Secure File Storage Using Hybrid Cryptography

Shivani Adsule[1], Sejal Agarwal[2], Priya Gorade[3], Yogesh Deokar[4], K.G. Sawarkar[5]
[1,2,3,4] *Students Rajiv Gandhi Institute of Technology, Mumbai*
[5]*Faculty, Rajiv Gandhi Institute of Technology, Mumbai*

***Abstract*—Computing security is an emerging topic in academia right now. Many businesses are migrating from traditional data storage to cloud storage, which allows them to access data from anywhere at any time. However, the primary stumbling block for businesses considering cloud computing is data security. This study presented a cloud computing security strategy based on multilayer cryptography. The majority of consumers and businesses are shifting to the cloud since it is considerably cheaper and more convenient. Information security relies heavily on cryptography. Instead of using a single encryption algorithm, users employ hybrid encryption to secure cloud storage. In comparison to the present system, this approach raises data security to the highest level possible and takes less time to upload and download text files.**

***Index Terms*-Fernet, Hybrid cryptography, Security, Storage**

I. INTRODUCTION

Trends and movements are emerging as a result of technological developments that improve people's quality of life. People's main concern in today's fast-paced world, when everyone has a smartphone and internet access, is the security of their personal information stored online. This security problem also extends to files that are kept on the cloud. The majority of corporations are transitioning from traditional data storage to cloud storage, which provides an efficient way to access data anywhere, at any time. However, one of the major challenges in implementing cloud computing for businesses is data security. This is something that cryptography can help with the technology of cryptography converts original data into an unreadable format. Symmetric key cryptography and public key cryptography are the two types of cryptography. This method uses keys to convert data into an unreadable format. As a result, only authorized individuals have access to data stored on the cloud server. Everyone can see the cipher text data. As a result, only authorized users with the appropriate key can access data stored on the cloud storage server. Cryptography's major goal is to protect data from hackers, online/software crackers, and other third-party users. The loss of confidentiality occurs as a result of unauthorized user access to information. Security has the characteristics to prohibit or stop this type of illegal access or any other malicious attacks on the data here. A private key and a public key are the two types of keys. The private key is kept private, whereas the public key is widely known. The public key is used for encryption, whereas the private key is used to decrypt the encrypted communication, which can only be decrypted by the private key that corresponds to it.

[1]This introduced a new security technique that combines several symmetric key and steganography cryptographic algorithms. To secure data, the suggested system employs the 3DES (Triple Data Encryption Standard), RC6 (Rivest Cipher 6) and AES (Advanced Encryption Standard) algorithms. are used to secure information from unauthorized access. 128-bit keys are being used in all of the algorithms. Because of the importance of the information held on the cloud and the services given to users, security is seen as a critical feature in the cloud computing environment. A hybrid encryption algorithm has been developed based on a mixture of the RSA and AES algorithms. In their system, the user requires and stores an RSA private key while uploading data, and also an RSA public key. In the cloud, the system processes the file using the RSA and AES algorithms before correctly storing it on the server. The LSB algorithm is used for both encoding and decoding. The data from this approach can be placed in the title image's Least Significant Bit. Even then, the human eye is unable to detect the image's hidden text.

[2]Malicious attacks are particularly prevalent when one single key is used for both encryption and

decryption. This difficulty is overcome in the hybrid algorithm by using three separate keys for encryption and decryption. . In order to enforce security features, a hybrid encryption mechanism based on the AES and RSA algorithms is implemented, with AES employing a 128-bit secret key and RSA using a 1024-bit key. This study suggested a hybrid encryption algorithm that combines the RSA and AES algorithms to provide data security to Cloud users. The most significant benefit is that the keys are produced based on system time, which means that no intruder can guess them, providing us with greater security along with convenience. . The primary value of employing the RSA and AES encryption algorithms is that they supply three. After being uploaded, the data is encrypted and can only be decoded with the user's private key and secret key. The greatest benefit is that data in the cloud is highly safe.

[3]There is a short synopsis of the Fernet key encryption in this document, as well as the information that we can secure using the Fernet System. Several cryptography technologies and procedures can be used to secure data. Without the key, the Fernet network ensures that data encrypted with it cannot be changed or read. Fernet is a data encryption technology that shields information. This guarantees that a message encryption using it cannot be altered or read without the key. Fernet is a cryptographic implementation of symmetric authentication. When passwords are kept in the database, we may use typical ways to safeguard them, such as firewalls and role definitions, to prevent unauthorized access to the database. By changing the password to an inaccessible (encrypted) format, we may add an extra layer of protection. The password is maintained in plain text in the database and is not encrypted. Because the person who got into your database can access any account and do any tasks after logging in, these passwords are extremely insecure. To safeguard the password, any asymmetric encryption can be used. As a result, the plaintext password is saved in the database after being encrypted in the registry. The Fernet system can protect data by encrypting it with the Fernet key. Encryption from plaintext to ciphertext and decryption from ciphertext to plaintext are both encompassed by cryptography.

[4]There are a variety of approaches that can be used to address these difficulties. For data security, cryptography and steganography are becoming more prevalent. We have presented a new security mechanism based on the symmetric key encryption algorithm in this paper. Whatever part of the file is encrypted with which algorithm and key is mentioned in key information. The file is divided into eight sections. Each section of the file is encrypted with a separate algorithm. Author A. Shahade presents a hybrid cryptography algorithm. The hybrid algorithm employs the AES and RSA algorithms. The AES algorithm only needs a single key. Three keys are employed in the hybrid algorithm. AES secret key and RSA public key are essential for data upload to the cloud. Data integrity, security, confidentiality, and availability are all advantages of the hybrid algorithm. The RSA algorithm has a disadvantage in that it takes a long time to encode and decode data. To achieve a high level of security, the key is rotated. A hash value is generated for the purpose of data integrity. After encryption and before decryption, hash values are calculated. If both hash values are the same, the data is correct. The LSB method is used to secure key information. The SHA1 hash algorithm is used to ensure data integrity. Achieve the desired outcomes is used to attain a low latency value.

[5]Several businesses are migrating from traditional data storage to cloud storage, which allows them to access data from anywhere at any time. However, the primary stumbling block for businesses considering cloud computing is data security. This research provided a cloud computing security strategy based on multilayer cryptography. In this case, the Data Encryption Standard (DES) and RSA are used to enable multilevel encryption and decryption on both the sender and recipient sides, thereby enhancing the security of cloud storage. Despite the tremendous benefits of cloud computing, there are still a few barriers to its wider adoption. Since users' and businesses' data is stored on a platform that can be accessed by anybody, they have given over control of their data to a third party. As a result, it could be accessed by someone who isn't permitted. proposed a model in which counter propagation neural (CPN) networks are used to conduct both encryption and decryption. It's a step forward from the standard security system. It talks about how to improve information security via using three levels of

authentication. It makes no reference to the performance. The proposed solution also includes real-time system monitoring and the operation of the forensic virtual machine. . To improve the security of cloud storage, this study uses the DES and RSA encryption and decryption cryptographic algorithms. In comparison to previous cryptography-based methods, it also improves data security in cloud environments. This model can be used in the future to improve the security of cloud services through artificial intelligence techniques.

[6]Finding enough storage capacity to preserve all of the data that some computer owners have amassed is a major challenge. As a result, consumers are more likely to purchase enormous volumes of data or larger hard drives, despite the fact that they still have storage capacity difficulties. In order to mitigate security vulnerabilities, this security paradigm provides transparency to both cloud users and cloud service providers. The suggested model uses the cloudsim cloud simulator programme and is written in Java. Cloud computing provides numerous advantages, including increased flexibility, lower capital costs, and increased accessibility. Nonetheless, it is not widely recognized. Security is the main reason for this. When consumers put their data in the cloud, they grant a third party access to their data and relinquish control. As a result, attackers may be able to tamper with their data. In comparison to the present system, this approach raises data security to the highest level possible and takes less time to upload and download text files. We present a multilevel encryption and decryption cryptography algorithm in this work, which encrypts data at the client side after uploading it to the cloud server and decrypts it at the receiver side, adding an extra layer of data security. In the future, this model could be used to improve the security of cloud services utilizing artificial intelligence techniques.

II.METHODOLOGY

The main aim of the project is to secure confidential data (for example- Photo, pdf, word file) by encrypting, converting the data into binary form and storing it on the cloud.

1.To achieve secure file storage on cloud using hybrid cryptography

2. To implement the hybrid cryptography as it relate to securing file storage on cloud infrastructure

3. Achieved double security

4. Generated two different keys for encryption and description.

5. We can store n number of data on cloud using multiple login

6.Encrypt and decrypt confidential data like pdf, photo, word file

7. Upload and download data from cloud securely

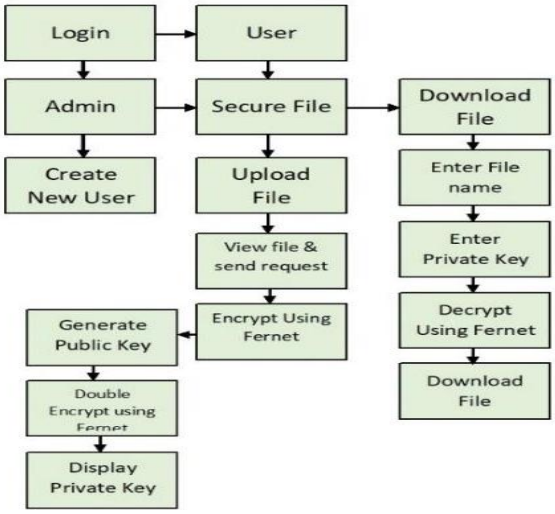

Fig 1. METHODOLOGY

For extremely secure file storage, the project intends to double security. The encryption in this case is a hybrid of two symmetric algorithms, fernet. The focus of this research is on cloud file security. The Fernet approach was applied twice for double security. Once for generating a public key and encrypting a file that has been uploaded. Encrypting the public key and providing the private key for the second time. The encryption of a combination of 20 random keys and the public key is required to encrypt the public key. A private key is created using the above encryption. .To access the uploaded file, one must have the private key and not just the public key. To download the file one must have the name and private key of that respective file. Using them the actual file can be downloaded. The information is kept in a database to which only the admin has access Database contains the data of login and uploaded files. Login data has the information of all the details of admin and users whereas data collection has the information of uploaded files like id, user type, public keys, edata, file name and time. Login details include user name, password and type.

User name, password, and type are all required while logging into the system.

III.TECHNOLOGIES USED

A.PYTHON 3.7.4

Python is a dynamic object-oriented programming language that may be used to create a wide range of software. It has strong integration support for various languages and technologies, as well as huge standard libraries and can be learnt in a matter of days. Many Python programmers claim that the language has increased their productivity and that it pushes them to write better, more maintainable code.

B.Visual Studio Code

Microsoft's Visual Studio Code is a source-code editor for Windows, Linux, and macOS. Debugging, syntax highlighting, intelligent code completion, snippets, code refactoring, and embedded Git are among the features

C.Robo3t

Robo 3T is a cross-platform graphical user interface solution for managing MongoDB workloads that is lightweight, open-source, and shell focused. Robo 3T allows user to construct databases, collections, users, and documents, as well as run one-time queries with auto-completion and display the results using a graphical user interface. It also keeps the track of data being edited

D.MONGODB

MongoDB is a cross-platform document-oriented database application that is open source. MongoDB is a NoSQL database application that works with JSON-like documents and optional schemas. MongoDB is a database that was created by MongoDB Inc. and is distributed under the Server Side Public License. It has a 500mb free to use storage and for more storage one has to buy a premium subscription. It is popular amongst developers of all kinds for developing scalable applications with evolving data schemas.

E. CSS

Cascading Style Sheets (CSS) is a language for describing the appearance of a document written in a markup language like HTML. Along with HTML and JavaScript, CSS is a key component of the World Wide Web. CSS isn't considered programming languages because they simply control the structure and appearance of the webpage you're creating. Like the other front-end languages, they don't have any instructions.

F.HTML

HTML, or Hyper Text Markup Language, is the standard markup language for texts that are intended to be viewed on a web browser. Technologies such as Cascading Style Sheets and scripting languages like JavaScript can help.HTML (Hyper Text Markup Language) is the most fundamental component of the Internet. It establishes the structure and meaning of web content. Other technologies are commonly used to describe a web page's appearance/presentation (CSS) or functionality (JS) in addition to HTML

G.FERNET:

We're starting to see a lot of software developers interested in cryptography, especially when it comes to testing programmes for vulnerabilities. So, when faced with RSA, AES, BCrypt, 3DES, DES, MD5, HMAC, private keys, and public keys, deciding which is the best route to go is quite tough. Fortunately, we stumbled upon fernet, a module that follows best practices. Fernet is a symmetric Q encrypted module that requires a key to process or read the data The keys are encoded using URL safe encoding. Fernet's authentication uses 128-bit AES and SHA256. Fernet provides a standardized token library that is relatively easy to integrate into a variety of applications. The auto keying feature also reduces the use of brute force attacks. AES offers top-notch encryption, and SHA-256 eliminates many of the issues that MD5 and SHA-1 cause (as the length of the hash values is too small). We get an output from CBC (Cipher Block Chaining) that is based on a random value (the IV value). We can also give authenticated access from both sides using HMAC.HMAC aids in the hashing of the generated key, resulting in a more secure key. Because fernet is a symmetric encryption technique, it creates only one key: the encryption key. The data decryption key is decrypted twice to recover the data. As a result, hybrid cryptography is available.

VI.RESULT AND DISCUSSION

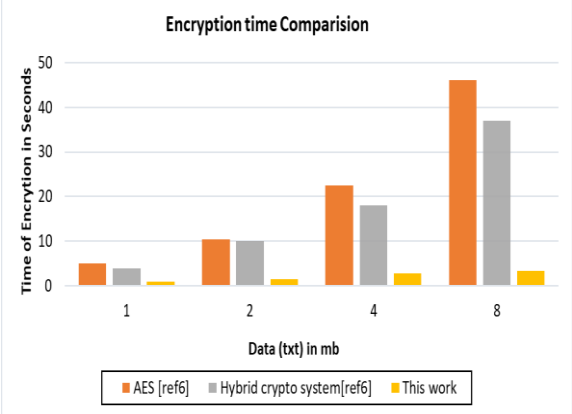

Fig 2: Encryption time comparision

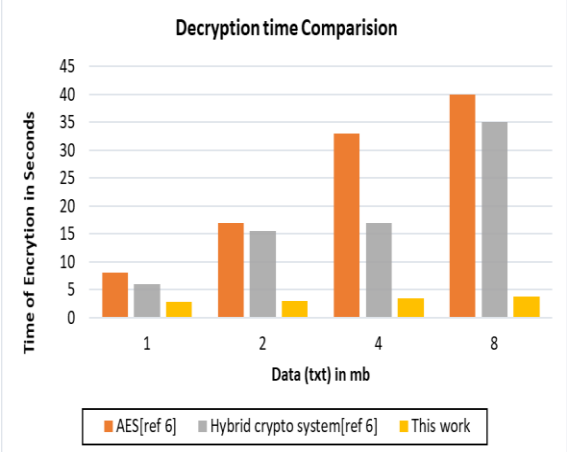

Fig 3: Decryption time comparision

This paper presents a highly efficient model for encrypting huge files in a short amount of time. Here we can see in fig 2 and fig 3, we have compared our proposed system with etal ref[6] Kartik Prajapati's research paper. Encryption time of Hybrid Cryptography using fernet significantly takes less time than other systems. While it takes lesser time to encrypt the file and decrypt the file it does not alter the security level of the proposed system. Since the proposed system is hybrid the security of the file is certain.

The cryptosystem uses combined keys (symmetric and asymmetric) cryptography that runs continuously in a hybrid algorithm. We can see that the proposed cryptosystem takes less time to encode files in comparison to others..

The methodology used in this is fernet, and it generates keys of size (128 -256bits) which are smaller in size than other RSA algorithm, which is (1024-4096 bit). Fernet can be used for larger amount of data in comparison to other algorithms such as the RSA algorithm.

VII. CONCLUSION

A hybrid technique of cryptography algorithms is used in the model. The upload of files are always done using one key and access to the file is done using a second key. In comparison to the present system, this approach raises data security to the highest level possible and takes less time to upload and download text files. The key is also safe as it is not easily predicted and decodable.

The fundamental obstacles of handling sensitive data have been met. If this system has a flaw, it is that it requires an active internet connection to connect to the server, despite the fact that it offers several benefits. The image file is completely secure, and it has been encrypted twice with Fernet.

This project can be expanded on the industrial/corporate level by adding paid subscription to users. So that the users can get premium service on the space or storage basis. In the future, this model could be used to improve the security of cloud services utilizing artificial intelligence techniques.

ACKNOWLEDGMENT

We would like to express our gratitude to Dr. Sanjay U. Bokade, our Principle, and Dr. Sanjay D. Deshmukh, our Head of Department, for providing us with all of the lab support and resources we needed for this research study. We'd also like to express our gratitude to our parents for their constant support and encouragement as the project progressed.

REFERENCES

[1] A. K. Shahade, V.S. Mahalle, "Enhancing the Data Security in Cloud by Implementing Hybrid (Rsa & Aes) Encryption Algorithm", IEEE, INPAC, pg 146-149, Oct 2014.

[2] Klaus Hofmann and S. Hesham, "High Throughput Architecture for the Advanced Encryption Standard Algorithm" IEEE, International Symposium on Design and Diagnostics of Electronic Circuits & Systems, pages 167- 170, April 2014.

[3] A. Chauhan and J. Gupta, "A novel technique of cloud security based on hybrid encryption by

Blowfish and MD5," 2017 4th International Conference on Signal Processing, Computing and Control (ISPCC), Solan, 2017, pp. 349-355. doi: 10.1109/ISPCC.2017.8269702.

[4] Anshika Negi, Mayank Singh, Sanjeev Kumar, "An Efficient Security Framework Design for Cloud Computing using Artificial Neural Networks" in International Journal of Computer Applications (0975 – 8887) Volume 129 – No.4, (2015).

[5] herief H. Murad and Kamel Hussein Rahouma, "Hybrid Cryptography for Cloud Security: Methodologies and Designs"

[6] International Journal of Computer Applications (0975 – 8887) Volume 175 – No.18, September 2020 "Security of Fog Storage by using Hybrid Cryptography"

[7] Kun Liu, Long-jiang Dong "Research on Cloud Data Storage Technology and Its Architecture Implementation" 2012 International Workshop on Information and Electronics Engineering (IWIEE).

[8] M.Lakshmi Neelima et al, International Journal of Computer Science and Mobile Computing, Vol.3 Issue.5, May- 2014, pg. 966-971 "A STUDY ON CLOUD STORAGE". International Journal of Computer Science and Mobile Computing.

[9] Isaac Odun-Ayo, Olasupo Ajayi, Boladele Akanle, Ravin Ahuja " An Overview of Data Storage in Cloud Computing". 2017 International Conference on Next Generation Computing and Information Systems (ICNGCIS).

[10] Shalini Bhaskar Bajaj, Aman Jatain, Sarika Chaudhary, Pooja Nagpal "Cloud Storage Architecture: Issues, Challenges and Opportunities". International Journal of Innovative Research in Computer Science & Technology (IJIRCST) ISSN: 2347-5552, Volume-9, Issue-3, May 2021 https://doi.org /10.21276/ijircst.2021.9.3.12 Article ID IRP1164, Pages 70-73 www.ijircst.org.

[11] Nikhita Reddy Gade, Ugander G J Reddy "A Study of Cyber Security Challenges And Its Emerging Trends On Latest Technologies".

[12] International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 Published by, www.ijert.org VIMPACT - 2017 Conference Proceedings "A Review Paper on Cyber Security" Saloni Khurana.

[13] 2016 Fifth International Conference on Future Generation Communication Technologies (FGCT), IEEE, "Data Security in Cloud Computing" Ahmed Albugmi, Madini O. Alassafi ,Robert Walters, Gary Wills.

[14] Xiaowei Yan, Xiaosong Zhang, Ting Chen, Hongtian Zhao "The Research and Design of Cloud Computing Security Framework"

[15] Elisa Bertino "Data Security and Privacy: Concepts, Approaches, and Research Directions" 2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC).