Securing Confidential Files using Cryptography

Sanket Baghade[1], Balakrishna Das[2]
[*1]Tulsiramji Gayakwad Patil College of Engineering and Technology
[*2] Assistant Professor Tulsiramji Gayakwad Patil College of Engineering and Technology
(Affiliated to RTMNU) Nagpur (MH), India

ABSTRACT – Security is now becoming the important aspects in daily computing. Daily we are using internet to send some files to our friends and relatives. After sending data unauthorized person can access this data using various ways. Unauthorized person can access the data for his own use. To counter above problem cryptography is used. There are numerous algorithms are used to secure the data. Some cryptography algorithms are Symmetric key, Asymmetric key, Hash function, Steganography, Stream ciphers, Block Ciphers, etc.

To increase the security of algorithm we have to increase key size also after this it becomes more difficult for the unauthorized person to guess right key because in increasing the size of key means that there are more possible combinations to form key.

But only increasing the size of key does not ensure security, the algorithm also plays a vital role in the security of data. In general size of key should be enough to securing the files.

The discussed paper focus on the cryptography techniques which is used to secure the data and what are the outcomes we are getting by using this algorithm.

Problem Statement -
The possibility of being vulnerable to quantum computing assaults is currently one of the primary issue statements for cryptography methods. As quantum computing technology advances, it will be possible for quantum computers to address issues that are currently beyond the capabilities of classical computing technology, such as factoring very big integers and decrypting some encryption techniques.

Making sure that the keys used for encryption and decryption are securely delivered to all parties that require them, without the keys being intercepted or compromised by an attacker, is another problem statement.

The final consideration is legal and compliance with the rules and legislation relating to the application of cryptographic techniques**.**

Keywords-Cryptography, Symmetric key, Asymmetric key, Hash function, Stenography, Stream ciphers, Block ciphers, Encryption, Decryption, quantum computing

I. INTRODUCTION

In this modern world organization, private and government companies, schools, colleges, and even hospitals have the confidential information stored in their desktop or in the cloud. To secure this information cryptography algorithms are use, data present in the desktop is converted from plaintext to cipher text with after set to read only and delete option disabled for all the encrypted files. The term cryptography has the specific meaning as “Secret Writing”. In cryptography two major processes happens encryption of data and decryption of data.

The conversion of plain text to cipher text is encryption and conversion of cipher text to plain text is called decryption.

To maintain the confidentiality of data there are lot of cryptography algorithms is used are as: AES(Advanced Encryption Standard), DES(Data Encryption Standard), Blowfish, Two fish, RSA, Elliptic Curve Cryptography, Diffie-Hellman, Hash Function, etc.

According to users requirement this algorithms are used. This algorithms can be categorized on the basis of their security requirements:

Privacy Algorithms: These algorithms are used to protect the privacy of information by encrypting it so that only authorized parties can access it. Examples of privacy algorithms include symmetric key algorithms such as AES and asymmetric key algorithms such as RSA.

Integrity Algorithms: These algorithms are used to ensure the integrity of information by detecting unauthorized changes or modifications to data.
Examples of integrity algorithms include hash functions such as SHA-256

Authentication Algorithm: This algorithm is used to verify the identity of a user or device.
Examples of authentication algorithms include digital signatures and password-based authentication.

Key exchange algorithm: This algorithm is used to exchange keys between two parties in communication. Examples of significant cha nges include Diffie-Hellman and elliptic curve Diffie-Hellman.

Non-repudiation Algorithm: This algorithm is used to prevent users from denying certain actions. Examples of non-repudiation algorithms include digital signatures and public key infrastructures (PKIs).

But the most important to note for most real cryptography application it is important to combine the features of two different algorithms to provide a complete security because no single cryptography technique is able to secure the data. For example, secure communication can be achieved by using symmetric key algorithms (AES or blowfish or two fish) for integrity hash function can be used. For authentication digital signature and public key infrastructure(PKI).

II. RELATED WORK

Security is still a challenge in the transmission of data. To counter this lots are algorithms are used, many papers have proposed various approaches in terms of securing data transmission.

[1] This paper discusses a technique of quick messages and textual content files cryptography turned into added, implemented, and tested; other general methods (DES, 3DES, AES,) have been additionally applied the use of the same messages and textual content files. The proposed method introduced enhancements to the usual techniques of records cryptography with the aid of rapidly growing the efficiency and throughput of the encryption-decryption procedure. The proposed approach offers a tremendous stage of cryptography first-rate by means of maintaining MSE and PSNR appropriate and meets the necessities of proper cryptography. The delivered method gives a high level of statistics security and protection by using a complex PK, this secret's to be generated by way of a secrete and replicable speech document making the hacking technique very low. The proposed technique can be used effortlessly to protect quick messages and textual content documents of any length
Highly Secure Data Encryption (HSDE) method is used to destroy the data in the encryption stage and recover the data in the decryption phase, this method reduces the previous encryption algorithm where if size of data to be encrypted is small at this time method is efficient but if the size of data increase, then efficiency will get decrease. Also, private key must be complex. HSDE algorithm use the speech file for generation private key for encrypting and decrypting the data , and ability of this speech file is change after some interval of time to secure our data. After getting private apply XOR operation will perform on text file with data ASCII value and decrypt using private key we will get encrypted data.

[2] Arockiam, L., and S. Monikandan implemented A hybrid symmetric encryption algorithm combines symmetric and asymmetric key algorithm . Paper implements a symmetric encryption set of rules for cloud

person records in cloud storage. The set of proposed encryption rules is described in Elements, and the decryption process is the reverse of encryption. This algorithm is used to encrypt user statistics within the cloud because the person has no control over the records as soon as their consultation is logged out, the control over the records as soon as their consultation is logged out, the user. through making use of this encryption algorithm, consumer guarantees that the data is saved best on secured storage and it can't be accessed by means of administrators or intruders.
In this technique symmetric key is used for encryption and decryption of data and asymmetric key is used for encryption of secret key. This algorithm efficient for large size of input. Sender use symmetric key for encryption of data and after encrypting the data he will use the asymmetric key for encryption of secret key and this encrypted data and encrypted key is sent in the receiving side.
When the recipient receives the encrypted data, the recipient uses the private key for decryption of symmetric key and the symmetric key for decryption of data.
This algorithms also have some drawbacks are as- Complexity - This algorithm is complex than the pure symmetric and symmetric key algorithm , because of this this can lead in difficulties in implementation.
Performance – It is slower than the symmetric and asymmetric key algorithm when user deals with the large amount of data it will take more time than the previous algorithms.

[3] Rayarapu, Aditya, Abhinav Saxena, N. Vamshi Krishna, and Diksha Mundhra implemented Advanced Encryption Standard (AES) is a secret key algorithm. By using this single key is required (for encrypting , decrypting the data. It uses fixed size block i.e. 128 bits and size of key is 256,128,192 bits. The main idea to build this algorithm after encrypting the file this algorithm makes this file as read only and delete option for all encrypted files. The AES encryption process involves a series of transformations, which include the addition of a round key, substitution of bytes using a pre-defined table, shifting of rows, and mixing of columns. The number of rounds performed based on the key size. The first step is to XOR the plaintext with the key, followed by substitution, shifting, and column mixing. In the final output column mixing is omitted and the output Ciphertext . To decrypt the ciphertext, the same process is used with

the round keys applied in reverse order. If user enter wrong secret key for number of times, then pop up message will display as file cannot be encrypted. At the time of decrypting if user enter wrong secret key the same pop-up message will display like unable to decrypt the data. Shown In Fig 1(A) and (B).

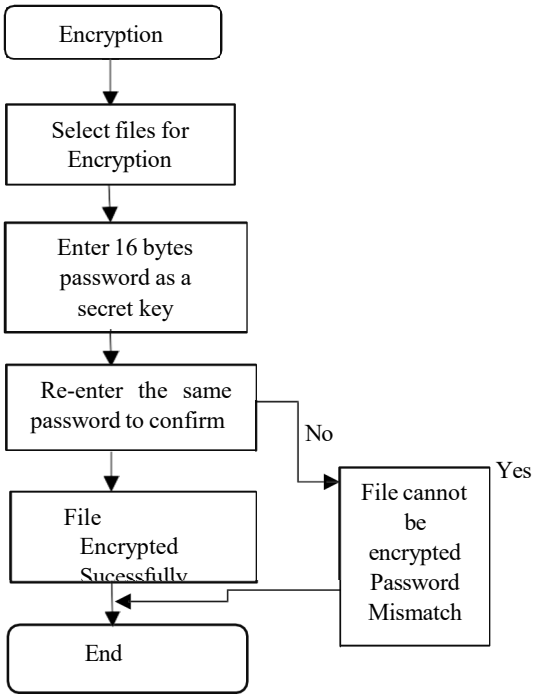


Fig. No. 1(A)Encryption Phase

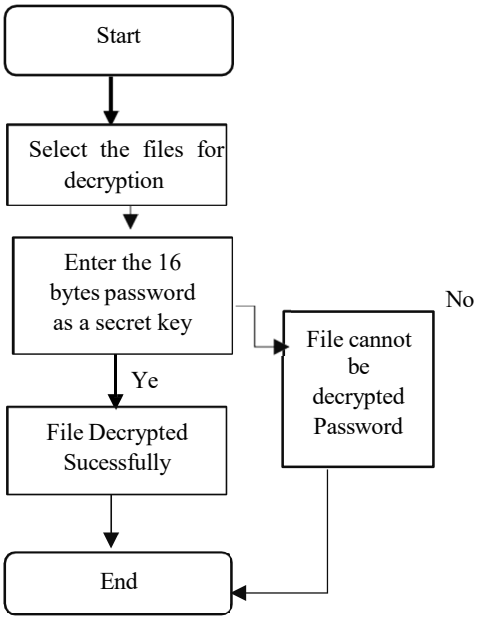


Fig No.1(B) Decryption phase

[4] Pairat Thorncharoensri has proposed the new algorithm name is signcryption which is the combination of sign and encryption. According to survey only encryption of data is not enough to secure the data because after encrypting the data sender will send the encrypted text and secret key to the receiver but what if this secret key is comes under the hands of attacker. If secret key is comes under the hand of attacker he can now decrypt text and access the data. To overcome this problem this paper introduced signcryption. In signcryption we are using signing algorithm to generate the digital signature for the message, this will ensure the authenticity of the message, as uses the sender's public

key for verification of recipient. After verifying sender will encrypt the both the message and digital signature and send the signcrypted message to the receiver. On the other end receiver first use the sender's public key for verification of digital signature and he will ensures that message is authentic or not. After this receiver use the shared symmetric key for decryption of cipher text into plain text and digital signature for getting the original message.
This algorithm uses the digital signature algorithm for authentication and symmetric key algorithm AES for secure data transmission.

[5] L. Shen, Ji. Ma, Y. Miao, Hai Liu, implemented an aggregate signature scheme is used; it is the scheme in which digital signature will allows multiple users to create a combined signature on the message. In this scheme every user will generate public unique private key and corresponding public key. For creating aggregate signature on the message each and every user have signed the message with their private key, after it will combine all individual signature and combine into the single.
For verification of aggregate signature receiver has to obtain the individual public key of all the users who has signed the message.
But this algorithm have some drawbacks like Key management , complexity.
i)Key Management – In this scheme each user will generate the pair of key that is public key and private key. Because of the large number of key , management of the keys become complex and time consuming also especially when groups contain large number of users. ii)Complexity – This algorithm is very complex and implementation is also very challenging

[6] Bhandari, Rajiv R., and Nitin Mishra. "Cloud Computing a Crm Service Based on Separate Encryption and Decryption Using Blowfish Algorithm." .In cloud data is stored in the one environment and security measures are in the different environment. Data stored in this environment after encryption but if the storage and security of data is in the same environment then there is a possibility to access the data by internal staff to counter this scenario blowfish algorithm is used with CRM service. This Blowfish algorithm is used to encrypt the data like first plaintext will be divided into 64 bits blocks and after that each block will get encrypt one by one .
In decryption phase one by one each and every block will get decrypted. By using this algorithm data is encrypted in one service provider and data get stored in the other service provider. After encryption of data, it will get stored in the other service provider and the administrator of this server will not have the information about the encrypted key service provider of encryption. If any unauthorized user tries to access the data , he will unable to use this data because he will not get decryption key because the data is stored in the different service provider and encryption is happened in the other service provider.

[7] J. Wei, W. Liu and X. Hu, suggested "Secure Data Sharing in Cloud Computing Using Revocable-Storage Identity-Based Encryption," proposed a concept of RS-IBE with gives identity revoking , updating the ciphertext repeatedly to secure previous access shared data from the revoked user. Next,RS-IBE concrete structure is presented. The proposed RS-IBE scheme state to be adaptable-secure in standard model under the decision- making assumption.
Reason behind to propose this method is if one of the use's authorization gets expired but still he can access the data share on the cloud , to overcome this , revocation algorithm is used , in revocation algorithm sender will decrypt the data which he shared on the cloud and re- encrypt the data to change the keys of that data after doing re-encrypting that user whose authorization get lost cant use the file which is in the cloud.

[8] Liang, K., Liu, J.K., Wong, D.S., Susilo, W. implemented Revocable identity-based Proxy re-encryption scheme is used to re-encrypt the , sender can re-encrypt data using his public key and able to create re-encryption key which will allows a proxy user to decrypt the data. The original sender can revoke the proxy users from accessing the data shared by him just by updating the re-encryption key. This process of revocation will happen given amount of This revocation process

occurs during a period in which the cloud, acts like a proxy, re-encrypts user ciphertexts for the current period until the next period. In future, if the user is revoked, the expired private key can no longer be used for decryption of ciphertext.

[9] Fuhry, Hirschoff, Koesnadi, Kerschbaum used “Secure Group File Sharing in the Cloud Using Enclaves”, SeGShare i s an end-to-
end encrypted group file sharing solution that supports large groups using a trusted employment environment (TEE). . Se GSare protects the confidentiality and integrity of information content, information processes, permissions, existing grou ps and group membership. This feature instantly removes permissions and ownership. It supports deduplication that redu ces back-and-forth attacks and has separate authentication and authorization.
Cloud Security Data Sharing Using Enclave is a technology that allows you to share data security in a cloud-
based environment. An enclave is essentially a secure storage area that is isolated from the system and can be used to pro tect sensitive data.

When a user wants to share information in a group, he must first encrypt the information using the group key managed b y the enclave. Encrypted data will now be stored in the cloud. Enclave will provide a secure location for encrypted data i n the cloud and allow authorized users to decrypt and access the data.
Enclaves provides secure key management and encryption which will stop the attackers to access the data.

[10] Tabit, Fursan, S. Alhomdi, Ab. Ha. Al-
Ahdal and S. Jaghtap used a new deep encryption method. This is called the New Lightweight Cryptozoology Algorithm (NLCA) and is used to improve security in the workplace.
It is based on symmetric encryption technology to encrypt the truth. The algorithm is a 16-byte (128-
bit) block cipher that requires a 16-byte (128-
bit) key to encrypt the statistics. The process is simple and very secure encryption/decryption. DES, AES and Blowfish r equire the use of various parameters such as block size, time key, arithmetic, password type and security. Experimental r esults show that the NLCA algorithm has high security and low cost, has a good security level, and achieves significant i mprovement in encryption/decryption.
Lightweight cryptography uses symmetric key algorithms to encrypt and decrypt information; the difference is that we ca n reduce the size to 128 bits (16 bytes) and the ciphertext to 128 bits. We can make data encryption more efficient by red ucing the size of keys and block ciphers. Algorithms for data encryption divide data into blocks.
But this algorithm will face poor security because we use small keys and divide the data into blocks, which also reduces t he transmission security.
[11] Subhasri, P., and A. Padmapriya praposed "Implementation of Reverse Caesar Cipher Algorithm for Cloud Computing." A Caesar is the basic encryption algorithm in which each and every letter of the plain text is shifted to a certain number position down the alphabet to form cipher text. And decryption cipher text into original plain text Reverse Caesar Cipher algorithm is used.
As shown in fig No.2 For encryption first the letter is converted into its ASCII value and it will add to the key which is given by the user and resultant of this will get converted into letter. And it will append to the cipher text.
For the decryption process first, each letter is converted into its ASCII form and it will get subtract from the key and resultant will convert into original plain text.

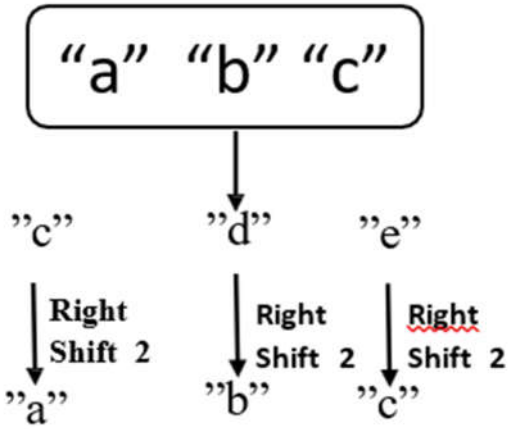
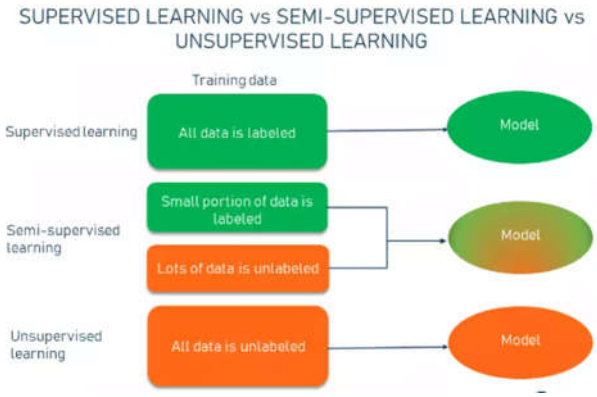


Fig. No. 2 Caesar Cipher Algorithm

[12] Self destruction of data using public and private key is using asymmetric key for encryption and decryption of data. But in the decryption phase each ciphertext is marked with the time interval.
This algorithm is divided into 5 phases.

1. Authentication and Authorization: In this phase, the customer registers first, after which the user can retrieve the information base. After the user completes registration, they can log in to the website.
2. File encryption : In this phase user started sharing the data on cloud at this phase data is encrypted using asymmetric key algorithm.
3. File sharing : The shared data is shared with the client who us requested to access the data which is shared by previous user. The data owner has authority to remove this data at any time from the cloud. The private key of the shared files is sent by Email.
4. File decryption and download : This phase client will download the file using private key shared by user if he entered wrong key many times data get erased , and suggestion mail will get sent to the user.
5. File auto-disassembly and access control for data: If the client does not download the record within the specified time, the data will be automatically deleted and the proposal email will be sent to the user again.

[13] counter key escrow and it also help to revoke the access of unauthorized users from accessing the data. Key escrow is the system in which trusted third party is known as escrow agent holds the copy of the encrypted key which is used for security of data if government agency or authorized agency wants to use the data so they can request the escrow agent to share the key and after this they can decrypt the data. But this escrow agent scheme raises concerns about government surveillance , abuse of the system by unauthorized parties. In the CP- ABE algorithm, each user is given a private key associated with an attribute. The user can decrypt the ciphertext only if the ciphertext attributes satisfy the access policy. Provide access policies directly to users and eliminate the need for a third party to manage keys. If a user loses permission to access their data, permission to re-encrypt that user's data is also revoked.



III. PROBLEM DEFINITION

Algorithm / Parameter	AES	HSDE	Hybrid symmetric encryption	Lightweight	Reverse Caesar cipher	Blowfish
Efficiency	Moderate	Excellent	High	Moderate	Weak	High
Attack	Side-Channel attack	Side-Channel attack	Chosen-Cipher Text Attack	Side Channel Attack	Brute Force Attack, Frequency analysis	Dictionary attack
Block cipher	Binary	Decimal	Binay or Decimal	Binary	Binary or Decimal	Binary
Security level	Excellent	Excellent	Excellent	Moderate	Weak	Excellent
Throughput	Low	High	High	High	Very Low	Very High

Comparison between algorithms

A recommendation system using RNNs can be limited in their ability to handle large and complex data sets, and may not be as effective in incorporating feedback or multiple objectives into the learning process.

IV. ANALYSIS AND LEARNING

From the study of above papers, we can conclude that there are some factors which can affect the efficiency of algorithm.

Block size – Number of bits present in the data can affect the efficiency of algorithm. Larger the block size led to slow down the performance , and it also require more security. Shorter the size of block means less time required to process bits in the data.

Key size – key is also important factor which affect the efficiency of the algorithm. A smaller the key leads to less computation which means it helps in faster performance. Algorithm design – Encryption algorithm is also playing vital role for efficiency of the algorithm.

Number of rounds - some of the encryption algorithm requires multiple rounds for encryption of the data, as increase in the number of rounds means more computation needs which can lead for slow performance.

One more thing only one algorithm cannot ensures the complete security so for complete security of cryptography application combination of two or more algorithm is used.

These are some factors which affect the efficiency of the cryptography algorithm , by maintaining these factors we can increase the efficiency of the algorithm to secure the data , and it can also lead faster performance of encryption and decryption process.

V. CONCLUSION

Technology has surpassed the limits of human expectations. Along with the new technologies come new challenges and one of the biggest challenges is the security and protection of the user's potential information from attackers. The focus paper is to study cryptography algorithms that are more efficient, secure, and powerful enough to handle security breaches. Various encryption and decryption algorithms like hybrid symmetric algorithms, Advance Encryption Algorithms, and hash functions are there, that can be improved by increasing the key size and adding multiple rounds of encryption phase can make them more efficient.

REFERENCES

[1] Mua'ad, M., and Ziad A. Alqadi. "Using Highly Secure Data Encryption Method for Text File Cryptography." IJCSNS 20.11 (2020).

[2] Arockiam, L., and S. Monikandan. "Data security and privacy in cloud storage using hybrid symmetric encryption algorithm." International Journal of Advanced Research in Computer and Communication Engineering 2, no. 8 (2013): 3064-3070.

[3] Rayarapu, Aditya, Abhinav Saxena, N. Vamshi Krishna, and Diksha Mundhra. "Securing files using AES algorithm." Int. J. Comput. Sci. Inf. Technol 4, no. 3 (2013): 433-435.

[4] Pairat Thorncharoensri, Willy Susilo, Yang-Wai Chow,ssss,Theoretical Computer Science,Volume 916,2022.

[5] Limin Shen, Jianfeng Ma, Yinbin Miao, Hai Liu, Provably secure certificateless aggregate signature scheme with designated verifier in an improved security model , 2019.

[6] Bhandari, Rajiv R., and Nitin Mishra. "Cloud Computing a Crm Service Based on Separate Encryption and Decryption Using Blowfish Algorithm." International Journal on Recent and Innovation Trends in Computing and Communication 1, no. 4 (2013): 217-223.

[7] J. Wei, W. Liu and X. Hu, "Secure Data Sharing in Cloud Computing Using Revocable-Storage Identity-Based Encryption," in IEEE Transactions on Cloud Computing, vol. 6, no. 4, pp. 1136-1148, 1 Oct.-Dec. 2018, doi: 10.1109/TCC.2016.2545668.

[8] Liang, K., Liu, J.K., Wong, D.S., Susilo, W. (2014). An Efficient Cloud-Based Revocable Identity-Based Proxy Re- encryption Scheme for Public Clouds Data Sharing. In: Kutyłowski, M., Vaidya, J. (eds) Computer Security - ESORICS 2014. ESORICS 2014. Lecture Notes in Computer Science, vol 8712. Springer.

[9] [9] B. Fuhry, L. Hirschoff, S. Koesnadi, and F. Kerschbaum, “SeGShare: Secure group data sharing in the cloud using Enclaves,” 2020 50th IEEE/IFIP International Dependable Systems and Networks (DSN) Annual Meeting, Valencia, Spain, 2020, p. 17. 476-488, doi: 10.1109/DSN48063.2020.00061.

[10] Sabit, Fursan, Sharaf Alhomdy, Abdulrazzaq HA Al-
Ahdal and Sudhir Jagtap. "A new lightweight encryption algorithm to improve data security in cloud com puting." Proceedings of the Global Reform Conference 2, no. 1 (2021): 91-99.

[10] Subhasri, P., and A. Padmapriya. "Implementation of Reverse Caesar Cipher Algorithm for Cloud Computing." International Journal for Advance Research in Engineering and Technology 1, no. VI (2013).

[11] Prasanna, S., S. Chinnapparaj, D. Devi, A. Athithya Janani, and S. Sophia. "Self-destruction of data in cloud using asymmetric key with key generator." Materials Today: Proceedings 37 (2021): 2818-2821.

[12]Han, Ke, Qingbo Li, and Zhongliang Deng. "Security and efficiency data sharing scheme for cloud storage." Chaos, Solitons & Fractals 86 (2016): 107-116.