



Data Security in Cloud Environment Using Cryptography Algorithm

Prof. Y. N. Patil¹, Mangesh D. Namewar²
Department of Computer Engineering^{1&2}
Dr. BAT University, Lonere, Raigad (MH, INDIA)

Abstract: In recent years, cloud computing is the new technical era and next generation architecture for IT as well as business industries and in which providing strong security to client data is the biggest issue for cloud service provider. Several cloud service provider gives the some short of secure services to client data but they are paid services and do not give the guarantee of data security from unauthorized access. In order to avoid this, we analyzed some cryptographic algorithm on different data to provide most secure and efficient algorithm. These algorithms perform encryption/decryption operation on data at client machine before storing data into the cloud. The cryptographic keys like public, private are to be used to give secure system. In this paper, we propose cryptographic analysis on data and avoid departure of data from unauthorized access and proposed technique gives more optimal solution for data security in cloud.

Keywords: Cloud Environment, Cryptography algorithm, Data Security, Keys, Authentication.

I. Introduction

Cloud computing is synonym for distributed computing which build with virtualization concept over a network and provide computing resources accessible via internet where client or organization can store data. Virtualization is a most important component of cloud computing and able to separate operating system from hardware that means transferring application from one system hardware to another. Cloud computing have some efficient advantages: on-demand services, wide network access, resource pooling dependent on need of client, rapid elasticity of resources, measurement of services to provide transparency for client[1], due to which it has been rapidly increasing and made famous among all IT enterprises. Cloud computing have three service model [2][4] based on services offered by cloud which are IaaS, PaaS, SaaS. Infrastructure as a service (IaaS) where cloud user can deploy and run arbitrary software on virtual machine provided by cloud provider and installation done by client itself. Platform as a Service (PaaS) where deployment of user created application using programming languages, libraries, services and tool supported by the cloud service provider. Software as a Service (SaaS) which provides capability to user is to use provider's application running on cloud infrastructure and this service is also called as "on-demand software". Example of these service models are Amazon EC2, Amazon S3, Google App Engine and Google sites and youtube video streaming respectively.

Due to such type of major functionalities cloud used to storage huge amount data and providing security to those data must be requisite. Some cloud service provider like Amazon, Azure and Google App Engine provide secure services but sometimes those services may be impotent. This brings many disputes in data security as the organization put their private data on cloud which are not under their own control. So, there may be chance of data loss.

II. Security Issues

As we already know, every coin has two side and cloud computing is no exception. There is some criticism in cloud because administrator have access to data stored in cloud, but exception in private cloud where organization do not have control over cloud equipment. Instead of thinking about data privacy on cloud, most of the organization trying to create their own cloud infrastructure. There are number of security issues related with cloud but these issues fall into two major class: security issues faced by cloud provider and security issues faced by cloud customer [6]. The provider must assure that their infrastructure is secure and their client data and applications are protected while the customer must assure that the provider has taken proper security measures to protect their data.

III. Cryptography and Analysis of Algorithm

Like different disease have different medicine, different cloud security issues have different solutions like cryptography is one of them. There are many cryptography algorithms like AES, RSA, DES, MD5 etc which are

used for security purpose where encryption of data takes place. These algorithms execute encryption/decryption operation on data, with encryption original data is converted into undecipherable format which cannot be easily understand without doing its conversion back into its original data format, this reverse conversion can do with decryption operation. To do encryption decryption operation on data the key plays important role, without keys nothing is possible.

RSA uses public and private key for encryption/decryption, public key is used to encrypt data and known to everyone. Data encrypted with public key can only be decrypted with private key. The choice of choosing key size is most critical task because it determines the security level. Practically choosing key size of 2048 bit or 4096 bit is not pre-determined and it can be balanced with range of some other decision like key lifetime, dedicated application some support 2048 key and some support 4096 key size, and is it mobile based application. When data is encrypted by using such keys and suppose an attack is found that permit a 2048 bit key to be hacked in 200 hours that does not mean that a 4096 bit key can be hacked in 40 hours, it may still need many years to crack a single 4096 key.

AES uses only one key to encrypt or decrypt the data. Since the same key is used, it must keep secret or with authorized user because compromise of this key would mean compromise of data. The key size of AES is 128, 192 or 256 bits. The strength of all key size of the AES is sufficient to protect data up to top secret level. The NIST states that it would take an RSA key size of 15360 bits to be equivalent to 256 bit AES. AES encrypted data unbreakable in the sense that no known cryptanalysis attack can decrypt the AES decrypted data without using the brute force search through all possible 256-bit keys.

DES has a 56-bit key and 64-bit block size and so it is not considered secure by today's standards because key size is too small.

Key used to encrypt data must be strong enough powerful to assure that encryption take place by using key, cannot be easily decrypted by any unauthorized user.

IV. Proposed Methodology for Data Security in Cloud

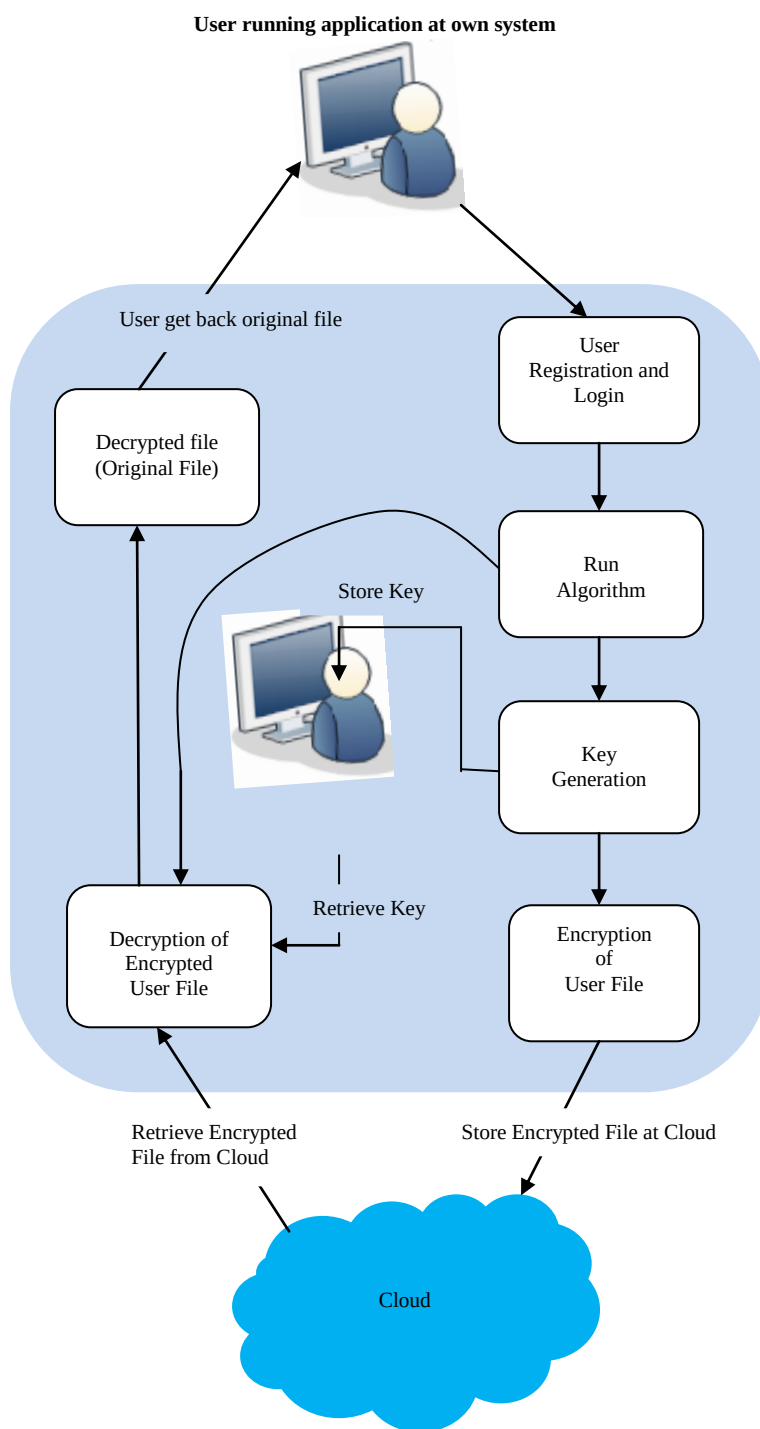
Now we are here proposing the system architecture for security of user data file in cloud environment using above cryptography algorithm. We have already seen that AES cryptography algorithm is the one of best optimal algorithm as compared to other. As we know RSA has good length of key size than AES but NIST state that even though key size of symmetric algorithm is smaller than asymmetric algorithm.

The security level of symmetric algorithm is approximately equal to asymmetric. So in following system architecture we have done analysis on how we can use AES algorithm in efficient way due to which user can secure his own data in cloud database storage. Here in our system architecture we have shown that only one cloud is used because working of our proposed system is at user desktop machine. That means the encryption of user data done at user machine and generated key is stored at user machine only. Due to which generated key must be isolated from cloud storage. So cloud contain only encrypted file. The overall working of system is as follows.

When users want to store own data on cloud the security of that private data must be requisite for user. Proposed system definitely gives secure system for user data. For this user first have to registered the system, if the user is new to the system. System is responsible for generating encrypted data of user's original data. When encrypted data generate at the same time a key is also generate and it is safely stored at user system not to the cloud storage. That generated data is different from original data which cannot be easily interpreted. To keep key securely is user responsibility. Without this key user or anybody cannot understand that encrypted data easily. Before the encrypted data is stored onto the cloud, the key is stored at user machine. For our practical purpose we used amazons cloud for data storage. This encrypted file may be differing in size as compared to original file. We used only simple storage services (S3) of amazons which provide memory to amazon's user by taking some amount as per data size and duration of data will keep in their memory storage.

The below Figure 1 shows the secure system for data before stored onto the cloud. After specific time of period user stored data onto the cloud and after that user wants own data back again then decryption process come into the picture. Then user again must have to sign in the system, if user did not sign out. Then user again run the same algorithm and take encrypted file data from cloud as a input, also take previously generated key at the time of encryption. The same key is needed for decryption without same key user cannot get back original data. The decrypted files will same in size as compared to original file size. So, there is no issue of data loss or data miss match. That means user get back his original file securely or without any loss of data.

Figure 1 Architecture of Proposed System



V. Conclusion

We explored security system for data using cryptography algorithm, and analyzed how it has been useful in cloud environment. Data security requirements are rapidly increasing in business sector, IT industries, private organizations, school, colleges, government sectors and everywhere else. The proposed method is protecting the data and also gives authentication to user. This system gives optimal solution about data security in cloud because if anybody access user data from cloud then they cannot understand the content of data. Since, data is in encrypted form. The system is implemented in such a manner it will always be useful of cloud user who do worries about data protection in cloud. In this way this system assure about security of data which is most essential requirement of cloud user. This proposed system itself gives assured of data protection before data store into cloud. As the system works efficiently for some type of data like .pdf file, .doc file, images etc. So further work need to be done for other types of data such as video, audio etc.

References

- [1] P. Mell and T. Grance, "The NIST Definition of Cloud Computing", NIST Special publication 800-145
- [2] T. Prabhakar and B. Sodhi, "Introduction to Cloud Computing," http://cse.iitk.ac.in/users/sodhi/cloud_lect.html
- [3] C. Wang, S. Chow, Q. Wang, K. Ren, W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage," IEEE Trans. Computers, vol. 62, No. 2, February 2013.
- [4] F. Shaikh and S. Haider, "Security Threats in Cloud Computing," Dec 2011 Abu Dhabi, United Arab Emirates.
- [5] E. Mohamed and H. Abdekar, "Data Security Model for Cloud Computing," ICN 2013.
- [6] "Cloud Computing Security" Internet : <http://en.wikipedia.org/wiki/CloudComputingSecurity>
- [7] Amazon web services <https://aws.amazon.com>
- [8] Leena Khanna and Prof. Anant Jaiswal "Cloud Computing: Security Issues and Description of Encryption Based Algorithms to Overcome Them" vol.3 Issue 3 March 2013 ISSN 2277 128X.
- [9] William Stallings, "Cryptography and Network Security," Pearson Publication, 2013.
- [10] Parsi Kalpna et. al. "Data Security in Cloud Computing using RSA algorithm".

Acknowledgments

I would like to thanks Prof. Y. N. Patil for his worthful guidance and Prof. Dr. A. W. Kiwelekar head of Department of Computer Engineering. Also I would like to thanks my parents for their support.