Hybrid Cryptography

Prof. Deepashri Sonawale[1] Vinayak Kumbhar[2] Shubham Gherde[3] Bhupendra Kadu[4]

[1,2,3,4]Department of Information Technology

[1,2,3,4]MGM College of Engineering and Technology, Kamothe, Navi Mumbai, Maharahtra, India

Abstract— Cryptanalyst are expert in how to break the encryption techniques. We need to safe our programs and documents from cryptanalyst. Security of information means protecting data from unauthorized access in cloud environment. There are many techniques to achieve the security of information from unauthorized access. There are two cryptographic techniques used for data encryption which are Symmetric and Asymmetric techniques. There are some advantages and disadvantages of these block cipher algorithms. Rijndael had a potentially lower security margin and better performance than being arguably simpler than many encryption techniques. Symmetric key encryption algorithms are computationally fast compared to asymmetric encryption algorithms (like RSA). However, since the same secret key is used for symmetric encryption and decryption, we have the difficult problem of securely distributing that secret key. Conversely, asymmetric key infrastructure in PKI does not rely on distribution of any private key. However, the common asymmetric algorithms are too slow to be used for bulk encryption with current computation capability. While SHA is better collision resistant to various block cipher algorithms. Thus for better security performance, we propose a system which would incorporate the advantages of these algorithms namely SHA, AES-RIJNDAEL and RSA which will be a hybrid approach of encrypting data. SHA is adopted in this mechanism to verify the integrity of the message. Three major security principles such as authentication, confidentiality and integrity are achieved together using this scheme.

Keywords: Hybrid Cryptography, RSA, DES

I. INTRODUCTION

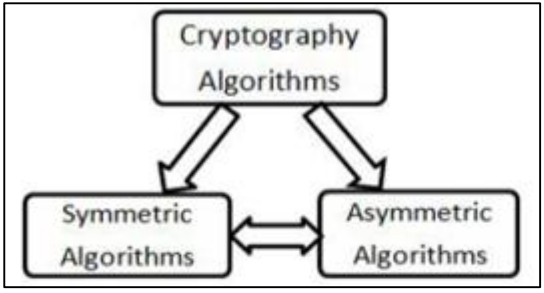
With advancements in computer technology and the widespread reach of the world-wide-web i.e. the Internet, people lives are changing rapidly. The liberalization, internationalization and personalization features of Internet have been attempting to bring revolutionary reform to government agencies, enterprises and institutions, at the same time help to boost the work efficiency and market response to improve their competitiveness by the use of Internet. But how to make the information system confidential and make sure that it is not leaked, even if they are stolen it is difficult to be identified, if they are identified after all the difficulty, they are extremely difficult to be modified. To prevent confidential information from being accessed, modified, and fabricated, to keep that protected has become a hot research topic in the IT industry.

In today's times Cloud computing has a significant impact on the IT industry. With growing popularity more and more organizations are making use of cloud services. Although cloud services have a widespread acceptance but the fear pertaining to security and privacy of these services still continue to be an open challenge. With rapid technological advancements these services could be easily accessed through smart phones thus allowing users to share pictures, video, documents and other important data across various platforms on a real time basis. However, a security breach in there Security has always been a concern in the domain of information technology. With Cloud services handling critical data which can be accessed from anywhere through the internet makes security a prominent concern. The pervasive nature of Cloud and its disbursal of data across various geographical locations amount to high security risks. While talking of Cloud Security there are many aspects which one needs to consider such as, trusted authentication, appropriate authorization, data security and privacy. These are some of the basic security goals which are extremely essential for every cloud provider to incorporate. Since security has been seen as an attribute for information technology, data encryption has been one of its key measures in ensuring data security protection.

II. HYBRID CRYPTOGRAPHY DESCRIPTION

The encryption technology (Cryptography) is the basic safety techniques used in current e-commerce and banking websites which are of extreme importance. Information encryption technology can not only meet the security requirements of confidentiality of information, but also avoid the leakage of the important information which are of high security especially in the security (defence) and hospital, banking sectors. Therefore, encryption technology is the base of authentication technology, as well as many other security technologies that are used today. Cryptography is an art of writing and reading the secret information. It uses mathematics in science to protect the information. It is a method of encrypting the original information into a form that is not easily interpreted by anyone. Original message can be revealed only after decrypting the encrypted message. Public and private keys are used for this purpose. Generally, the cryptographic systems can be classified into symmetric and asymmetric. In symmetric cryptography, same key is used for the encryption and decryption whereas in asymmetric cryptography separate keys are used for the encryption and decryption process. There are two types of cryptography algorithm that are given below:

– Symmetric key cryptography algorithm
– Asymmetric key cryptography algorithm



To increase the security level, this proposed scheme overcomes the limitation of "Basic encryption algorithm proposed till date. The proposed enhanced scheme includes

RIJNDAEL, RSA and SHA. RIJNDAEL (Variant of AES) strengthens the security of data stored in cloud. Reason behind for selecting RIJNDAEL rather other encryption algorithms is that, the key used for encryption and decryption is suspected to meet-in-middle attack. RSA is used to solve the key distribution problem and in addition to this, SHA to verify the integrity of the data. Use of SHA algorithm in combination of cryptographic algorithm provides strength in security of data stored in cloud.

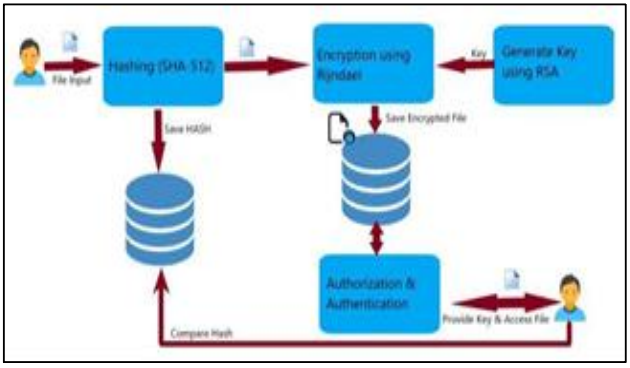
Due to small key size DES is insecure and has weaknesses. Triple DES which is an enhancement to DES, the original DES algorithm was applied thrice to increase the security. But it was found to be very slow. Blowfish algorithm runs faster than other symmetric algorithms. AES algorithm is the best encryption algorithm. The blowfish algorithm is fastest as compare to other algorithms but it has less security than the AES.

III. Need

The confidentiality, integrity and availability of resources are three major issues in this cloud computing security. IT infrastructure developers are eager to deal with gradually increasing secure algorithms in cloud networks. Still the area of cloud is open for data security in cloud network and seeking for more reliable, secure and less complex model. The security in the field of cloud being more improved when the attribute based encryption implemented in cloud data. Where the encryption of data with the key and that key is encrypted with adopted attribute, the whole combination of ciphertext, key and attribute combine to become master key. Hybrid Encryption plays an important role in mitigating risk related to the many threats listed in this guide. If sensitive information stored on your computer is encrypted, it will take a secret key to decode it. If sensitive information in route to others is encrypted, only someone that knows the secret key can read what it says. When you encrypt sensitive information and it ends up logged by others in the course of communicating online, encryption keeps those without the secret key from knowing the contents of the message. Most of the Defensive Technology articles will cover practical ways to apply encryption to particular communications (like email) or particular applications (like web browsers). Encryption is absolutely essential to maintaining information security. Moreover, modern computers are powerful enough that we can aim to make encryption of our communications and data routine, not just reserving encryption for special occasions or particularly sensitive information.

IV. The proposed system

To increase the security level this proposed scheme overcomes the limitation of "Hybrid encryption algorithm proposed by Wuling Ren. The proposed enhanced scheme includes Rijndael, RSA and SHA-1. Rijndael (Variant of AES) strengthens the security of data stored. Reason behind for selecting Rijndael rather than other is that the key used for encryption and decryption is suspected to meet-in-middle attack. RSA is used to solve the key distribution problem and in addition to this, SHA-1 to verify the integrity of the message. Use of message digest SHA-1 algorithm in combination of cryptographic algorithm provides strength in security of data storage in cloud. Here we specify different modules of envision system.



V. Existing system

In the current encryption systems, individual algorithms are used to secure data. Such as Linux systems use MD5 encryption algorithm while some others use maybe AES or DES algorithms to encrypt their passwords. But each of these mentioned algorithms have been cracked some or the other time, which means they are not invincible and can be broken by a skilled hand. Thus the security of the data (passwords in many cases) is highly and threateningly compromised. All these algorithms are very famous all around the globe and are used by many, some are even open source. This means that the algorithm's flaws are well known to all and in some cases, even the source code is well known to many. This adds up to the security woes of these algorithms. Thus there needs to be a system which overcomes these drawbacks while upholding the positive aspects of these widely known algorithms.

VI. Conclusion

In this report we have stated how we are going to work on making our system more secure using hybrid cryptography. Having security aspect in mind we have discussed algorithms such as Rijindael algorithm, RSA algorithm, SHA-512 algorithm. We have discussed how these algorithms would be implemented in the proposed system. We have described main drawbacks that are present in the present system and how those issues can be resolved to an extend using hybrid cryptography which is our proposed system.

Acknowledgement

Professor K.S.Charumathi has guided us throughout our project and we would like to offer our deepest appreciation for his efforts and patience. We would like to acknowledge and appreciate Head of Department. Sharvari Govilkar for her support throughout the project. Our final appreciation is directed towards our Principal R.K Moorti for always keeping his doors open for consultation or advice required.

References

[1] Chauhan [1] present that hybrid cryptography is better approach to maintain confidentiality and privacy of information during communication. They also proposed a hybrid algorithm for strong encryption. They state that there are various algorithms are available for cryptography but all of them have certain drawbacks.

Proposed algorithm is designed with combination of two symmetric algorithm techniques known as AES and DES. Proposed solution is implemented using 128 bit keys. Proposed solution is implemented using java technology. Here, they provide facility to select security algorithm as per requirement which may be AES, DES or hybrid algorithm. The complete work concludes that possibility of an algebraic attack on hybrid model is too poor and gives strong strength to encryption approach.

[2] Shankar Address that RSA is one of the most common algorithm for encryption and decryption. Subsequently, Round-robin scheduling is one of the most common useful algorithms for task scheduling and processing. Authors proposed a technique to integrate RSA algorithm with Round robin scheduling algorithm to extend level of security. In this approach method uses RSA algorithm to generate cipher text based on priority. Receiver receive message and decrypt the message according to priority. Proposed method reduces probability of man-in-middle attack and timing attack.

[3] Subasree Explore that computer network is an group of interconnected nodes. Various security threats attempt to compromise the network security and modify the content of packet. Confidentiality, authentication and integrity are the most crucial security principle used to maintain level of security. It requires the certain security algorithms to maintain security and maintain communication private. Proposed algorithm integrates Elliptic Curve Cryptography, Dual RSA algorithm and Message Digest MD5. This new security protocol has been designed for better security with integrity using a combination of both symmetric and asymmetric cryptographic techniques.

[4] Tianfu [4] address that internet is one of the most unsafe communication medium due to huge connection and public network. Information protection is one the of essential requirement. At present various security algorithms are proposed to achieve security during communication. All of them have certain good point and certain bad point. To improve the strength of encryption algorithm they proposed a hybrid model. Proposed model is combination of AES and DES. Both algorithms are symmetric key technique and itself they are very much capable for encryption. Integration of AES and DES would give a strong level of security at encryption end. A significant improvement in results has been observed with proposed solution.