communication overheads for cloud users, cloud servers, and TPA.

Yannan Li et al. (2019) addressed the key research challenge of public auditing schemes: key management. A fuzzy identity-based auditing protocol is proposed to simplify the key management issue. The private key is generated based on the fuzzy identity (i.e.) biometrics of the cloud user. A fuzzy identitybased signature is used to perform integrity verification. The research directs to implement the proposed scheme in real-time cloud applications.

Aiping Li et al. (2019) suggested a cloud computing-based verifiable data integrityverification technique based on data fragment structure &index hash table. The scheme generates a constant amount of metadata and reduces computation time for cloud users. The scheme supports public verifiability and data dynamics. The research suggests focussing on efficient public auditing schemes by reducing computation and communication costs for cloud users, TPA, and cloud servers.

Hossein Nematzadeh et al. (2020) suggested a novel symmetric encryption technique based on a Binary Search Tree (BST) and DNA sequence. The suggested encryption technique has been subjected to entropy analysis, statistical attack, brute force assault, and differential attack analysis. The study intends to improve the cryptosystem using appropriate data formats.

Jianan Hong et al. (2020) presented a system for ensuring the secrecy of cloud-outsourced data by combining Ciphertext-policy Attribute-based encryption with timed-release encryption. The suggested method is intended to provide fine-grained access control and timely data posting. The suggested scheme's security &performance analysis is efficient and meets the security standards.

Feng Wangetal. (2020) suggested a public/private auditing approach for cloud storage based on asymmetric bilinear pairing. The proposed approach is based on lightweight certificate-based auditing mechanism that has been demonstrated to be secure against the random oracle model. The suggested scheme's efficiency is demonstrated by the security proof and implementation assessment. The research directs to focus on auditing various block sizes with the random number of blocks and designing efficient private/public auditing schemes.

A multi-copy data integrity verification approach for multi-agent cloud storage was presented by Chunbo Wang and Xiaoqiang Di (2020). For key generation, the approach employs the bilinear

mapping method, a multi-branch authentication tree for multi-copy data signature, and a directed acyclic graph for task connection among several agents. According to the trial data, average auditing efficiency is increased by 20%.

Viswanath and Krishna etal. (2021) used a hybrid (AES) encryption technology using s-box &Feistal network to improve security in a multi Cloud scenario. The hybrid encryption approach framework splits the data, indexes it, and encrypts it. The hybrid encryption architecture outperforms the AES &Triple DES techniques. The hybrid encryption framework approach is resistant to DoS attacks, tampering attacks, and insider attacks. The hybrid encryption system encrypts both properties and data, but it takes longer to compute.

Denis and Madhubala et al. (2021) used Discrete Wavelet Transform steganography using a hybrid encryption approach. For secure diagnosis of data contained with (RGB) channel in medical cover picture, hybrid encryption techniques such as AES and (RSA) are used. Nonetheless, the (AGA-OPAP) requires enhancements to its data concealing capabilities for imperceptibility aspects.

For secure Cloud storage, Ming et al. (2021) used revocable multi-authority attribute-based encryption (RMA-ABE). The RMA-ABE approach outperformed the Diffie-Hellman issue and could survive adaptive selected plaintext attacks. The (LSSS) approach was used to increase the expressiveness of access policies, but it was computationally costly.

Rafiqueetal. (2021) used Crypt-DICE to improve the security of cloud data. CryptDICE supported several data encryption mechanisms, and annotation was employed to meet access search requirements. The Crypt-DICE offers suitable trade-offs &encryption decision execution at various levels of data granularity.

Jayapandianetal. (2021) used the Tabu search idea for encryption, &the Tabu search approach assures that average encode and decode time in multi-media data is reduced. Although Crypt-DICE &Tabu search algorithms were effective in scheduling encryption, they required a local memory table to hold the data.

Ramachandra etal., (2022) investigate large data cloud application security &monitoring in order to host extremely sensitive data for Cloud platforms. To address this issue, the (TDES) technique is suggested to offer security for massive data on the Cloud. The suggested TDES approach provides considerably easier way for protecting against assaults and defending data privacy by increasing length of keys in (DES). The experimental findings demonstrated that the suggested TDES approach is successful in providing security &privacy to large amounts of healthcare data on the Cloud. When compared to the existing (IFHDS) technique, the suggested TDES methodology required less encryption and decryption time.

Cuzzocrea etal.(2022) used an attribution based method to improvedata security in Cloud. The presented solution used an appropriate encryption mechanism for the dominating relationship. However, while processing bigger databases, the SB-DS approach &the standard attribution-based technique increase calculation time.

Rashmi et al. (2022) used the (ICE) approach to boost randomness based security, although it was a difficult procedure in big scale databases. To boost security, the Chaos encryption method is used with the Lorentz 96 methodology.

A, Reyana etal., (2023) provides a unique approach to protect integrity of data & improve access control. To accomplish a unique improved storage retrieval technique is developed to increase performance of cloud's storage and retrieval procedures. The upload, download, encryption, and decryption times are all considered while evaluating the approach. The time it takes to upload afile

rises in proportion to its size. Similarly, the time required to encrypt data of various sizes & formats demonstrated that it is dependent on file size and format. As a result, the encryption time grows as file size increases, illustrating suggested system's performance.

OBJECTIVE OF THE STUDY

- To provide data confidentiality in Improved Secure Cloud Data Storage Framework for multi-user data incloud.

ENHANCED ELGAMAL CRYPTOSYSTEM

The following is ElGamal's algorithm (Elgamal 1985).

User A - Receiver:

Key Generation:

Choose q, a largeprime number, & α, primitive root of q

Choose X, a randominteger suchthat $1 < X < q-1$

Compute Y as $\alpha^X \bmod q$

Private Key: X, Public Key: {q, α, Y}

User B - Sender:

Encryption:

Represent messageas integer m, such that $0 \leq m \leq q-1$

Choose a random integer k, such that $1 \leq k \leq q-1$

Compute one-time key, $K = Y^k \bmod q$

Encrypt message 'm' as a pair of integers (C_1, C_2) where

$C_1 = \alpha^k \bmod q$, $C_2 = K.\ m \bmod q$

User A - Receiver:

Decryption:

Recover key by computing $K = C_1^X \bmod q$

The message, m canbe retrieved as

$m = C_2 . K^{-1} \bmod q$

If the private key X is generated in the ElGamal cryptosystem, entire system can be readily cracked because the message can be obtained as m =C2C1-X mod q. The complexity of discrete logarithm issue contributes to the ElGamal cryptosystem's security. To solve the discrete logarithm issue, several algorithms have been developed, including naïve, Pollard's rho technique, &baby-step/giant-step methods.

Data will be shared in real time b/w user's web browser and a cloud service providersuch as Google, Amazon, or others. To encrypt data, a symmetric key cryptosystem is utilised, & a public key cryptosystem is used to manage keys needed to authenticate DO and DU. This approach is adapted in the proposed Improved Secure Cloud Data Storage Framework, which employs unique cryptosystems. To maximize data security, unique cryptosystems must be presented.

The Enhanced ElGamal Cryptosystem was designed and applied in this research paper to overcome key management concerns in multi-user data sharing. The enhanced ElGamal cryptosystem must

guarantee data security by enhancing the complexity of the intruder's derivation of the DU's private key.

Security is important aspect of cloud computing. To assure data security when exchanging data among multiple users and to increase cloud security, the Enhanced ElGamal cryptosystem was designed as an asymmetric cryptosystem for key management among multiple users.

PROPOSED SYSTEM ARCHITECTURE

Significant stakeholders who deal with multi-user data in acloud environment, such as Data Owner, who distributes data to a group of users known as Data Users, are included in the proposed system design. Initially, the Data Owner dynamically creates a group and shares a secret token k3 generated among the group members (Data Users) for further communication. Data Owner generates an intron sequence and shares it with Data Users, using the enhanced ElGamal Cryptosystem.

The Data User thenrequests hint or key file from Data Owner. The Data Owner encrypts the key file using Enhanced ElGamal cryptosystem using the Data User's public keys and secret token k3 shared. The DataOwner then sends encrypted key file to Data User, who uses Data User's private keys to decode it. The Enhanced ElGamal cryptosystem's (EEC) security is based on randomization and discrete logarithm problem. The increase in unpredictability improves the cryptosystem's security. It also employs private and public keys to verify identity of the Data Owner and Data User. Using his/her private key, only designated Data User may decode the key file. Thus, in a cloud context, the confidentiality of multi-user data is maintainedamong stakeholders.

SHARING SECRET OF MULTI-USER'S

The Enhanced ElGamal Cryptosystem (EEC) is used by cloud users to compute the system's public and private keys. The DataOwner creates group and gives the Data User the secret token k3. After that, the Data Owner selects the public key & key file that will be transmitted to Data User. The Data Owner invokes the encryption function to encrypt the key file with computed keys. The ciphertext will be sent to Data User through any network. The Data User will use the key file and the secret token k3 to decrypt the ciphertext. EEC is also employed in the distribution of intron sequences among Data Users. The proposed EEC algorithm is provided as pseudo-code below.

Data User:

KeyGeneration:

Select q, a huge prime integer, &, q's primitive roots.

Determine d = (,)-1 mod q.

Select X as a random number such that 1 X q-1

Calculate Y as Y = (,)X mod q

Private Key: X,, d; Public Key: q,, Y

Choose the shared secret token k3, 1 k3 q-1

Share k3 with the Data User in secret.

Data Controller:

Encryption: Represent the message as an integer msuch that 0 m q-1.

Select two random numbers k1,k2, suchthat 1 K1, k2 q-1Compute one-time-key $K = (k_1)^{k2} .Y^{k3} \mod q$

Compute $C_1 = \alpha^{k3} \bmod q$, $C_2 = k_1^{k2} \bmod q$, $C_3 = K.m.Y \bmod q$

Ciphertext $C = (C_1, C_2, C_3)$ send it to Data User.

Data User:

Decryption:

Recover one-time-key bycomputing $K = C_1^X$, $C_2\ \beta^{k3X} \bmod q$

Find K^{-1} and retrieve message $m = K^{-1} C_3\ d^X \bmod q$

The Enhanced ElGamal cryptosystem (EEC) operates asfollows: The keygeneration process involves selecting a large prime number, q, determining its primitive roots, & executing modular inverse for many values of the primitive root, which is denoted as 'd'. It also requires selecting a random integer, 1 X q-1, for constructing a private key X and determining public key from random number Y. The encryption method consists of selecting two random numbers as k1 and k2, as well as a shared secret token as k3. To encrypt the key file, use these two random numbers plus a secret key to generate the one-time secret key K. The encryption key for key file is C= (C1, C2, C3). The decryption process starts with obtaining one-time secret key K. To decrypt ciphertext, the value of K & the private key X,d must be determined.

The ElGamal cryptosystem's security is predicated on discovering the value of private key 'X' by solving discretelogarithm problems. The researchers revealed how to solve discrete logarithm problem utilising the naive, Pollard's rho, & baby-step/giant-step techniques. The enlarged ElGamal cryptosystem utilises two primitive roots, two random numbers, two private keys, and three ciphertext parameters in contrast to the ElGamal cryptosystem. Four factors ensure security of the improved ElGamal cryptosystem: one-time secret key 'K,' the private key 'X,' the modular inverse of the product of the primitive roots 'd,' and the shared secret token 'k3'.

For adversary, the computation cost has been increased in enhanced ElGamal cryptosystem compared to ElGamal cryptosystem. The suggested method may be mathematically proven as follows: The decryption equation m= K-1.C3.dX mod q is used, & proof consists of recovering original messagefrom it.

$m = K^{-1}.C_3.d^X \bmod q$ (substitute K)

$= C_1^{-X}.C_2^{-1}.\ \beta^{-k3X}.\ C_3.d^X \bmod q$ (substitute C1, C2)

$= \alpha^{-k3X}.k_1^{-k2}.\ \beta^{-k3X}.\ C_3.d^X \bmod q$ (substitute C3)

$= \alpha^{-k3X}.k_1^{-k2}.\ \beta^{-k3X}.\ K.m.Y.d^X \bmod q$ (substitute K e)

$= \alpha^{-k3X}.k_1^{-k2}.\ \beta^{-k3X}.\ k_1^{k2}.Y^{k3}.\ m.Y.d^X \bmod q$ (substitute Y)

$= \alpha^{-k3X}.k_1^{-k2}.\ \beta^{-k3X}.\ k_1^{k2}.\ \alpha^{k3X}.\ \beta^{k3X}.\ m.Y.d^X \bmod q$

(inverses cancel each other)

$= m.Y.d^X \bmod q$ (substitute Y value)

$= m.\ \alpha^X.\ \beta^X.d^X \bmod q$ (substitute d value)

$= m.\ \alpha^X.\ \beta^X.\ \alpha^{-X}.\ \beta^{-X} \bmod q$ (inverses cancel each other)

$= m$

Thus, proposed EEC algorithm has beenproved mathematically.

Data Owner:

Encryption

Choose two random integers k_1, k_2 suchthat $1 \leq k_1, k_2 \leq q-1$, $k_1=25$, $k_2=16$Compute one-time-key $K = (k_1)^{k2} . Y^{k3} \bmod q$, K=54

Compute $C_1 = \alpha^{k3} \bmod q$, $C_1=27$, $C_2 = k^{k2} \bmod q$, $C_2=52$Convert key file characters into ASCII values as,

Key file

=> 000300160003ATCGCTAG$D*N@A

=>{48 48 48 51 48 48 49 54 48 48 48 51 65 84 67 71 67

84 65 71 36 68 42 78 64 65}

Let message m = {48 48 48 51 48 48 49 54 48 48 48 51 65

84 67 71 67 84 65 71 36 68 42 78 64 65},

Compute $C_3 = K. m. Y \bmod q$, C_3= {2 2 2 40 2 2 82 78 2 2 2 40 49

54 7 24 7 54 49 24 52 87 27 79 70 49}

Ciphertext $C = (C_1, C_2, C_3)$ are sent to Data User.

Data User:

Decryption

Recover keys bycomputing $K = C^K . C_2 . \beta^{k3.K} \bmod q$, K=54Retrieve message m= $K^{-1} . C_3 . d^K \bmod q$,

m = {48 48 48 51 48 48 49 54 48 48 48 51 65 84 67 71 67

84 65 71 36 68 42 78 64 65}

Convert ASCII values into characters to obtain original key file as

=> {48 48 48 51 48 48 49 54 48 48 48 51 65 84 67

71 67 84 65 71 36 68 42 78 64 65}

Key file => 000300160003ATCGCTAG$D*N@A

PERFORMANCE ANALYSIS

The suggested solution is realized by establishing a private cloud with Eucalyptus. As Data Owners or Data Users, twelve nodes are constructed. The Data owner is the node that begins the upload of a file and is responsible for encrypting and sharing the key file with users. The Data Owner encrypts data and uploads it to cloud storage server. The Data Owner will provide the key file to Data Users. The original data will be obtained by the Data Users when they have accessed the encrypted file from cloud storage server & the key file from Data Owner. By uploading the encrypted original updated file to the cloud storage server, Data Users might assume the position of Data Owner. The present data synchronisation mechanism is used to assure the consistency of shared data. The performance of the proposed framework has been assessed using this cloud configuration.

To commit that Enhanced ElGamal Cryptosystem is more secure than ordinary ElGamal cryptosystem, private key term must bemade challenging against cryptanalysis. In this scenario, X is a private key, is a primitive root, & d is the inverse of primitiveroot multiples, which is not disclosed to the Data Owner.

Incryptanalysis, X must be computed by solving discretelogarithm problems, & d must be chosen at random. In ElGamal cryptosystem, m = C2. C-K mod q, making cryptanalysis simple by identifying private key 'X' at random. The Enhanced ElGamalCryptosystem defines m as (CK. C2)-1. C3. dK mod q. As a result, cryptanalysis has gotten more sophisticated, with the private key being introduced numerous times & modular inverse of public terms being used to complete the decryption. As a result, it will take longer to break the Enhanced ElGamal cryptosystem than it did to crack the ElGamal cryptosystem.

Encryption in ElGamal cryptosystem requires two powermodulus & one multiplication modulus operation, whereas decryption requires one power modulus, one multiplicative inverse, & one multiplicativemodulus operation. However, with the Enhanced ElGamal cryptosystem, encryption requires (i) four power modulus and three multiplication modulus operations, and (ii) three power modulus, one multiplicative inverse, & four multiplicative modulus operations.

As a result, an Enhanced ElGamal cryptosystem's encryption and decryption timings will be longer than those of an ElGamal cryptosystem. Nonetheless, the level of security is better than with the prior ElGamal cryptosystem. Only the key file and intron sequence are sent on a regular basis between Data Owner & Data Users in order to preserve proposed system's security level while using the recommended Enhanced ElGamal cryptosystem at a lower computing cost than the current ElGamal cryptosystem.

CONCLUSION

The research work focuses on ensuring data confidentiality for multi-user data: In multi-user, Data Owner needs to generate data and store it in the cloud. Later, Data Users may retrieve and update the data in the cloud. The key file to decrypt the stored data will be shared with Data User based on the demand. For sharing the key file and intron sequences securely, Enhanced ElGamal cryptosystem is proposed to provide confidentiality in the data transfer. The experiments are conducted in the cloud setup, and results prove that the proposed cryptosystem is efficient. The Enhanced ElGamal cryptosystem complexity is improved to increase the security provided for sharing intron sequences and key files. The results show that Enhanced ElGamal cryptosystems perform slower compared to exiting ElGamal Cryptosystem. However, the security analysis proves that the proposed Enhanced ElGamal cryptosystems ensure data confidentiality in the cloud framework. As a result, it was concluded that the Improved Secure Cloud Data Storage Framework (ISCDSF) is developed and evaluated with proposed cryptosystems and data auditing protocols for ensuring data confidentiality, integrity, and availability of single owner and multi-user data in the cloud.

REFERENCES

1. V inaykumar Pant & Ashutosh K umar 2016, 'DNA cryptography an new approach to secure cloud data', International Journal of Scientific & Engineering Research, vol. 7, no. 6, pp. 890-895.
2. Rongmao Chen (2006), 'AV ISPA: Automated V alidation of Internet Security Protocols and Applications', ERCIM News.
3. Joseph, K , Liu, K aitai Willy Jianghua & Y ang 2016, 'Two-Factor data security protection mechanism for cloud storage system', IEEE Transactions on Computers, vol. 65, no. 6, pp. 1992-2004.
4. Zheng Y an, Mingjun Wang, Y uxiang Li & V asilakos Athanasios, V 2016, 'Encrypted data management with deduplication in cloud computing', IEEE Cloud Computing, vol. 3, no. 2, pp. 28-35.

5. Hui Tian, Y uxiang Chen, Chin-Chen Chang, Hong Jiang, Y ongfeng Huang, Y onghong Chen & Jin Liu 2017, 'Dynamic-hash-table based public auditing for secure cloud storage', IEEE Transactions on Services Computing, vol. 10, no. 5, pp. 701-714.
6. Jian Shen, Jun Shen, X iaofeng Chen, X inyi Huang & Willy Susilo 2017, 'An efficient public auditing protocol with novel dynamic structure for cloud data', IEEE Transactions on Information Forensics and Security, vol. 12, no. 10, pp. 2402-2415.
7. Wang, Xingyuan (2018), 'Color image DNA encryption using NCA map-based CML and one-time keys', Signal Processing, Elsevier, vol. 148, no. 1, pp. 272-287.
8. Zhang (2018), 'Achieving verifiable, dynamic and efficient auditing for outsourced database in cloud', Journal of Parallel and Distributed Computing, Elsevier, vol. 112, no. 1, pp. 97-107.
9. Manreet Sohal & Sandeep Sharma 2018, 'BDNA-A DNA inspired symmetric key cryptographic technique to secure cloud computing', Journal of K ing Saud University–Computer and Information Sciences, Elsevier, vol. 2018, no. 1, pp. 1-9.
10. Su Peng, (2019), 'Efficient, dynamic and identity-based Remote Data Integrity Checking for multiple replicas', Journal of Network and Computer Applications, Elsevier, vol. 134, pp. 72-88.
11. Yannan Li, Y ong Y u, Geyong Min, Willy Susilo, Jianbing Ni & K im-K wang Raymond Choo 2019, 'Fuzzy identity-based data integrity auditing for reliable cloud storage systems', IEEE Transactions on Dependable and Secure Computing, vol. 16, no. 1, pp. 72-83.
12. Aiping Li, Shuang Tan & Y an Jia 2019, 'A method for achieving provable data integrity in cloud computing', The Journal of Supercomputing, Springer, vol. 75, no. 1, pp. 92-108.
13. Hossein Nematzadeh, Rasul Enayatifar, Mehdi Y adollahi, Malrey Lee & Gisung Jeonge 2020, 'Binary search tree image encryption with DNA', Optik-International Journal for Light and Electron Optics, vol. 202, pp. 1-10.
14. Jianan Hong , K aiping X ue , Y ingjie X ue , Weikeng Chen , David, S, Wei L, Nenghai Y u & Peilin Hong 2020, 'TAFC: Time and attribute factors combined access control for time-sensitive data in public cloud', IEEE Transactions on Services Computing, vol. 13, no. 1, pp. 158-171.
15. Feng Wang, Li X u, K im-K wang Raymond Choo, Y uexin Zhang, Huaqun Wang & Jiguo Li 2020, 'Lightweight certificate-based public/private auditing scheme based on bilinear pairing for cloud storage', IEEE Access, vol. 8, pp. 2258-2271.
16. Xiaoqiang Di (2020), 'Research on integrity check method of cloud storage multi-copy data based on multi-agent', IEEE Access, vol. 8, pp. 17170-17178.
17. Viswanath and Krishna etal. (2021) "A Hybrid Cryptographic Model Using AES and RSA for Sensitive Data Privacy Preserving" Webology, Volume 18, Special Issue on Current Trends in Management and Information Technology, October, 2021 Received May 06, 2021; Accepted August 08, 2021 ISSN: 1735-188X DOI: 10.14704/WEB/V18SI05/WEB18219.
18. Denis, R.; Madhubala, P. Hybrid data encryption model integrating multi-objective adaptive genetic algorithm for secure medical data communication over cloud-based healthcare systems. Multimed. Tools Appl. 2021, 80, 21165–21202.
19. Ming, Y.; He, B.; Wang, C. Efficient revocable multi-authority attribute-based encryption for cloud storage. IEEE Access 2021, 9, 42593–42603.
20. Rafique, A.; Van Landuyt, D.; Beni, E.H.; Lagaisse, B.; Joosen, W. CryptDICE: Distributed data protection system for secure cloud data storage and computation. Inf. Syst. 2021, 96, 101671.
21. Jayapandian, N. Cloud Dynamic Scheduling for Multimedia Data Encryption Using Tabu Search Algorithm. Wirel. Pers. Commun. 2021, 120, 2427–2447.
22. Ramachandra, Mohan Naik, Madala Srinivasa Rao, Wen Cheng Lai, Bidare Divakarachari Parameshachari, Jayachandra Ananda Babu, and Kivudujogappa Lingappa Hemalatha. 2022. "An Efficient and Secure Big Data Storage in Cloud Environment by Using Triple Data Encryption Standard" Big Data and Cognitive Computing 6, no. 4: 101.

23. Cuzzocrea, A.; Karras, P.; Vlachou, A. Effective and efficient skyline query processing over attribute-order-preserving-free encrypted data in cloud-enabled databases. Future Gener. Comput. Syst. 2022, 126, 237–251.
24. Rashmi, P.; Supriya, M.C.; Hua, Q. Enhanced Lorenz-Chaotic Encryption Method for Partial Medical Image Encryption and Data Hiding in Big Data Healthcare. Secur. Commun. Netw. 2022, 2022, 9363377.
25. A, Reyana, Sandeep Kautish, Sapna Juneja, Khalid Mohiuddin, Faten Khalid Karim, Hela Elmannai, Sara Ghorashi, and Yasir Hamid. 2023. "Enhanced Cloud Storage Encryption Standard for Security in Distributed Environments" Electronics 12, no. 3: 714.
26. Elgamal, T 1985, 'A public key cryptosystem and a signature scheme based on discrete logarithms', IEEE Transactions on Information Theory, vol. 31, no. 4, pp. 469-472.