International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 04 | April - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Cloud Security Using Two Key Encryption

Ms Mala Bharumathi M
Rathinam College of Arts and Science
Coimbatore, Tamil Nadu, India.
malabharumathi@gmail.com

Ms Deepti R
B.Sc. Computer Science
Rathinam College of Arts and Science
Coimbatore, Tamil Nadu, India.
deepti05ramesh@gmail.com

Ms Kaaviya Sri S V
B.Sc. Computer Science
Rathinam College of Arts and Science
Coimbatore, Tamil Nadu, India.
kaaviyaselladurai@gmail.com

ABSTRACT

This project focuses on the development of a secure file encryption and decryption system using asymmetric cryptography. By utilizing a two-key mechanism—public and private keys—the platform ensures that only authorized users can access encrypted files, making it highly secure for data storage and transmission. The system is built using PHP for backend processing, HTML for the user interface, and MySQL for storing metadata related to encrypted files. The AES algorithm forms the core of the encryption logic, offering both reliability and proven security. The design follows a three-tier architecture that separates user interaction, processing logic, and data storage, enhancing both scalability and maintainability. Deployed locally using XAMPP, the system was tested across various scenarios to ensure efficiency and user-friendliness. It supports core functionalities without storing the actual files in the database, thereby minimizing risk and reducing system load. This encryption tool serves as a practical demonstration of cybersecurity principles and provides a solid foundation for future upgrades like biometric logins and cloud integration. The project successfully meets its objectives while addressing current digital security demands.

Keywords: Cloud Computing, Cloud Platform, Data Privacy, Data Security.

I.INTRODUCTION

In the recent years, Cloud Computing is being used to deliver the services help of computing resources such as hardware and software. Nowadays Cloud computing can be widely used to enable the users or clients to use and create software from anywhere at any time without being concerned about the execution of the data or instructions.

Cloud storage is a model of data storage services where the developers can access and store digital data in cloud and the cloud resources are typically owned, managed and controlled by a service provider. These cloud storage providers are responsible for keeping the data available and accessible, and the resources protected and running.

The advantages of the storage servers are flexible with reduced cost and they also manage the risk associated with data loss. The data is properly stored and prevented by the remote services. The remote data integrity checking procedure ensures high cloud storage reliability, improved error localization and also easily identifies misbehaving server in the cloud storage and detects the errors in the data. In the future work well-organized flexible storage scheme is designed by partitioning algorithm to guarantee the accessibility of data and data correctness

II. LITRATURE SURVEY

1.Certificateless public key cryptosystem:

Certificateless public key cryptosystem (CLPKC) is a desirable cryptographic system because it refrains from both certificate management and key escrow. In CLPKC, how to revoke a misbehaving or compromised user is an important issue. However, the existing revocable methods in CLPKC are impractical because of the use of either an expensive mediator or a burdensome key generation center (KGC). In order to overcome this drawback, introduce outsourcing computation into CLPKC for the first time and design an outsourced revocable certificateless signature (ORCLS) scheme, and the revocation functionality is outsourced to a cloud server. The amount of computation needed to revoke a user is borne by the cloud server, which greatly reduces the burden on the KGC.

2.Identity-Based Access Control:

Revocable Identity-Based Access Control for Big Data with Verifiable Outsourced Computing by Hu Xiong, Kim-Kwang Raymond Choo Senior Member, IEEE, and Athanasios V. Vasilakos, Senior Member, IEEE

To be able to leverage big data to achieve enhanced strategic insight, process optimization and make informed decision, in this work need to be an efficient access control mechanism for ensuring end-to-end security of such information asset. Single encryption is one of several promising techniques to simultaneously achieve big data confidentiality and authenticity. However, single encryption suffers from the limitation of not being able to revoke users from a large-scale system efficiently.

Identity-based encryption (IBE) is a public key cryptosystem and eliminates the demands of public key infrastructure (PKI) and certificate administration in conventional public key settings. Due to the absence of PKI, the revocation problem is a critical issue in IBE settings.

Due to the absence of PKI, the revocation problem is a critical issue in IBE settings. Several revocable IBE schemes have been proposed regarding this issue. Quite recently, by embedding an outsourcing computation technique into IBE, Li et al. proposed a revocable IBE scheme with a key-update cloud service provider (KU-CSP). However, their scheme has two shortcomings. One is that the computation and communication costs are higher than previous revocable IBE schemes. The other shortcoming is lack of scalability in the sense that the KU-CSP must keep a secret value for each user.

III. PROBLEM STATEMENT

With the usage of cloud services increasing, all across the globe we witness and increase in the number of people accessing the cloud services as well And again with the increased usage of the cloud services , the potential risk that the users may face also increases.

IV. PROPOSED WORK

This research proposes the development of a double encryption based system that ensures two layer security for user‘s files. The key steps include:

User Module:

1.User Registration:

Before logging to the cloud, user has to register their details like user id, password. This registration will used to avoid anonymous users. By this user will get a user name and password for their account. Every user must be register then only they can log in the cloud.

2.Log in:

In this module user enter their username and password what they registered. After logging in to cloud, user can manage their cloud data.

3.Upload File:

In this module user can upload the file to cloud, for each files uploaded, random private key is generated and these private keys will encrypt the uploaded file and gets stored in cloud. User can view the encrypted file that is stored in cloud. User can select the available Cloud Service Provider and store the data in cloud.

4.View Uploaded File:

In this module user can view the original uploaded file by specifying public key given for specific uploaded file by Cloud Service Provider. Once again user has to enter Private Key given for specific uploaded file. Here double decryption is done to get the original data. If a hacker gets the access to uploaded file, only encrypted data will be shown to him, instead of original data.

Cloud Service Provider Module:

1.Log in:

In this module Cloud Service Provider enter their user name and password. After log in to cloud, for each user files uploaded, random public key is generated and these public keys will encrypt the uploaded file and gets stored in cloud.

2.View Encrypted File:

Cloud Service Provider can view the encrypted file that is stored in cloud. Cloud Service Provider can view the available user files that are allotted to them. He can’t view other Cloud Service Provider files.

TOOLS REQUIRED:

1.PHP:

PHP is a standard HTML file that is extended with additional features. Like a standard HTML file, PHP contains HTML tag that can be interpreted and displayed by a web browser. Anything we could normally place in an HTML file Java applets, Blinking text, server side scripts .we can place in PHP.

2.HTML:

HTML (Hyper Text Markup Language) is used to create the structure and layout of the web pages. It provides the frontend interface where users can interact with the system — for example, registering, logging in, uploading files, or entering encryption keys. HTML works alongside CSS (for styling) and JavaScript (for functionality) to build a responsive and user-friendly interface for secure cloud operations**.**

3.MYSQL:

The MySQL database can act as a backend database for this project. MySQL supports the user with its powerful database management functions.Another good reason to use MySQL as backend tool is that it is a component of the overwhelmingly popular Open source software**.**

VI. RESULT ANALYSIS:

1.Successful Encryption & Decryption:

Files were accurately encrypted with the public key(cloud admin) and private key. decrypted using the private key and public key ensuring end-to-end confidentiality.

2. Secure Key Handling:

The system maintained strict separation between public and private keys, avoiding unauthorized access during any stage.

3. User-Friendly Interface:

The front-end was intuitive and allowed smooth navigation for users with little to no technical background.

4. Efficient File Handling:

Files were processed quickly without major performance lag, even when handling moderately sized data.

5. No Data Loss Observed:

During testing, all decrypted files matched the original versions without any data corruption or truncation.

6. Consistent Database Logging:

File activity and metadata were logged accurately into the MySQL database, enabling future auditing if needed.

7. Platform Stability:

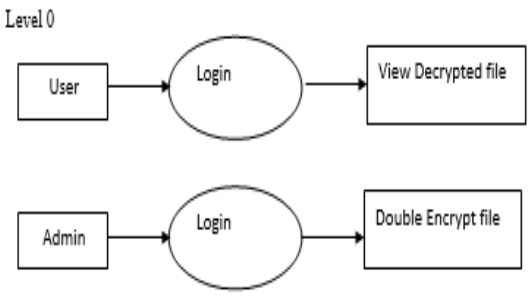
The project ran reliably on XAMPP without crashes or unexpected behavior, even after multiple operations.

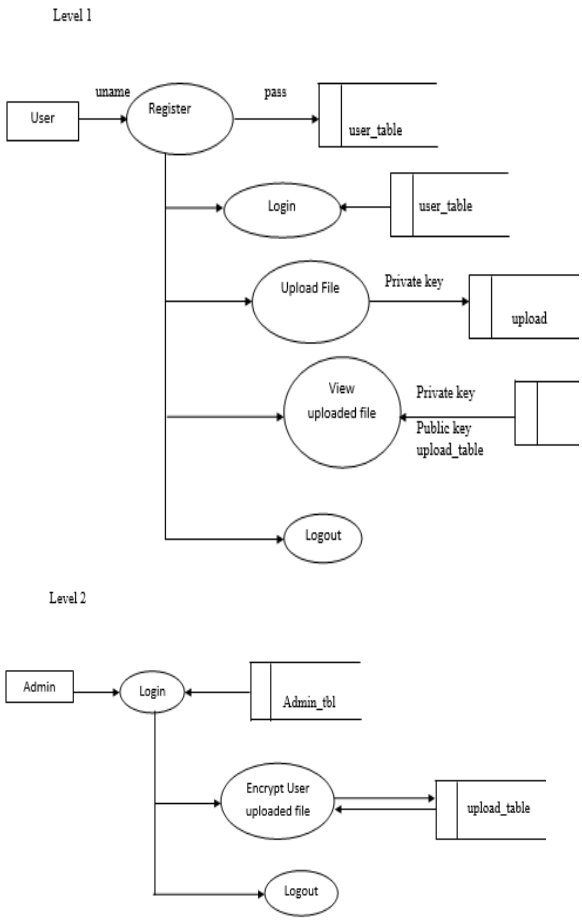
8. Successful Local Deployment:

The application was fully functional in a local environment, demonstrating the viability of real-world implementation.

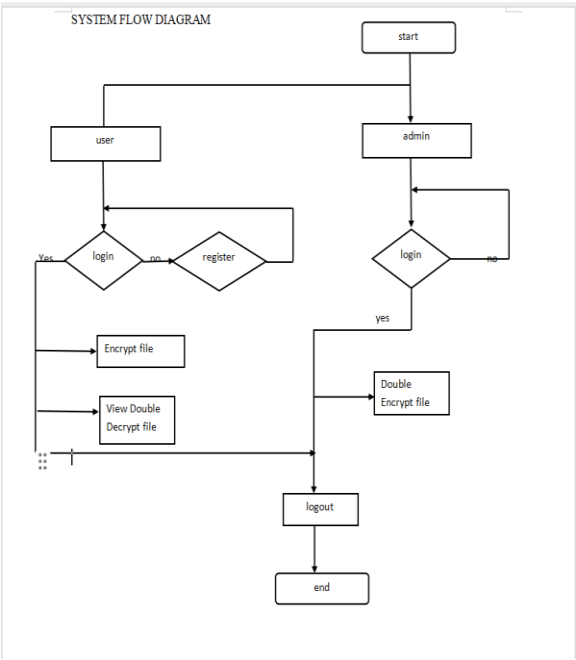
VII. FLOW DIAGRAMS:

1. Data flow Diagram:





2.System flow Diagram:



VIII. FUTURE ENHANCEMENT

To enhance the security of the encryption-decryption system, future implementations can explore the integration of biometric authentication methods such as fingerprint scanning or facial recognition. By combining biometric verification with two-key encryption, access control can be made significantly more robust. This dual-layer security would reduce the chances of unauthorized decryption even in the event of a compromised key. Biometrics also eliminate the need for users to remember passwords or manage private keys manually. The system could store encrypted biometric templates securely, only unlocking the decryption interface after identity confirmation. Such integration will align the project with modern zero-trust architecture models. Additionally, it introduces a personalized experience for users, making the encryption system more user-friendly. This can be especially useful in sectors like healthcare or defense, where privacy is paramount.

A promising direction for future development is incorporating blockchain technology to manage and verify public keys in a decentralized environment. By leveraging the immutability of blockchain, the system can prevent key tampering, spoofing, or unauthorized replacements. Each public key issued can be stored on a blockchain ledger, allowing users to verify its authenticity in real-time. This approach can eliminate reliance on a central certificate authority (CA), reducing single points of failure. Moreover, smart contracts could automate secure key exchanges and notifications about key expirations or compromises.

To push the envelope of key security, future versions of the project can implement Multi-Party Computation (MPC) using Shamir's Secret Sharing scheme. Instead of storing a private key in a single location, the key can be split into multiple fragments, distributed among different parties or servers. Only when a certain threshold of shares is combined can the original key be reconstructed. This drastically reduces the risk of a full key being exposed through a single point of failure or attack. Such architecture is especially useful in high-security environments like banking, where no one individual should have full decryption rights. The

protocol also allows for flexibility in authorization, such as board-level approvals for access. While slightly complex, tools and libraries are available to ease this integration. The result would be a system that truly embodies the philosophy of "security by design."

IX. CONCLUSION

Cloud computing is changing the way IT departments buy IT Businesses have a range of paths to the cloud, including infrastructure, platforms and applications that are available from cloud providers as online services.

Security is a major requirement in cloud computing when we talk about data storage. Information needs protection, there are many Security Threats, and different types of security risks need to be discussed. In order to improving the security and protection and building the Secure Cloud, There are number of existing techniques used to implement security, and one of them is our project "Cloud Security using Two Key Encryption".

X. REFERENCES

[1] G. Ateniese, K. Benson, and S. Hohenberger, 2009 ,"Key-private proxy Re-encryption," in Topics in Cryptology–CT-RSA vol. 5473. Berlin, Germany: Springer-Verlag, pp. 279-294.

[2] Sun Microsystems, 2009, "Introduction to Cloud Computing Architecture", Sun Microsystems Inc., white paper, pp. 1-17

[3] MELL, P. and GRANCE, T, 2009. "Definition of Cloud Computing", Draft NIST working, vol.5, pp. 7-19.

[4] J. Shao, 2012, "Anonymous ID-based proxy re-encryption," in Information Security and Privacy vol. 7372. Berlin, Germany: Springer-Verlag, pp. 364–375.

[5] Bellare, Mihir; Rogaway, Phillip (21 September 2005), "Introduction to Modern Cryptography, by random grids, vol.1, pp.10-21.