Abstract: The Network and data security plays a vital role on the network. Security of data is the main concern when data transmission takes place in the network. This paper describes the cloud security algorithm to secure the data at the data center. Blend technique is the advance techniques to secure the data. In this paper combination of AES, RSA and digital signature has been shown. Here private key generation is done using the two different algorithm AES and RSA where AES is symmetric and RSA is asymmetric cryptographic algorithm. After private key generation, that key will apply to digital signature which provide data authentication in the system. For verification we are using the 1024 bits public key of RSA algorithm. Also we have analyzed the performance of the same algorithm in basis of time because it takes the less time as compare to the existing hybrid algorithm.

Index Terms: Hybrid Technique, Cloud computing, Data Security, Key Generation

1. Introduction

The term “Cloud Computing” is latest research topic in IT sector. It is difficult to explain definition of cloud computing. As per the US National Institute of Standards and Technology(NIST)[3] cloud computing as follows:’ Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources(e.g, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction’. Cloud is an internet based environment which provides services on based of hardware, software.

Recently, the usage of cloud computing is increases rapidly due to easy accessibility. It allows people to do any things at any time and any were without buying and building IT infrastructure or to understand and underlying technology. The numbers of people can easily connected with cloud and shared their data over internet also some individuals and small businesses can shed the burden of basic good security practices such as breaking up critical data, malwares checking [33]. So they demands to cloud providers to deliver these services which needs full trust to service providers. At that time user need to manage and implement the data security of own data. Thus, the uses of services from third party and at the same time providing security to that data is biggest challenge in cloud computing.

As far as security is a concern, cryptography is one way to protect our data before outsourcing. Cryptography is process which convert original data into encrypted form using different cryptographic algorithm. Many symmetric and asymmetric cryptographic techniques are available like Caesar cipher, hill cipher, playfair cipher, DES, AES, and RSA. Etc. Hybrid cryptographic techniques (combination of symmetric and asymmetric encryption algorithm) increase more data security as compare to basic cryptographic algorithm. In this paper we have proposed hybrid cryptographic techniques using symmetric cipher AEs and asymmetric cipher RSA.

The basic idea behind hybrid techniques is improving efficiency of the existing algorithm. Many hybrid techniques are used to encrypt the data some of them are explain below

A. Dual RSA

A new public key cryptography algorithm, It is also called RSA-CRT, because it is used Chinese Remainder Theorem, CRT for its Decryption [2]. Dual-RSA has been developed for better performance in terms of computation costs and memory storage requirements. RSA takes one block at a time to encrypt and decrypt the data. But Dual RSA takes two blocks during encryption and decryption [12]. Encryption time of Dual RSA is more as compare to
decryption of two blocks. Thus Dual-RSA increases the performance as compare to RSA.

B. AES-RSA

Symmetric algorithms are faster to encrypt data as compare to asymmetric techniques. RSA (Asymmetric algorithm) takes more processing time to encrypt data due to longest key size. A new symmetric and asymmetric hybrid model has been developed to increase the level of security. In AES-RSA [5] hybrid techniques, AEs first generate 256-bit key. That 256-bit key are expanded to 1024-bit key and used in RSA as private key.

C. AES-ECC

This proposed model is combination of AES and EC (Elliptic curve) cryptography. Initial encryption of original data is done by AES algorithm when user sends their data. In this process dynamic security become an issue. To become data more secure, key which is generated by AES key generation will again encrypted by ECC. During above process one secure dynamic key is generated and send it to receiver to decrypt the data at receiver side.

2. Literature Review

Dimitrios et al. studies cloud security in depth in 2012 [6]. The authors proposed security solution by using trusted third party. The solution is based on Single-Sign-On (SSO) mechanisms and the lightweight directory access protocol (LDAP) [7] that is cryptography specifically in public key infrastructure. This is to make sure the security proposed solution consists of using cryptography to ensure confidentiality and integrity of involved data. However, it does not recognize which encryption algorithms used. But, this solution does not recognize the encryption algorithm to be used.

Cunsolo et al. in 2009 [8] came up with mechanism that protected data in distributed systems such as grid, cloud, autonomic, etc. In this paper author implement the techniques using symmetric and asymmetric algorithm. The limitation of this technique is that, the concept of sharing resources is contradicted because data access was done by owner only in the cloud environment.

Hashizume et al. [9], classified different cloud service models (SaaS, PaaS and IaaS) to solved security issues. The relation between cloud layers and the common threats shows the main vulnerabilities in cloud computing. Solution of splitting some available countermeasures is a technical implementation, which is not covered in this study.

Rahmani et al. [10], they implemented new technique Encryption as a Service (EaaS) as a solution based on XaaS concept for cryptography in cloud computing. The security risks and the inefficiency of cloud provider’s encryption and of client-side encryption can be prevented by this solution respectively. Moreover, this solution does not show a comparative study of cryptographic algorithms that can be integrated.

Performaces of cryptographic algorithms in cloud platform are evaluated using symmetric and asymmetric algorithms by the Mohammad et al. [11]. Different encryption techniques which are based on key size, the performance and the size of the output file are discussed in this paper. Distribution of encryption keys in a secure way is not proposed, but it proposed AES algorithm to encrypt data for more security.

In [6 paper, secure cloud architecture using cryptography was first proposed by this D. Zissis. For cloud storage they proposed to use cryptographic algorithms [10] [12]. But, they do not specify which algorithm is recommended to encrypt data and how to distribute cryptographic keys while maintaining adequacy with cloud characteristics. So these solutions remain incomplete.

In [1] Belguith proposed a new lightweight cryptographic algorithm which is combination of AES as public key algorithm to encrypt data and RSA as public private key algorithm to distribute keys. During conserving the rights of users to access data by a secured and authorized way this combination helps to benefit from the efficient security of asymmetric encryption and the rapid performance of symmetric encryption.

Various encryption algorithms hide a sequence of bits into random number generator function from other plain text message. It is an encryption algorithm which can be used for secure data over communication. As the name suggests its basic functions, which include insertion and hiding of plain text and the term hybrid is used as it has features of data hiding techniques. Ramaraj, Karthikeyan and Hemalatha (2009), proposed a encryption technique using hybrid method for security of online transaction. The combination of symmetric as well as asymmetric cryptographic methods is known as the hybrid encryption technique. This hybrid method provides all the main three cryptographic security properties these are, integrity, confidentiality and authentication. With the combination of symmetric cipher and public key which is RSA with some hash function a new design protocol is proposed. Encryption can be converted in some form that will make it difficult to read and make it more secure. In this method some substitution is done with each letter of plaintext replaced by fixed count of alphabets. As Julius Caesar used this method for communication with his generals so it was named after him. The final result can be a data
which now decrypted again from its encryption form. So we can say that Caesar cipher algorithm can be used to secure data using hybrid encryption techniques. Kuppuswamy and Chandrasekar’s (2011) describe one new algorithm which deals with linear block cipher. This concept is completely based on modular 37 which mean alphabets and numerals both can be used. Whereas previous algorithms based on only modular 26 (only alphabets).

Kuppuswamy and Al-Khalidi (2012) proposed that providing security in the network with the help of better encryption techniques by implementing them in simple and powerful method should be the research main goal. This Paper proposed a technique using modular 37 which selects any number randomly and after that its inverse is calculated by using some modular 37 technique and we should done that distribution of the symmetric key in a very secured way. We have to also calculate the effectiveness of the new algorithm by comparing it with other symmetric algorithm which already exists.

Sandeep K Sood [13] proposed that in information technology which has some major features like performance, accessibility, low cost etc used in cloud. Using this method we can increase the new capabilities by not investing much in stuffs like infrastructure, having new personnel and buying or licensing some new software from the market. This helps in providing huge amount of data storage and fast processing for its customers over the network. As it can send large data, database and applications to the center called Cloud. Large companies want to deploy cloud in their business as it provides huge variety of luxuries. Security of data can be the major challenge in the area of cloud that works as a challenge while implementing cloud. In this paper we have proposed a frame work which comprises of different techniques with different methods or procedures and all these help in securing our database at all the stages, starting from its master to cloud’s end user.

3. Proposed Work

The Proposed technique uses RSA and AES for the encryption and decryption. RSA uses two keys private key and public key through which a digital signature is also produced. On the other hand DES with the help of a key generation algorithm uses 256 bit keys and also apply a for loop it generates a 1024 bit private key. Now the private key of both RSA as well as DES together passes through XOR and we got output B.

Now for digital signature generation the output B which is our private key is converted from bit to byte and a message on which hash function is applied and then they both i.e. private key in byte and message with hash function are encrypted and finally digital signature is generated.

Third and final step is the verification phase in which hash code is verified by applying decryption on digital signature and in the end output is compared with the previous result i.e. C.
4. Result

The result for each can be seen from figure 4 to figure 11 and from all the results we can see private key is the combination of AES and RSA private key (1024 bit) and applied in digital generation scheme in the form of bytes. Figure 10 shows the Signature verification, if the signature will be same then signature will be verified and in other case signature will not be verified. With the combination of ASE, RSA and Digital Signature the function is nonlinear and more Avalanche effect is generated.

AES private key generation:

Figure 4. AES private key generation RSA private key & public key generation:

Figure 5. RSA private key & public key generation RSA & AES Private Key X-OR Operation:

Figure 6. RSA & AES Private Key X-OR Operation Digital Signature Private Key Generation:

Figure 7. Digital Signature Private Key Generation Digital Signature Public Key Generation:

Figure 8. Digital Signature Public Key Generation Digital Signature Message:
5. Conclusion

Cloud security is the latest stream in the field of computer technology. Many researchers are working on the upgradation of security technique and every day new algorithm is coming into the picture. Hybrid techniques are the best solution to het the more security. In hybrid technique the combination of the RSA and AES is the best example with digital signature. Private key is the combination of AES and RSA (1024 bit) and we are using RSA public key for the digital signature verification. Finally the result shows that hybrid technique takes less time and gives more security.

References


