International Journal of Computer Science and Information Security (IJCSIS),
Vol. 14, No. 4, April 2016

A Hybrid Hashing Security Algorithm for Data Storage on Cloud Computing

Noha MM. AbdElnapi
Computer science department
Nahda University
Beni Suef, Egypt

Fatma A. Omara
Computer science department
Cairo University
Cairo, Egypt

Nahla F.Omran
Mathematics department
South Valley University
Qena, Egypt

***Abstract*— In today's modern IT everything is possible on the web by cloud computing, it allows us to create, configure, use and customize the applications, services, and storage online. The Cloud Computing is a kind of Internet-based computing, where shared data, information and resources are provided with computers and other devices on-demand. The Cloud Computing offers several advantages to the organizations such as scalability, low cost, and flexibility. In spite of these advantages, there is a major problem of cloud computing, which is the security of cloud storage. There are a lot of mechanisms that is used to realize the security of data in the cloud storage. Cryptography is the most used mechanism. The science of designing ciphers, block ciphers, stream ciphers and hash functions is called cryptography. Cryptographic techniques in the cloud must enable security services such as authorization, availability, confidentiality, integrity, and non-repudiation. To ensure these services of security, we propose an effective mechanism with a significant feature of the data. This paper is to show how to improve the security of the Cloud storage using the implementation of a hybrid encryption algorithm and hash functions. It proposes the implementation of two algorithms, Rivest-Shamir-Adleman (RSA) and Advanced Encryption Standard (AES) with a secure hashing algorithm (SHA256) by using Netbeans IDE 8.0.2, JDK 1.7 tool and EyeOS2.5 as a cloud platform on ubuntu14.04.**

***Keywords*— Cloud Computing, Security, Advanced Encryption Standard (AES), Rivest-Shamir-Adleman (RSA), Hybrid Algorithm, Hash functions, Secure Hash Algorithm (SHA256), Encryption, Cryptography, availability, confidentiality, integrity, authorization, and non-repudiation.**

I. INTRODUCTION

Cloud computing is the concept of internet based technology, which offers a variety of remote services over the internet such as infrastructure, data storage, software, and hardware. Which mean that applying a broad set of policies, technologies, and controls to protect data, applications, and the associated infrastructure of Cloud Computing technology. The essential principles of the cloud computing are; on-demand computing resources, founding a pay-as-you-go business model for computing and information technology services that you will use, elastic scaling, and elimination of up-front capital and operational expenses. [1]. Security plays the most important role in the cloud and the major concern over the internet in order to serve all the services and benefits of it. Secrecy of the data over the network can be achieved by using cryptography technique which is the process of encryption and hash functions [2].

Converting plain text into a cipher text by using special key is a technique called encryption [3]. There are three common types of encryption algorithms are the implementation of symmetric, asymmetric, and hybrid algorithms that can be used to encrypt data in the cloud computing storage. In symmetric and asymmetric encryption schemes, the data that will be encrypted referred to as plaintext, using an encryption algorithm and generating decrypted text (ciphertext) [4]. A cryptographic hash function takes a message of arbitrary length and creates a message digest of fixed length. A hash function produces short and fixed length message digest, which is unique for each message [5, 6].

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

Scanned with CamScanner

Moreover, to enhance Security in the cloud data storage; a hash function with a hybrid encryption algorithm can be used. It is a technique that proposes a concept of the digital signature with the hybrid algorithm, for encrypting the data while it is being transferred over the network.

II. CRYPTOGRAPHY

The science of designing ciphers, block ciphers, stream ciphers and hash functions is called cryptography. Cryptography is critical for the security and integrity of the data that is stored in the cloud. The essential objective of using cryptography is to fulfill the following fundamental information security services:

A. Confidentiality

It aims to avoid unauthorized disclosure of the protected data. Since, various devices and applications can access cloud storage that may cause an increase in the number of access points, which accordingly adds to the threat of unauthorized disclosure [6]. Therefore, to maintain the confidentiality of the data stored in the cloud storage; some methods must be introduced such as encryption [7, 8].

B. Integrity

Integrity is a key component of cloud data storage security, which means that data will be protected against illegal modification and deletion [9]. It is a serious issue in the cloud environment so that authorization mechanisms are applied [10]. The authorization specifies the access rights for every authenticated user to block the unauthorized users. However, due to the increase in access points and system entities, it is essential to be ensured that only authorized entities are allowed to access the protected data [11]. The digital signature is a common method used for ensuring the data integrity on cloud environment [12].

C. Availability

It refers to data, software, but also storage being available to authorized users upon demand at cloud computing environment. Availability includes a cloud system's ability to carry on operations even when some authorities misbehave [13].

D. Authorization

It means to identify who can access information and other computing services. It begins with some specific procedures and administrative policies. The policies recommend what information and computing services can be accessed, by whom, and under what conditions [14].

E. Non-repudiation

It means the ability to ensure that a sender cannot deny the authenticity of his signature on a document or the sending of a message that he originated. In other words, a sender should not be able to falsely deny later that he sent a message [15].

Cryptography provides different stronger tools and techniques can be used to provide these security services. These techniques are encryption algorithms, digital signature, and hash functions

III. ENCRYPTION ALGORITHMS

A. Symmetric Algorithms

Symmetric key cryptography (private key); uses a common key for both encryption and decryption of data, as shown in figure 1. The most common symmetric key algorithms are: Data Encryption Standard (DES), Triple-DES, International Data Encryption Algorithm (IDEA), Rivest Cipher 4 (RC4), and Advanced Encryption Standard (AES) [16].

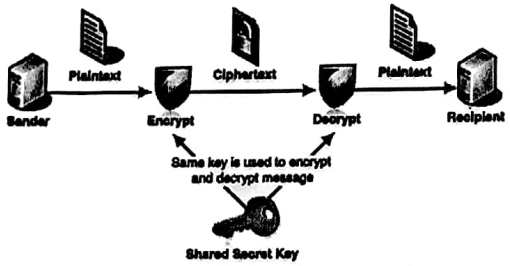

Fig. 1. Symmetric Private Key Cryptography [17].

B. Asymmetric Algorithms

Asymmetric-key cryptography is also known as Public-key cryptography, uses different two keys for encryption and decryption, as shown in figure 2. There are different types of asymmetric algorithms (public key algorithms) such as: RSA, Diffie-Hellman, ElGamal, and so on [18].

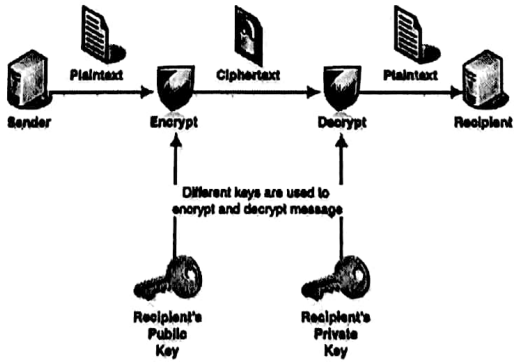

Fig. 2. Symmetric Private Key Cryptography [19].

C. Hybrid Algorithms

Hybrid encryption is a type of encryption that combines two or more encryption algorithms. In other words, it is the process of using either the same or a

Crypto splitting
- Data

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

Scanned with CamScanner

different algorithm for encrypting an already encrypted message one or more times. Encryption and decryption provide an easy possibility to use multiple encryptions. Top reasons to use multiple encryptions for most information security and to prevent Brute Force attacks; you can encrypt the same text or file multiple times. Multiple encryptions provide good protection from plaintext attacks, making ciphering stronger [20]. A good example of hybrid encryption/decryption algorithm is that consists of symmetric algorithm such as (AES) and asymmetric algorithm such as (RSA).

IV. LITERATURE REVIEW

A lot of studies and researches have been done to enhance the security of cloud computing storage and environment using encryption and other techniques. The researchers have found the following studies and literature as relevant to the security of cloud computing being proposed.

Vanishreeprasad. S and Mrs. K N Pushpalatha (2015) have improved the data security by proposing an architecture that integrates the cryptographic algorithms, Advanced Encryption Standard (AES) algorithm and the Hash function, SHA-2 [21]. Bernd Gastermanna, Markus Stopper, Anja Kossik, and Branko Katalinic (2015) have proposed and implemented a secure cloud storage solution for small and medium-sized enterprises (SMEs) [22]. M. Meenakumari and G. Athisha (2014) have introduced to achieve data integrity and confidentiality during sending data in the cloud by using the technique of combining encryption algorithm (AES) with the hash function (MD5) [23]. B. Sowmya Sri (2013) has proposed a technique for sending data securely in a cloud storage system by using Erasure coding for encoding and RSA, AES algorithms for encryption [24]. Uma Somani, Kanika Lakhani, and Manish Mundra (2010) have Implemented Cloud Storage Methodology to assess Data in the cloud by the Implementation of digital signature with RSA algorithm in a secure manner [25]. Kamara et al. (2010) presented secure cloud storage by using encryption techniques. Using these techniques at first, the data will be indexed then by using symmetric algorithms (AES) with a unique key it will be encrypted. Then by using attribute-encryption scheme and searchable encryption, the unique key and index are encrypted [26].

A. Rivest-Shamir-Adleman (RSA)

The RSA is an algorithm used by modern computers to encrypt and decrypt data stored in the cloud storage. It is a type of an asymmetric cryptographic algorithm. RSA algorithm includes two keys a public key and a private key. The public key is distributed to all so will be known to everyone, it is used to encrypt messages. Messages encrypted with public key only decrypted with private key [27]. RSA can be used for digital signatures, key exchange, or encryption of small block data. The size of the key that is used by RSA algorithm is variable not fixed and also the size of the encryption block. RSA has been widely used for establishing a secure communications channel and for authentication and the identity of the service provider over insecure communication medium [34]. In proposed scheme RSA algorithm is used to find out the key pair for both mobile user and third party auditor. These keys are used to encrypt and decrypt the file [35]. The following procedures describe the encryption and decryption of RSA [28]:

- Choose random "large" prime integers p and q roughly are the same size, but not too close together.
- Choose a random encryption exponent e less than n that has no factors in common with either p -1 or q – 1.
- Calculate the product n=p q.
- Calculate $\Phi(n) = (p-1) * (q-1)$.
- Calculate d= e-1 (mod Φ (n)).
- The encryption function is E (m) = me mod n, for any message m.
- The decryption function is D (c) = cd mod n, where c is the ciphertext.
- The public key (published with all) is the pair of integers (n, e).
- The private key (kept secret) is the triple of integers (p, q, d).

B. Advanced Encryption Standard (AES)

AES is a symmetric encryption algorithm block cipher that uses cipher keys with lengths of 128, 192, and 256 bits to encrypt data [29]. To use this algorithm for encrypting data; this encryption process consists of 10 rounds for 128 bit keys. All rounds are same except the final round as shown in figure 3. There are four phases are formed each round except the final [30].

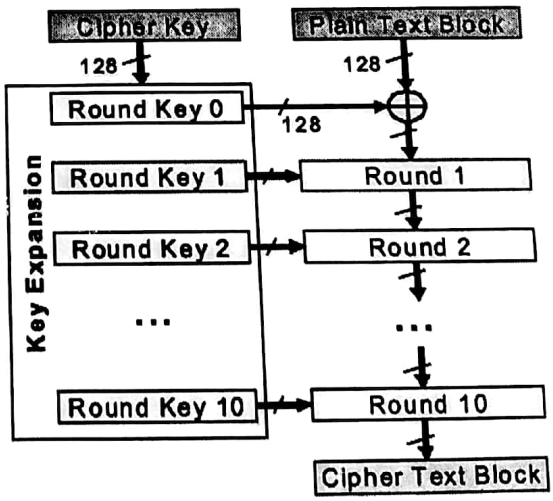

Fig. 3. Structure of AES Algorithm [31].

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

Scanned with CamScanner

- SubBytes
- ShiftRows
- MixColumns
- AddRoundKey

C. Secure Hash Algorithm (SHA256)

Hash functions are used in many applications for digital signatures, data integrity, password protection, message authentication, pseudo-random number generation, key derivation, and cryptography protocols [32]. The hash function algorithms compute a fixed length cryptography hash for a given data called the message digest.

V. METHODOLOGY

Such data storage provided by cloud service providers must ensure the main criteria of security which are: confidentiality, privacy, integrity and availability. Confidentiality states to keep data private. Privacy is meant as data leaves the boundaries of the holder. Integrity is a degree of confidence that refers to protect data in the cloud from being modified by unauthorized parties. Availability means that cloud user can able to use the system as predictable.

According to this paper, using combination cryptography encryption algorithms such as the hybrid algorithm (RSA and AES), and hash functions are one of the possible protection solutions for securing cloud storage. The proposed mechanism provides the three security primitives – confidentiality, integrity, and authentication.

The hybrid algorithm proposes/provides more security, scalability and speed which can be provided by a secure system. Performance improvement of AES and RSA has been achieved by implementing the hybrid algorithm. The hybrid encryption algorithm has the advantages of the strength of each form of encryption, which are: the safety of the asymmetric encryption and the speed of the symmetric encryption as well. In addition, using SHA256 to generate a signature with the hybrid algorithm; will achieve the integrity to improve the level of security in the cloud data storage.

The proposed mechanism is taken for implementing hybrid encryption Algorithm with hashing function by using Netbeans IDE 8.0.2, JDK 1.7 tool and EyeOS2.5 as a cloud platform on ubuntu14.04 as follow:

A. Generate the public key using a symmetric algorithm (AES)

This algorithm generates a public key used for encrypting data in the cloud as shown in Figure 4.

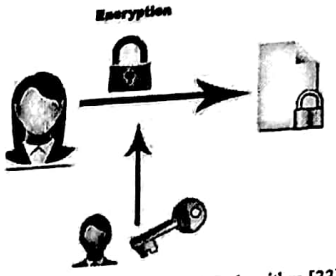

Fig. 4. Encrypt data using AES algorithm [33].

B. Using an asymmetric algorithm (RSA) to generate the secret key

The secret key is used for encrypting the public key as shown in figure 5.

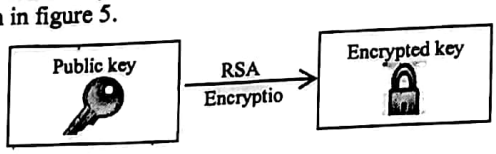

Fig. 5. Encrypt public key using the RSA algorithm.

C. Generating the signature

Secure Hash Algorithm (SHA256) will be used to generate the signature, which will be sent to the recipient with the encrypted file as shown in figure 6.

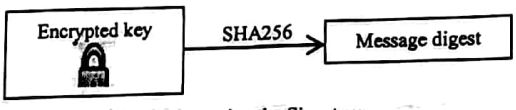

Fig.6. Generating the Signature

D. Signature verification and decryption

The following steps should be done by the recipient to verify the signature and decrypt the file

1) *Extracts the message digest of the key file information by using the same hash function.*

2) *Compute the message digest of the information that has been signed*

3) *If both message digests are matching, the signature is valid and then he can decrypt the file.*

VI. THE IMPLENTATION RESULTS

Using different data input sizes (34, 67, and 93) kb, the execution time of encryption for Hybrid and Hybrid-SHA256 algorithms are listed in Table I and presented in Figure 7 and the execution time of decryption is listed in Table II and illustrated Figure 8.

As shown in the experimental results listed in Table I & II, and illustrated in Figure7 and 8; it is found that the encryption and decryption phases using the proposed hybrid-SHA256 algorithm outperforms the Hybrid algorithm in security but it consumes more time than the other.

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

Scanned with CamScanner

The computational overhead time is the yardstick in measuring the performance of the mentioned method. The overhead time is defined as the ratio between hybrid-SHA256 to hybrid (AES, RSA) algorithm while measuring its performance with respect to hybrid (AES, RSA) algorithm.

The optimum result obtained from encryption phase is approximately 32% with respect to hybrid (AES, RSA) algorithm, and the optimum results obtained for decryption phase is nearly 33% with respect to hybrid (AES, RSA) algorithm.

The figures show a comparison of total time between hybrid algorithm and new proposed hybrid-SHA256. When comparing with hybrid, proposed model requires more time for encryption and decryption. Whereas proposed model is more secure encryption algorithm than hybrid, because the proposed model includes hashing and digital signature concept, which is more difficult for the intruder to find the plain text from the secret message. Moreover, proposed model provides the three security primitives -- confidentiality, integrity, and non-repudiation.

TABLE I. COMPARISON PERFORMANCE OF ENCRYPTION EXECUTION TIME OF HYBRID (AES, RSA) AND PROPOSED HYBRID-SHA256

Input data size (kb)	Time of execution (ms)		
	Hybrid (AES, RSA)	*Hybrid-SHA256*	*Computation overheads with respect to Hybrid (AES, RSA)*
34	365	579	58.63013699 %
67	493	726	47.26166329 %
93	600	801	31.5 %

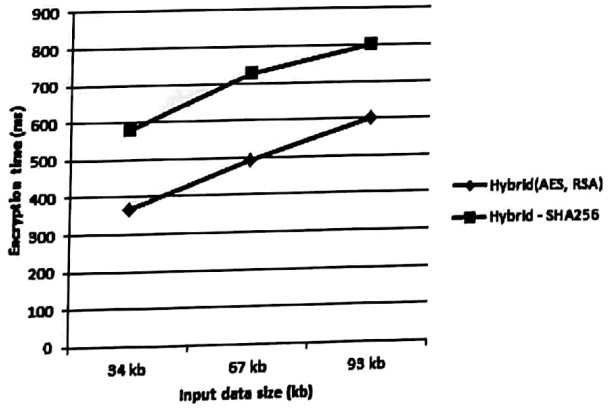

Fig. 7. Encryption execution time of hybrid (AES, RSA) and proposed hybrid-SHA256.

TABLE II. COMPARISON PERFORMANCE OF DECRYPTION EXECUTION TIME OF HYBRID AND PROPOSED HYBRID-SHA256

Input data size (kb)	Time of execution (ms)		
	Hybrid (AES, RSA)	*Hybrid-SHA256*	*Computation overheads with respect to Hybrid*
34	270	484	79.25925926 %
67	317	540	70.34700315 %
93	440	577	33.13636364 %

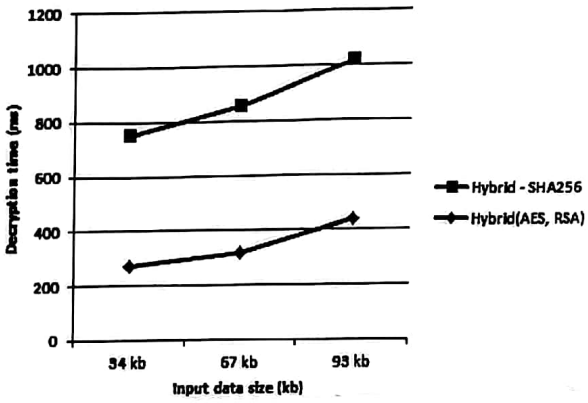

Fig. 8. Decryption execution time of hybrid (AES, RSA) and proposed hybrid-SHA256.

VII. CONCLUSION

Encryption algorithms; symmetric (AES), asymmetric (RSA) and hybrid algorithms are the most algorithms used to encrypt data in the cloud storage in order to make the data more secure from theft. A hash function is the best way to achieve the integrity of data in the cloud environment. Using a combination of cryptography encryption algorithms such as AES and RSA with SHA256 is one of secure and convenient technique for secure data via cloud storage services and achieve the confidentiality, integrity and non-repudiation. In the future, we will try to apply this method using GPU scheduling concepts to reduce the execution time for encryption and decryption phases.

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

Scanned with CamScanner