IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

SECURE FILE STORAGE USING HYBRID CRYPTOGRAPHY

Vaishnavee.S[1], Fathima.G[2], Dr. S. Latha[3]

[1]Centre for Cyber Forensics and Information Security, University of Madras, India
[2] Guest Faculty, Centre for Cyber Forensics and Information Security, University of Madras, India
[3]Director i/c[c,] Centre for Cyber Forensics and Information Security, University of Madras, India

ABSTRACT

Secure file storage is essential to protecting sensitive data from unauthorized access or tampering. Hybrid cryptography is a widely used technique combining the benefits of symmetric and asymmetric encryption to provide robust security. This study has been undertaken in order to provide an efficient way to secure confidential files and sensitive information. In general, either a strong encryption algorithm is used to protect files or either authentication is done, or digital signatures are used. This provides only midlevelsecurity to the files. In the proposed system, all these security implications are provided alongwith access controls. Moreover, three strong symmetric encryption algorithms are used along withan asymmetric algorithm that secures the key. The Key Derivation Function generates the key using the password and hash. To add an additional layer of protection to the files, the cipher texts are digitally signed using a Digital Signature Algorithm. In this proposed research, the contents of the file are divided into 3 segments. Each segment is encrypted using a different symmetric algorithm. The first segment is encrypted using Advanced Encryption Standard (AES) Algorithm, the second segment is encrypted using Fernet Algorithm and the third segment is encrypted usingChaCha20 Algorithm. The Key Derivation function used is Argon2. This adds an additional layer of security as it provides better protection against brute-forcing attacks. The keys are digitally signed using ECDSA (Elliptic Curve Digital Signature Algorithm) and the keys and signature along with the cipher texts are stored in a password-protected zip file with access controls set in such a way that only the user can read/write the file. The password is provided by the user and the user must use it to recover his/her files. This file is uploaded/stored in the database with access controls. This method provides all kinds of security measures such as confidentiality, integrity, authentication, authorization, access controls, and non-repudiation.

Keywords – Secure Storage, AES algorithm, Fernet Algorithm, ChaCha20 Algorithm, DigitalSignature, ECDSA Algorithm, Key Derivation Function, Argon2.

INTRODUCTION

The significance of secure file storage using hybrid cryptography is that it provides a high level of security for sensitive data, such as personal or financial information. With the increasing amount of data breaches and cyberattacks, it is crucial to have a secure method of storing and sharing information [1]. This research addresses the need for confidentiality, integrity, availability, authentication, authorization, access controls, and non-repudiation. These are essential aspects of information security that ensure that the data is protected from unauthorized access, modification, or deletion. By using a hybrid cryptography approach, it provides an extra layer of security by combining the strengths of symmetric and asymmetric encryption algorithms [2]. The use of hashing algorithms and password-based key derivation functions further enhances the security of the approach. This makes it accessible to a wide range of users, including individuals, small businesses, and organizations [3].

LITERATURE REVIEW

Security is never absolute. No matter how secure a system is, there is always a possibility of someone finding a way to break into it. While this project uses various security measures, it is not completely immune to attacks[4]. This may be a limitation for users who are not familiar with cryptography. The hybrid cryptography approach can be computationally intensive, This could lead to slower file upload and download times, which may not be ideal for users who require fast access to their files.

D. P. Timothy and A. K. Santra [2017], proposed the need for the current investigation is to protect data from unauthorized access or hackers in cloud at the time of data transmission by encrypting the user data. Cloud computing constitutes several security issues including data access control, identity management, auditing, integrity control and risk management therefore, this hybrid cryptosystem is designed and comprises of both symmetric and asymmetric cryptography algorithm in which Blowfish symmetric algorithm deals with data confidentiality whereas, RSA asymmetric algorithm deals with an authentication. This method also includes the Secure Hash Algorithm -2 for data integrity. In their study they concluded that the method provides high security on data transmission over the internet and proper network access on demand to a shared tank of constructive computing resources, mainly net, server, and storage application [5].

M. Kaur, A. B. Kaimal and et al, [2023] proposed a multilevel cryptography-based safety solution for cloud computing is designed. The paradigm is a combination of asymmetric & symmetric key cryptography techniques. The RSA and Data Encryption Standard (DES) are used in their methodology to provide several levels of encoding and decoding at the sender & recipient side, increasing the safety of cloud storage. This paradigm increases the data security to the highest possible level as compared to the current system [6].

B. S. Rawal and S. S. Vivek discussed that most of the security tools have a finite rate of failure, and intrusion comes with more complex and sophisticated techniques; the security failure rates are skyrocketing. Once we upload our data into the cloud, we lose control of our data, which certainly brings new security risks toward integrity and confidentiality of our data. In their work, they discuss a secure file sharing mechanism for the cloud with the disintegration protocol (DIP) and also introduces new contribution of seamless file sharing technique among different clouds without sharing an encryption key[7].

Aayushi Priya and etal [2018]discussed about theAnonyControl to address the information protection, as well as the client character security in existing access control plans. AnonyControl decentralizes the central authority to restrain the character spillage and accordingly accomplishes semianonymity. Furthermore, it likewise sums up the document get to control to the benefit control, by which advantages of all operations on the cloud information managed in a fine-grained way. Along these lines, display the AnonyControl-F, which ultimately keeps the character spillage and accomplish the full secrecy. Our security assessment demonstrates that both AnonyControl and AnonyControl-F are secure under the decisional bilinear Diffie-Hellman presumption, and our execution assessment shows the attainability of our plans [8].

METHODS AND MATERIAL USED

Secure file storage using hybrid cryptography combines both symmetric and asymmetric techniques to achieve high security. In the proposed system, after user authentication, the file uploaded by the user is divided into 3 segments and is stored in 3 separate files. The symmetricalgorithms are chosen in such a way that they provide high security and are widely used. The first segment is encrypted using Advanced Encryption Standard (AES) Algorithm. AES is a reliable algorithm that is widely used. It is known for its security and speed in the encryption and decryption process. The second segment is encrypted using Fernet Algorithm. Fernet guarantees that a message encrypted using it cannot be manipulated or read without thekey . The third segment is encrypted using ChaCha20 Algorithm which is a stream cipher. ChaCha20-Poly1305 is an Authenticated Encryption with Additional Data (AEAD) algorithm, that combines the ChaCha20 stream cipher with the Poly1305 Message Authentication Code [9]. The key for each algorithm is generated using a secure technique to add an additionallayer of security, which is the Argon2 Key Derivation Function (KDF). A Key Derivation Function is used for deriving strong keys from passwords, shared secrets, or other keys . The Argon2 KDF is known for its efficient protection against password-cracking attacks, side- channel attacks, and GPU-cracking attacks. The 3 keys generated are stored in a list. The key is stored in a list that is digitally signed using ECDSA (Elliptic Curve Digital Signature Algorithm). The ECDSA is a Digital Signature Algorithm (DSA) that uses keys derived from elliptic curve cryptography (ECC). It is a particularly efficient equation based on Public Key Cryptography (PKC) [10]. The list of cipher texts, the keys, and the signature are stored in a separate file and are together stored in a password-protected zip file. The zip file is stored in the MySQL Database with access controls. To retrieve the file, the user must authenticate againand enter the password to open the password-protected zip file [11]. The user clicks a button ‘Retrieve File’. On clicking the button, the signature is verified and the file is decrypted. The file is retrieved successfully.

The methodology used in the Research includes several steps that are necessary to achieve steps as shown in the Figure 1.1. The methodology includes:

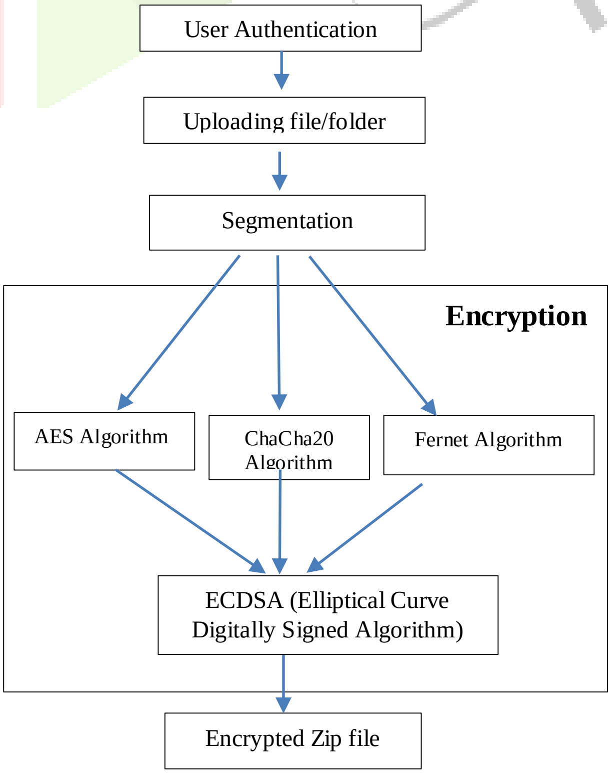

Figure 1.1 Hybrid encryption architecture

User Authentication: User authentication is the process of verifying the identity of a user attempting to access a system or application. This is typically done by requiring the user to provide some form of credentials, such as a username and password, that are then validated against a database of authorized users. It is an important security measure that helps protect against unauthorized access, data breaches, and other forms of cyber-attacks.

Uploading file/folder: In the context of web development, file uploading is often used to allow users to submit files, such as images or documents, to a web application. The uploaded files are typically stored on a server or in a database and can be accessed and processed by the application. When uploading a file, it is important to ensure that the file is valid and safe. **Segmentation:** The purpose of dividing a file into segments is to split a large file into smaller parts, which can be easier to manage or process. This can be useful in a variety of situations, such as when transferring or uploading large files, or when processing large amounts of data. By dividing a file into segments, you can also process each segment independently, which can make it easier to parallelize tasks and improve performance.

Encryption: Encryption is the process of converting data into a secret code or cipher so that it cannot be easily understood or accessed by unauthorized parties.in this proposed system encryoption is done by Fernet, Chacha20 and AES Algorithm. Encryption is commonly used to protect sensitive data, such as passwords, credit card numbers, and other personal or confidential information.

Key derivation function: Argon2 is a Key Derivation Function. It is used to hash passwords and provides better protection against password cracking. Argon2 is a cryptographic hashing algorithm that takes the password as the input and gives the hash of the specified length as the output. Argon2 comes in three variants - Argon2d which is fast and is less suitable for hashing secrets and is resistant to GPU attacks, Argon2i which is preferred for password hashing and password-based key derivation and is resistant to side-channel attacks, and Argon2id is a hybrid of Argon2d and Argon2i [12].

Storing in password-protected zip file: A password-protected zip file is a compressed file that has been encrypted with a password to prevent unauthorized access. This means that the contents of the zip file are only accessible to those who know the correct password.

Decryption: Decryption is the process of converting encrypted data back into its original, unencrypted form. It involves using a secret key or password to reverse the encryption process and make the data readable again. Decryption is often used in conjunction with encryption to secure data and protect it from unauthorized access. For example, when you send an encrypted email, the recipient uses their private key to decrypt the message and read its contents.

CONCLUSION

The aim of the proposed system is to securely upload, store, and retrieve files in order to maintain their integrity. The files undergo a few processes to store them securely. The processincludes encryption using 3 strong symmetric algorithms: AES, Fernet, and ChaCha20, the keyis encrypted and digitally signed using an asymmetric algorithm, ECDSA and finally all theseare stored together in a password-protected zip file. The zip file is stored in the MySQL Database. A system generally requires speed and security. This proposed system is highly secure because it uses 3 algorithms, key encryption and digital signatures, and access controls.3 algorithms might seem to be a complicated and slow process. So, to enhance the speed, the multithreading concept is used to simultaneously perform the three 3 algorithms which reduce time and increases speed. This proposed system provides confidentiality, integrity, authentication, authorization, access controls, high security, low delay, and non-repudiation

REFERENCES

[1] https://cryptography.io/en/latest/fernet/#:~:text=Fernet%20guarantees%20that%20a%20message,implementing%20key%20rotation%20via%20MultiFernet%20.

[2] https://en.wikipedia.org/wiki/ChaCha20-Poly1305

[3] https://www.comparitech.com/blog/information-security/key-derivation-function-kdf/

[5] . D. P. Timothy and A. K. Santra, "A hybrid cryptography algorithm for cloud computing security," *2017 International conference on Microelectronic Devices, Circuits and Systems (ICMDCS)*, Vellore, India, 2017, pp. 1-5, doi: 10.1109/ICMDCS.2017.8211728

[6] M. Kaur, A. B. Kaimal, J. K. Sandhu and R. Sahu, "Cloud Data Security using Hybrid Algorithm," *2023 3rd International Conference on Smart Data Intelligence (ICSMDI)*, Trichy, India, 2023, pp. 223-228, doi: 10.1109/ICSMDI57622.2023.00049.

[7] B. S. Rawal and S. S. Vivek, "Secure Cloud Storage and File Sharing," *2017 IEEE International Conference on Smart Cloud (SmartCloud)*, New York, NY, USA, 2017, pp. 78-83, doi: 10.1109/SmartCloud.2017.19.

[8] Priya, A., & Tiwari, R. (2018). “A survey: attribute based encryption for secure cloud”, IJOSTHE ISSN: 2349-0772 | Volume 5 Issue 3 June 2018

[9] https://www.comparitech.com/blog/information-security/what-is-fernet/

[10]https://cryptography.io/en/latest/fernet/

[11]https://pythoninformer.com/python-libraries/cryptography/fernet/

[12] https://argon2.online/