IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, March 2021
Impact Factor: 4.819

Message Passing Over Cloud Using Cascade Ciphering With Randomized Algorithm

Sankaramani S.S, Sulthan Abdul Kadar H, Prason Moses M, Sivaram S and Velusamy. A
Hindusthan Institute of Technology, Coimbatore, Tamilnadu

Abstract: *To solve the problem of poor security and performance caused by traditional encryption algorithm in the cloud data storage, we propose a cascade ciphering with randomized algorithm. The multiple encryption is a process to encrypt the data multiple times using the same algorithm or different algorithms, to provide multilayer and multilevel security over unreliable wireless network during communication. The encryption algorithms are AES, MD5, SHA 129, SHA 256, Whirlpool and Blowfish.*

I. INTRODUCTION

"The cloud" refers to servers that are accessed over the internet and the software and databases that run on those servers. Cloud storage providers offer cloud encryption services to encrypt data before it is transferred to the cloud for storage during data transaction. Encryption is regarded as one of the most effective approaches to data security.

1.1 Purpose

Organizations and developers are presented with many new choices in their use of cryptographic mechanisms. Inappropriate choices may result in an illusion of security but little or no real security for the protocol or application. This Recommendation (i.e., SP 800-57) provides background information and establishes frameworks to support appropriate decisions when selecting and using cryptographic mechanisms.

1.2 Audience

The audiences for this Recommendation for Key Management include system or application owners and managers, cryptographic module developers, protocol developers, and system administrators. The Recommendation is provided in three parts, which have been tailored to specific audiences.

1.3 Scope

This Recommendation encompasses cryptographic algorithms, infrastructures, protocols, implementations, applications, and the management thereof. All cryptographic algorithms currently approved by NIST for the protection of unclassified but sensitive information are within the scope of the Recommendation.

Purpose of FIPS and NIST Recommendations (NIST Standards) Federal Information Processing Standards (FIPS) and NIST Recommendations, collectively referred to as "NIST standards," are valuable because:

1. They establish an acceptable minimal level of security for government systems. Systems that implement these NIST standards offer a consistent level of security that is approved for the protection of sensitive, unclassified government information.
2. They often establish some level of interoperability between different systems that implement the NIST standards. For example, two products that both implement the Advanced Encryption Standard (AES) 10 cryptographic algorithm have the potential to interoperate, provided that the other functions of the product are compatible.
3. They often provide for scalability because the U.S. government requires products and techniques that can be effectively applied in large numbers. Authentication and source authentication. These services may be fulfilled using several different algorithms, and in many cases, the same algorithm may be used to provide multiple services. Cryptographic Hash Functions:

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, March 2021
Impact Factor: 4.819

II. CRYPTOGRAPHIC ALGORITHMS

FIPS-approved or NIST-recommended cryptographic algorithms shall be used whenever cryptographic services are required. These approved algorithms have undergone an intensive security analysis prior to their approval and continue to be examined to ensure that the algorithms provide adequate security. Most cryptographic algorithms require cryptographic keys and other keying material. In some cases, an algorithm may be strengthened by increasing the key size used. This Recommendation advises the users of cryptographic mechanisms on the appropriate choices of algorithms and key sizes.

This section describes the approved cryptographic algorithms that provide security services, such as confidentiality, identity authentication, integrity Cryptographic hash functions do not require keys for their basic operation. A cryptographic hash function (also called a hash algorithm) is a cryptographic primitive that produces a condensed representation of its input (e.g., a message or other data). Common names for the output of a hash function include hash value, hash, message digest, and digital fingerprint. The maximum numberof input and output bits is determined bythe design of the hash function.

Many algorithms and schemes that provide a security service use a hash function as a component of the algorithm (i.e., a hash function is used as a building block). For example:

1. To provide source and integrity authentication services, the hash function is used with a key to generate a message authentication code (MAC)
2. To compress messages for digital signature generation and verification
3. To derive keys from pre-shared keys
4. To derive keys using asymmetrickey-establishment algorithms
5. To generate random numbers

2.1 Symmetric-Key Algorithms

Symmetric-key algorithms (sometimes known as secret-key algorithms) transform data in a way that is fundamentally difficult to undo without knowledge of a secret key. The key is “symmetric” because the same key is used for a cryptographic operation and itsinverse (e.g., for both encryption and decryption). Symmetric keys are often known by more than one entity; however, the key shall be generated using a random process and shall not be disclosed to entities that are not authorized access to the data protected by that algorithm and key.

Symmetric-key Algorithms are Used for Example to

1. Provide data confidentiality – the samekey is used to encrypt and decrypt data.
2. Provide source and integrity authentication services in the form of message authentication codes (MACs) −the same key is used to generate the MAC and to validate it (MACs normally employ either a symmetric-key algorithmor a cryptographic hash function their cryptographic primitive).
3. Derive keying material from a pre-shared key using a key-derivationmethod.

2.2 Asymmetric-Key Algorithms

Asymmetric-key algorithms, commonly known as public-key algorithms, use two related keys (i.e., a key pair) to perform their functions: a public key and a private key. The public key may be known by anyone; the private key should be under the sole control of the entity that “owns” the key pair. Even though the public and private keys of a key pair are related, knowledge of thepublic key cannot be used to determine the private key. With an asymmetric-key algorithm, one of the keys of the key pair is used to applycryptographic protection, and the other key is used to remove or verify that protection. The key to use depends on the algorithm used and the service to beprovided.

1. Provide source, identity, and integrity authentication services in the form of digitalsignatures, and
2. Establish cryptographic keying material usingkey-agreement and key-transport algorithms.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, March 2021
Impact Factor: 4.819

III. CRYPTOGRAPHIC KEYS

Several different types of keys are defined. The keys are identified accordingto their classification as public, private, orsymmetric (i.e., secret) keys, and their use is indicated. For public and private key-agreement keys, their status as static or ephemeral keys is also specified for therequired protections for each key type.

3.1 Private Signature Key

Private signature keys are the private keys of asymmetric-key (public-key) key pairs that are used by public-key algorithms to generate digital signatures intended for long-term use. When properly handled, private signature keys can be used to provide source authentication and integrity authentication as well as support the nonrepudiation of messages, documents, or stored data.

3.2 Public Signature-Verification Key

A public signature-verification key is the public key of an asymmetric-key (public-key) key pair that is used by a public-key algorithm to verify digital signatures that are intended to provide source authentication and integrity authentication as well as support the non-repudiation of messages, documents, or stored data.

3.3 Symmetric Authentication Key

Symmetric authentication keys are used with symmetric key algorithms to provideidentity authentication and integrity authentication of communication sessions, messages, documents, or stored data. Note that for authenticate decryption modes of operation for a symmetric-key algorithm, a single key is used for both authentication and encryption.

3.4 Private Authentication Key

A private authentication key is the private key of an asymmetric-key (public-key) key pair that is used with a public-key algorithm to provide assurance of the identity of an entity (i.e., identity authentication) when establishing an authenticated communication session or authorization to perform some action.

3.5 Symmetric Random Number Generation Keys

These keys are used to generate randomnumbers or random bits.

3.6 Private Authorization Key

A private authorization key is the private key of an asymmetric-key (public-key) keypair that is used to prove the owner's right to privileges (e.g., using a digital signature).

IV. LITERATURE SURVEY

4.1 Multilevel Encryption Techniquein Cloud Security

Cloud privacy is a one of the tentative issue in cloud computing. As the entire cloud user do not have same demands regarding cloud privacy. Some of the clients are satisfied with current policy where as others are quite concerned about the corresponding privacy. As per the fundamental cloud architecture it is generally deployed via three core service models namely software as a service, platform as a service and infrastructure as a service. Particularly our technique shows that only authorized user can able to access the cloud data. Our algorithm isfast and safe in both direction such as upload and download of a file. As decryption technique is multilevel so if some data is lost then it is very difficult to decrypt the data.

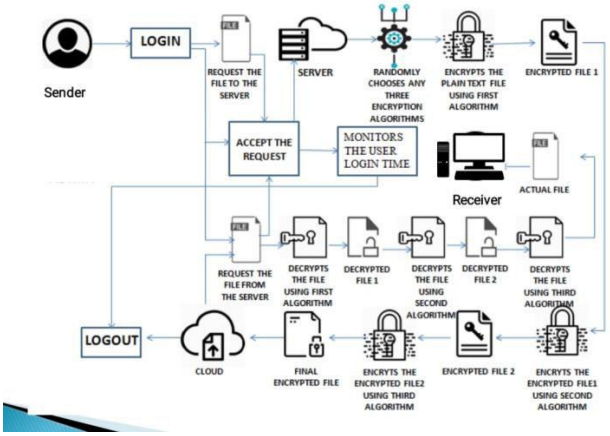
4.2 Secure File Storage in CloudComputing Using Hybrid Cryptography Algorithm

Cryptography and steganography techniques are more popular now a day's for data security. Use of a single algorithm is not effective for high level security to data in cloud computing. In this paper we have introduced new security mechanism using symmetric key cryptography algorithm and steganography. In this proposed system AES,

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, March 2021
Impact Factor: 4.819

blowfish, RC6 and BRA algorithms are used to provide block wise security to data. All algorithm key size is 128 bit.LSB steganograohy technique is introduced for key information security. Key information contains which part of file is encrypted using by which algorithm and key. File is splitted into eight parts. Each and every part of file is encrypted using different algorithm. All parts of file are encrypted simultaneously with the help of multithreading technique. Data encryption keys are inserted into cover image using LSB technique. Stego image is send to valid receiver using email.

ARCHITECTURE DIAGRAM



4.3 Encryption and Decryption Process of Cloud Storage

According to the hybrid encryption efficiency and security of the symmetric encryption AES algorithm and the asymmetric encryption ECC algorithm, symmetric encryption with high efficiency is used for large data blocks, and asymmetric encryption with low efficiency is used for small data blocks. It improves the security of data encryption and makes up for the defects of universal performance of asymmetric encryption. Among them the encryption process implemented by the uploadagent plug-in:

- **Step 1:** the user selects the file M to be uploaded.
- **Step 2:** according to the requirements, select the appropriate encryption ratio parameter K to segment the file, in whichthe large file block is block A and the small file block is block B.
- **Step 3:** use AES algorithm to encrypt datablock A, and use ECC public key to encrypt data block B and AES key.
- **Step 4:** merge all encrypted data obtained in step 3 to form the final ciphertext C.

After user login, user home page is opened user sends a file to someone. Thecloud contains the encryption algorithm; it inputs the file from the user and chooses any three random algorithms to encrypt the file. First it will encrypt the file using first algorithm then second and third and send it as a single encrypted fileto the receiver. The encrypted file stored in cloud is used for the backed up and archived data, both in transit and on storage media. The encryption process implemented by the downloadagent plug-in:

- **Step 1:** obtain the cipher text file C to bedecrypted.
- **Step 2:** according to the combination method of upload agent plug-in step 4, the cipher text file C is divided to obtainthe encryption part of data block A, andthe encryption part of data block B and AES key.
- **Step 3:** first use ECC private key to decrypt the data block B and AES key, andthen use the obtained AES key to decrypt the data block A.
- **Step 4:** reorganize the decrypted dataobtained in step 3 to form the final Download File M.

The entire text file transferred by the sender are encrypted by the system and stored in the cloud. The receiver sends a request to the admin to view the transferred file, the admin accepts the request from the receiver. Receiver enters the

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, March 2021
Impact Factor: 4.819

secret key to decrypt the file. Server checks whether the entered key matches with the encryption key, if it matches the encrypted file which is send in the cloud will get decrypted and will besent to the receiver as the original pain text. The sender can transfer as many as file and that can be decrypted and sent tothe receiver as the original plain text. If the entered key doesn't matches with theencrypted key, the receiver will not be allowed to view the requested file andhas to re enter the key to process the request.

V. CONCLUSION

The security problems of traditional cloud storage security encryption, the paper proposes a hybrid encryption algorithm based on AESand ECC. This method can meet the actual requirements of cloud storage encryption, because it can ensure the transmission security of symmetric encryption.

REFERENCES

[1]. NIST Special Publications 800-131A, Transitions: Recommendations for transitioning the use of cryptographic algorithms and keylengths, National Institute of Standards and Technology (NIST), November 2015,revision 1.

[2]. NIST Special Publications 800-57 Part 1,Recommendation for key management, National Institute of Standard and Technology (NIST),January 2016,revision 4,

[3]. ISO/IEC JTC 1/SC 27 N13432,ISO/IEC JTC 1/SC 27 Standing Document No.12 (SD12) on the Assessment of Cryptographic Techniques and Key lengths,4th edition, International Organization for Standardization, Geneve, Switzerland, May 2014.

[4]. ISO/IEC JTC 1/SC 27 N14908.First edition of SC 27/WG 2 Standing Document 4-Analysis and status of cryptographic algorithms.

[5]. M. Hogan and A. Sokol. NIST Cloud Computing Standards Roadmap Version 2. NIST Cloud Computing Standards Roadmap Working Group, NIST Special Publications 500-291, NIST, Gaithersburg, MD, 2013, p.1-113.