Improving Data Security in Cloud Computing

[1]R. Subha, [2]Vaijayanth S, [3]Sabari Mukundh J, [4]Sanjay R and [5]Santhosh T
[1,2,3,4,5]Department of Computer Science and Engineering, Sri Eshwar College of Engineering, Coimbatore, India
[1]subha.rcse@sece.ac.in,[2]vaijayanth.s2019cse@sece.ac.in, [3]sabarimukundth.j2019cse@sece.ac.in,
[4]sanjay.r2019cse@sece.ac.in, [5]santhosh.t2019cse@sece.ac.in

Article Info
A. Haldorai et al. (eds.),*2nd International Conference on Materials Science and Sustainable Manufacturing Technology,*
Advances in Computational Intelligence in Materials Science.
Doi:https://doi.org/10.53759/acims/978-9914-9946-9-8_5

Abstract - The objective of this project is to create a secure method of encrypting and storing data in cloud computing settings. In order to accomplish this, we compare the performance of three popular encryption algorithms—AES, DES, and MES—with various key lengths. Finding the ideal encryption technique and key length for our project is the goal of this evaluation. A secure system for encrypting and storing data in cloud computing settings is the anticipated result of this project, and it can help safeguard sensitive data from unwanted access and potential security breaches.This study can help with the future development of more effective cloud security solutions by illuminating the efficacy of various encryption approaches in protecting data in the cloud.

Keywords - Modular Encryption, Advanced Encryption Standard, Symmetric key, Data Encryption Standard, Role-based access control**.**

I. INTRODUCTION

The way we store, handle, and manage data has been changed by cloud computing. Organizations maynow expand their computer resources and services as needed, which lowers costs and boosts productivity.Yet, concerns regarding the security of data kept on the cloud have grown in recent years. The amount of sensitive data being processed and kept on the cloud has grown tremendously as a result of the widespread use of cloud-based apps, services, and storage solutions, making it a prime target for cyberattacks.

With cloud computing, data security is an important concern. It has a number of features like privacy, availability, secrecy, and integrity. Cloud service providers and their clients share responsibility for the security of the data they store in the cloud. While cloud service providers are responsible for maintaining the cloud infrastructure, customers are responsible for protecting their data and applications **Fig 1** shows cloud architecture.

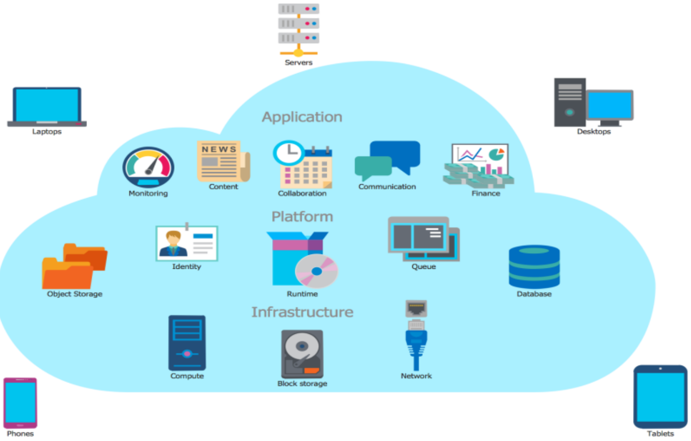


Fig1. Cloud Architecture

II. CONCEPTS INVOLVED

AES-256(Advanced Encryption Standard)

Symmetric encryption algorithms like AES-256 are frequently employed to protect sensitive data. With a 256-bit key size, it stands for Advanced Encryption Standard. AES-256 uses 128-bit blocks of data to encrypt and decrypt data using a 256-bit secret key. uses a number of intricate mathematical procedures, such as substitution, permutation, and XOR operations, to modify thedata.

The safety of the utilized encryption key determines the security of the encrypted data, even if AES-256 is a very powerful encryption method.

Modular Encryption Framework

The Modular Crypt Format (MCF), a framework for encoding encrypted passwords in a modular manner, may be what you're referring to. Several operating systems and applications use MCF to safely store user passwords. It provides flexibility in selecting the right security level for a particular system or application by allowing the use of various encryption algorithms and hashing operations. MCF operates by combining a password with a salt value, which is subsequently hashed using a predetermined algorithm.

ChaCha-20

A symmetric-key stream cipher technique called ChaCha20 is created to offer great levels of security and efficiency in software applications. In order to create the ciphertext, ChaCha20 first creates a keystream of pseudorandom bits, which is then XORed with the plaintext. To provide a distinct keystream for each encryption, it uses a 256-bit key and a 64-bit nonce (a number used just once). used in file transfer protocols, virtual private networks (VPNs), and instant messaging software programmes that call for quick and safe encryption.

ChaCha20 has been adopted by major technology companies and organizations, including Google, Cloudflare, and the Internet Engineering Task Force(IETF).**Fig 2** shows ChaCha-20 Flow Diagram.

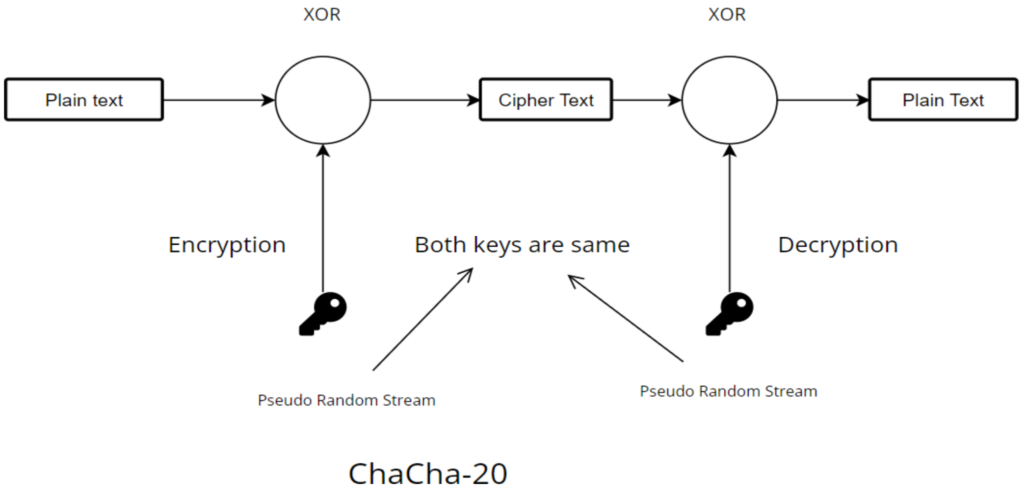


Fig2. ChaCha-20 Flow Diagram

Elliptic Curve Cryptography

Elliptic curve theory serves as the foundation for the public-key cryptographic technique known as elliptic curve cryptography (ECC). Compared to RSA and other public-key techniques, it is a contemporary and commonly used encryption technique that offers strong security with relatively modest key sizes. A secret key and a public key, which are connected, are used by ECC. While the owner keeps the private key a secret, everyone who needs to connect securely with the owner is given access to the public key. Digital signatures, secure communication, and key exchangeprotocolsarejustafewofthemanyusesfor ECC. useful in embedded and mobile devices, when processor speed and storage capacity restrictions render conventional encryption methods impracticable.**Fig 3** shows elliptic curve cryptography.

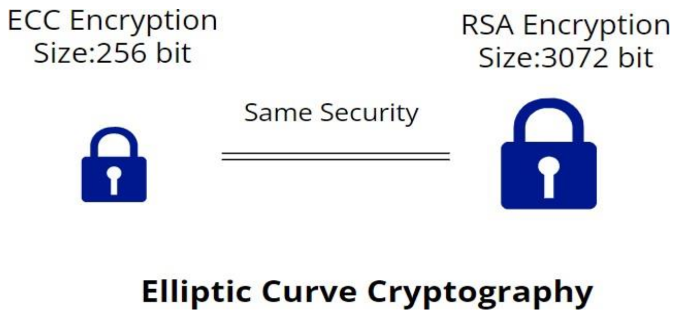


Fig3. Elliptic Curve Cryptography

Two Fish Storage

A symmetric-key block cypher method called Twofishis employed for both data encryption and decryption. Before being saved, sensitive data can be encrypted using Twofish. Twofishemploys keys with different lengths, ranging in size from 128 to 256 bits. It works with data blocks that are fixed at 128 bits in size. The data is encrypted by the method using a combination of substitution and permutation operations. Used for a variety of encryption-intensive applications, such as secure communication, digital rights management, and datastorage.

RBAC

Role-Based Access Control is referred to as RBAC. It is a technique for restricting access to resources based on the roles that users have been given. According to RBAC, a user's access to resources is determined by their position or role within an organization. Often, job functions are used to establish roles, such as manager, administrator, or operator. RBAC is frequently employed in corporate systems in order to safeguard users' access to only the resources they need to complete their tasks and prevent unwanted access to sensitive data.

CASB

A Cloud Access Security Broker (CASB) is a security tool that sits between an organization's on-premises infrastructure and the internet and the cloud services it utilizes. CASBs give businesses the ability to implement security regulations and defend against cloud-based attacks.

Identity and Access Management (IAM): CASBs are able to offer user authentication and access controls for cloud services, enforcing rules around who has access to what information and when.

Data Loss Prevention (DLP): CASBs are able to recognise and stop sensitive data from entering or leaving cloud apps. To safeguard data both in transit and at rest, they can additionally include encryption and tokenization.

Threat Protection: CASBs are capable of spotting and thwarting malware, phishing scams, and other attacks aimed against cloud applications.

III. LITERATURE SURVEY

[1] Nidhi and Ajay Rana's "Data Security in Cloud Computing: A Review" (2018). This paper provides an in-depth examination of cloud computing's data security, addressing the main threats to data security,obstacles to data security, as well as various data security methods and solutions. In order to defend against threats like malware, phishing assaults, and denial of service (DoS) attacks, the authors stress the significance of adopting multi-layered security techniques. A Survey of Security Problems and Solutions in Cloud Computing An overview of cloud computing security challenges, including data security, is provided by N. Thirunavukarasu and K. Selvi, who also examine potential remedies and ways to deal with these issues. The authors stress the significance of adhering to legal standards such as the Health Insurance Portability and Accountability Act and the General Data Protection Regulation (GDPR). Advanced Encryption Standard (AES) Improving Data Security in Cloud Computing An improved datasecuritysystem for cloud computing employing the Advanced Encryption Standard (AES) algorithm is proposed byA. Priyanka and M. Ramesh. The suggested approach offers high-level encryption and decryption skills to protect the integrity and confidentiality of data by combining symmetric and asymmetric encryption algorithms. The authors stress the significance of utilizing cutting-edge encryption methods to safeguard against data breaches and other forms of cyberattacks in cloud computing.'Secure Data Storage and Retrieval in Cloud Computing,' portion IV K. Sree Lekha and K. Srinivas has presented a secure data storage and retrieval system that uses encryption and decryption methods to protect the confidentiality and integrity of the data. The suggested approach uses a combination of symmetric andasymmetricencryptiontechniquestoencryptdata both in transit and at rest. It also includes access control features to prevent unauthorized access to data.[V] A secure data sharing model for cloud computing is put forth in the study "Secure Data Sharing in Cloud Computing" by S. Srinivasan and S. Venkatesan (2018). To safeguard the security and privacy of data, this model incorporates procedures for access control, authentication, and encryption. The requirement for secure and effective data exchange between various users and applications is noted by the authors as more enterprises shift their data and services to thecloud.

IV. EXISTING METHOD

The existing method has some following disadvantages.

Loss of control

The fact that businesses have less control over their data and equipment is one of the major downsides of cloud computing security. Organizations could lack transparency and confidence in the security of the cloud environment because security controls must be developed and maintained by the cloud serviceprovider.

Shared infrastructure

While using cloud computing, many users and applications share infrastructure and resources. This raises the possibility of data leakage and unwanted access to privateinformation.

Insider threats
Employees or contractors with access to cloud resources are examples of insider risks who may purposely or accidentally harm data and systems. In a cloud setting, this can be very difficult to detect andprevent.

Data breaches
Cloud environments are susceptible to data breaches, which could expose sensitive information and cause stakeholders and customers to lose faith inthem.

Compliance And Regulatory Issues
For businesses that operate in regulated sectors like healthcare and finance, compliance and regulatory difficulties can present a substantial barrier. The security rules of the cloud provider may be in disagreement with compliance standards, which couldhavenegativelegalandfinancialrepercussions.

V. PROPOSED SYSTEM

The solution we are proposing to change the way things are done now functions similarly to an encryption system that employs many algorithms at various levels. The same key is used for both encryption and decryption in the speedy and efficient AES encryption method. Using the same key for encryption and decryption could eventually lead to a lack of security, but ChaCha20 allows for a workaround by generating different keys for both encryption and decryption. Moreover, the procedure requires less memory and processing time when several keys are generated simultaneously. Elliptic curve cryptography is a different method for encrypting data. While RSA uses 3072 bits of memory, it only utilizes 256 bits. The public key is given to users so they may access the database's data, while the owner securely holds the private key. Secure communication and digital signatures work together to achieve this strategy. Role-based access control and third-party attack prevention are crucial functions of RBAC. The two fish storage system makes it possible to store the data in the required format.Basedonkeypermutationsandcombinations, the sizes used here range from 128 bits to 256 bits. As a result, the security of the data will be significantly increased by applying these modern encryptiontechniques.**Fig 4** shows flow diagram for data security.

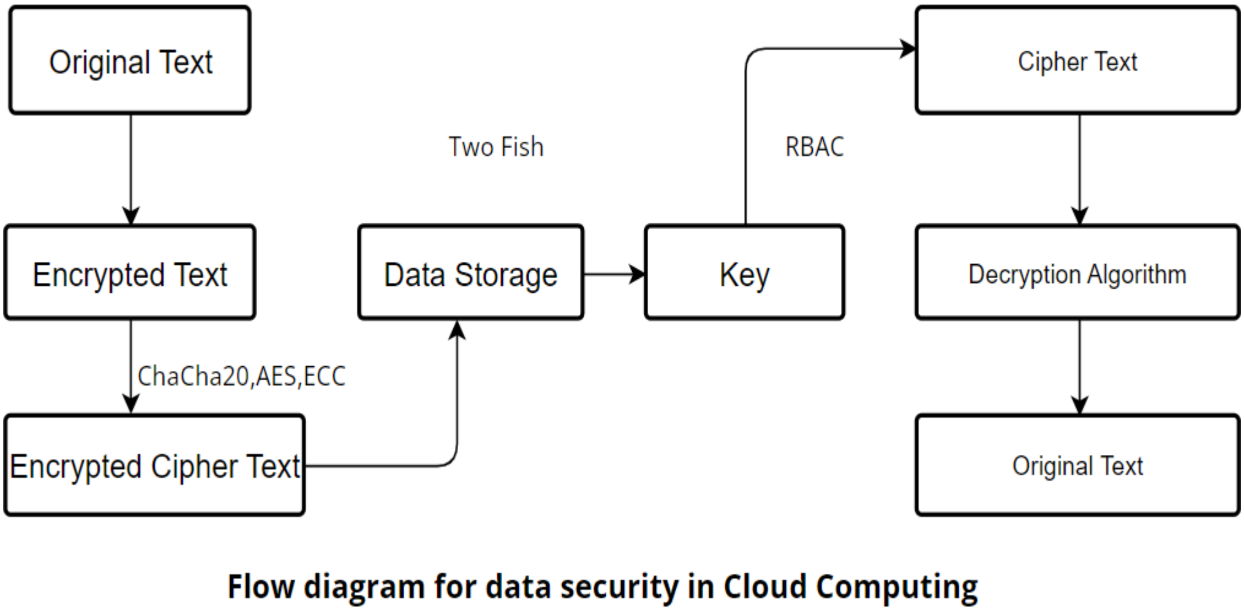
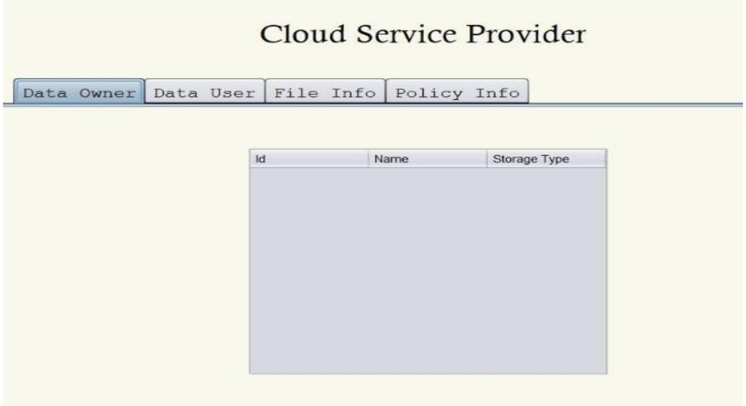


Fig4. Flow diagram for data security.

VI. EXPERIMENTS AND RESULTS

The front end of this project, which functions as a desktop application, was created using Java. Also, the database levels grant Role Based Access, and the data saved in the database can be stored and accessed using the MySQL server. This verifies the security of the data and determines whether it is encrypted and saved in the proper format. Since it uses symmetric encryption, the same key is utilised regardless of the user's role to access and retrievedata.**Fig 5** shows sample output.



Cloud Service Provider

Id	Name	Storage Type

Fig5. Sample Output

VII. CONCLUSION

Data is encrypted and decrypted using cryptography to protect data security. Our approach makes use of symmetric encryption techniques, enhanced algorithms, and role-based access control to further increase data security. The quantity of information communicated will depend on the function that person has been given; unless given special permission, they cannot access any further information. By utilizing several encryption techniques, it is memory and time efficient (AES, ECC,ChaCha20).

APPENDIX A- IMAGE REFERENCE

Fig. No	Reference
Fig.1	http://shorturl.at/oDPW2
Fig.2	http://shorturl.at/emBMR
Fig.3	http://shorturl.at/emBMR

References

[1]. Y. Al-Issa, M. A. Ottom, and A. Tamrawi, “eHealth Cloud Security Challenges: A Survey,” Journal of Healthcare Engineering, vol. 2019, pp. 1–15, Sep. 2019, doi: 10.1155/2019/7516035.

[2]. H. Jin, Y. Luo, P. Li, and J. Mathew, “A Review of Secure and Privacy-Preserving Medical Data Sharing,” IEEE Access, vol. 7, pp. 61656–61669, 2019, doi: 10.1109/access.2019.2916503.

[3]. D. Liu, Z. Yan, W. Ding, and M. Atiquzzaman, “A Survey on Secure Data Analytics in Edge Computing,” IEEE Internet of Things Journal, vol. 6, no. 3, pp. 4946–4967, Jun. 2019, doi: 10.1109/jiot.2019.2897619.

[4]. S. Chenthara, K. Ahmed, H. Wang, and F. Whittaker, “Security and Privacy-Preserving Challenges of e-Health Solutions in Cloud Computing,” IEEE Access, vol. 7, pp. 74361–74382, 2019, doi: 10.1109/access.2019.2919982.

[5]. T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, “Hey, you, get off of my cloud,” Proceedings of the 16th ACM conference on Computer and communications security, Nov. 2009, doi: 10.1145/1653662.1653687.

[6]. Garg, S., &Buyya, R. (2013). Cloud computing security: a review. In Security and privacy in communication networks (pp. 263-282). Springer, Berlin,Heidelberg.

[7]. Tsai, W. T., Lai, C. F., Chiang, M. C., &Chiang,W. Y. (2014). A review of cloud computing security issues. Journal of Internet Technology, 15(5), 643-650.

[8]. Almorsy, M., Grundy, J., & Müller, I. (2016). An analysis of the cloud computing security problem. arXiv preprint arXiv:1609.01107.

[9]. A. Algarni, “A Survey and Classification of Security and Privacy Research in Smart Healthcare Systems,” IEEE Access, vol. 7, pp. 101879–101894, 2019, doi: 10.1109/access.2019.2930962.

[10]. P. M. Mell and T. Grance, “The NIST definition of cloud computing,” 2011, doi: 10.6028/nist.sp.800-145.

[11]. W. Jansen and T. Grance, “Guidelines on security and privacy in public cloud computing,” 2011, doi: 10.6028/nist.sp.800-144.

[12]. Marian, R., &Butoi, B. (2013). Cloud computing security risks and controls. Informatica Economica, 17(2),139-149.

[13]. Rios, E., Mancuso, V., &Egea-Lopez, E. (2013). Towards a classification framework for security threats in cloud computing. Journal of NetworkandComputerApplications,36(1),273-285.

[14]. "Security Guidance for Critical Areas of Focus in Cloud Computing V4.0" by Cloud Security Alliance(CSA).

[15]. R. Vacca, “Cloud Computing Security,” Nov. 2020, doi: 10.1201/9780429055126.