International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 04
February 2018

Secure Cloud through progressive Encryption and Decryption methods

T. Rajesh, V.VidyaSagar, Dr Vamsi Krishna
[#1] **Asst.Professor,** Bhimavaram Institute of Engineering and Technology, Bhimavaram.
[#2] **Asst.Professor,** Andhra Loyola Institute of Engineering and Technology, Vijayawada.
[#3] Professor. KITS Engineering College.
[#1]rajesh.cse6@gmail.com,[#2]vidyasagar.vendrapati@gmail.com

Abstract*—Several user and organizations across the world are using cloud storage to store the data as it provides more accessibility and less maintenance cost. But the main problem with using cloud is its security which can be accessed by unauthorized users. Fully protection is needed to safeguard that the files placed in the server are only available to authorized person. This paper proposes a system that will combineRivest-ShamirAdleman (RSA) and Data Encryption Standard (DES) combination encryption process using USB device. The files may be read in the cloud but all the files present will remain encrypted till the USB device is plugged into the computer. By using this technique we can provide a secured mechanism which will generate a random password all the time it is been used. This provides a high security to the system. The suggested system will identify the USB that comprises the private-key used for the files to be downloaded from the cloud.*

Keywords-cloud computing security; cryptography RSA; DES; cloud storage; cloud server;

I. INTRODUCTION

In the present world of Internet, the increasing reputation of cloud computing have paying attention a huge amount of Internet users. Cloud computing can be defined as a model for allowingappropriate, on-demand network access to a shared pool of configurable and reliable computing resources, referred as real-time network with a large number of connected devices [1]. The connected devices may be PC, smart phones or tablets. Basically, any device that has a valid MAC address of integrated network adapter is included. The cloud computing is all about sharing of resources among users in real-time. Real-time refers to the distribution of data to be visible immediately to new users who has the authentication to access it.

One of the main advantages of cloud computing is that it distributes applications and storage spaces as services over the Internet for little to no cost [2]. Through internet one can access his data and applications from anywhere and can control them easily. By using cloud user can access the data from any computer which is not restricted to a single device.

Another important benefit is that cloud computing tremendouslydrops down the hardware cost of machines. Users are not necessary to use any high-end machines because the applications will be presented in the cloud and the computer will only show the results of what their applications are planned to produce. In addition all these,

Cloud computing has very important factors such as administration, scalability and extremely reduced hardware and software costs. All of the factors provide extremely attractive solutions for personal users and small or big business holders [3].

II. CLOUD COMPUTINGSECURITY ISSUES

Data security is one of the security issues in cloud computing that have been discussed by [4]. It is a primary concern for any technology, but it becomes a major task when Software-as-a-service (SaaS) users have to rely on their providers for proper security [9-11]. In other words, the main issue in cloud computing is the security leaks, which avoid people to fully accept the cloud systems. Since all the files are stored in the cloud servers and available at all times, hackers have full time of working hours for cracking the file safety walls such as encryption and authentication. Following are the issues regarding security in cloud service providers, which have been registered and are directly related to file storage.

A. Secure Data Transfer

Cloud computing is all about interacting which has real time communication channel with clients in order to send and receive data packages. However, these data packages can be tracked easily because the internet is used for communication and it is vulnerable to attacks at any time. Therefore, the cloud computing service providers must guarantee that the files, or the data file chunk, are properly secured for full protection [5].

B. Secure Data Storage

By using cloud user can have large amount of data stored. This data can be highly confidential which can't be accessed by others. In order to provide high security we are combining

the cloud storage with cryptographic techniques [5]. In all known cloud services, data are encrypted and kept in the cloud servers. When the user needs to view the data, the decryption key is applied to decrypt the data and then seen by the users. Such file encryption and decryption is applied in order to protect unauthorized access of users into cloud servers [5].

C.User Permissions

Another security issue in cloud computing is the accessibility over other users' files and documents for user is limited. A user is valid in the server when the correct login details are given. However, users are not allowed to access private files or non-public files uploaded by other users. Users must be clear of who has admin rights in the cloud service providers for data organization purposes because these people has the control of accessing data kept in the clouds [5].

D. Encryption and Decryption

According to [6], encryption is the conversion of any type of data into a form that is not understandable. Similar to encryption decryption is a reverse process of encryption which converts the encrypted data into understandable format. The encrypted text is call cipher text which is used to maintain high level of confidentiality of data.

The text is being encrypted by using a key to perform the reverse operation on the cipher text we require the same key. It is impossible to convert the text to understandable format without the key. Therefore, a decryption key must be safeguarded and protected properly. The more complex the encryption algorithm, the more challenging it becomes to break the cipher for opening the message without authorization.

There are many encryption algorithms proposed since the accessibility of earlier computer communications. Encryption algorithms are normally characterized differently according to their working principles. The most common encryption algorithms [13] used is such as DES, RSA, WPA, Twofish andAES.

RSA algorithm [8] is in the class of public-key encryption based on cryptography implementations. The RSA algorithm is based on the mathematical equivalent, which is invented by the English mathematician Clifford Cocks. This equal is near factoring the large integers and then returning them back to their original values with reverse steps. This is called prime factorization of the selected prime numbers.

The idea behind the RSA algorithm is that, the data is encrypted with an equation. RSA algorithm is asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e. Public Key and Private Key**.**As the name describes that the Public Key is given to everyone and Private key is kept private.

1.Key generation

As mentioned in earlier sections, RSA algorithm works with a public key and a private key pairs. It is totally safe to issue the public key to anybody for encryption purposes because the public key cannot be useful for the reverse process. The messages can simply be decrypted with the private key. The keys for the RSA algorithm are generated based on the mathematical theorems and formulations. The algorithm uses prime factorization as shown in (1).

$$n=pq$$

where$p$ and q are prime numbers.

The design of the private key of encryption is defined by the following formulation. The private key is the key for decryption of the cipher text so it must be kept secret at all times.

$$\Phi(n)=(p-1)(q-1)$$

Where Φ(n)*is the totient function*
e is a common factor of (p-1)(q-1)

2. Encryption

The encryption is done by both using the public key and private key. The person who needs to receive the message is given the public key. The person who encrypt the message haves private key. In the encryption method, the message is changed to a number, say it m, by applying the packing scheme method.

$$C = P^e \ mod(n)$$

The cipher text is then computing by following formula using exponentiation by squaring method. After the execution of the formula, instead of the original message m, the cipher text c is sent to the receiver.

3. Decryption

Decryption is the inverse process of the encryption technique. The same formula is used by applying reverse padding scheme method. The received cipher text from the sender is applied the following formula in order to get the original message which is encrypted in the sender machine. In order to decrypt the message, the received must use the private key of its own.

$$P = C^d mod(n)$$

III. PROPOSEDSYSTEM

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 04
February 2018

The proposed system recommends a new technique of how the files are kept in the cloud by combining the existing encryption method and cloud computing system. Most users are not happy by knowing that their private or confidential files can be read for various purposes by the cloud Server providers. This could be for maintenance purposes, security thread claims or even consistent file backup processes. Usually, these explanations are completely valid in order to protect the cloud Server status and performance. However, users are unwilling to upload their confidential files into cloud servers.

This proposed method uses an advanced technique for the protection of files. RSA is recognized as the toughest publicly existing encryption technique. This algorithm works with both private key and public key. The files are encrypted using the public key which can only be decrypted using private key. Before uploading the files into the cloud server these files are been encrypted using public key so that even a person gets access of the file he cannot read them without having private key.

Then, a removable device is used to generate the key which will encrypt the files during upload process.If the user wants to access the files present in the cloud server he need to plug in the same device which will generate the private key and decrypt the files that are downloaded from the cloud.

In case when users do misplace the removable device, a backup feature must be offered. Unfortunately if the user doesn't have a backup and loose the device the it is not possible to decrypt the files to the plaintext. Figure 1 illustrates the overall view of the proposed concept clearly.

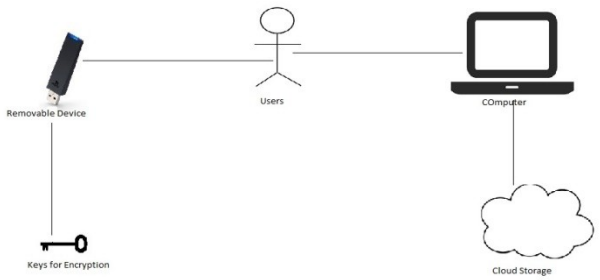

Figure 1.Proposed Concept Structure - Combination of cloud computing and RSA Algorithm

A.Comparison of Cloud System

This section relates between the investigated systems and their features. The comparison is for the cloud simulation which is required for the implementation of the encryption. This simulation will act like a cloud server which allows uploading and downloading encrypted files. This simulation is to be equipped with some features in order to show the working prototype of encryption and decryption security suggestion.

TABLE I. COMPARISONOFTHEINVESTIGATED MODELS.

#	Features	Google Drive	DropBox	SkyDrive
1	Encryption	Unencrypted	DES-256bit	Unencrypted
2	File Uploading	Supports	Supports	Supports
3	File Downloading	Supports	Supports	Supports
4	File Sharing	Supports	Supports	Supports
5	Synchronization	Supports	Supports	Supports
6	User Account	Supports	Supports	Supports

As we can see most of the drives doesn't encrypt the file during uploading process, so it is important to have a good encryption technique which can protect the privacy of the user. If required even the drop box doesn't encrypt the files for some constraints. However, all these three cloud based services are well trusted by their regular users. It is a challenge for users who would like to have their files completely secured even if the legal authorities ask the service providers to reveal.

It is noticed that cloud server integration with theencryption is not performed properly. All the user files can be accessed because files are stored unencrypted. Even when the files are encrypted; the decryption key is still stored in the cloud servers which can be able to access the files present in cloud. Because of these issues we are proposing an approach which combines the use of cloud server using powerful encryption techniques.

IV. METHODOLOGY

The proposed study is improved with Waterfall Development Methodology with which a sequential implementation of stage by stage is performed. The proposed system does not have many goals or user requests as it is a background process in which services are developed. In this type of improvements, users are less involved due to user irrelevancy. The Waterfall model is a powerful methodwhere we doesn't move to the next phase until requirement phase is completed.

A. Requirements

The first stage of the Waterfall model is the definition of system requirements. Here we collect what are the inputs and outputs of the system. In our proposed system our main concern is about providing the security to the files these files are stored in cloud which can be accessible from anywhere and can be accessed in any computer through internet. It can be considered as a middleware between the user and cloud server. The files are been encrypted before they are uploaded to the cloud server.

B. Design

This system can be implemented for any type of users. First the user needs to create an account in the cloud storage. Then he can upload his files into the cloud storage while uploading the files he need to encrypt the data which requires an USB device for the generation of key. The same device need to be used during the process of downloading of the files for the decryption process. The major goal of our system is encryption of decryption of data during uploading and downloading of data from cloud storage. If the data is been uploaded without encryption it can be accessed by others which compromises the privacy of the user.

C. *Implementation*

In order to implement the system efficiently, we are integrating two cryptographic techniques which are considered to be more powerful techniques.

D. *Verification*

Users will upload their confidential files into cloud servers. The files which are uploaded into the cloud should be encrypted first. While downloading the files from cloud verification process is required. There should not be any damage to content of files during the process of encryption.

In order to test the functionality, some of the sample files will be encrypted and are uploaded to the cloud storage. During the process of downloading the file we need to verify whether the files have the same size as original file and the content should not be changed after decrypted. This will guarantee that the files encrypted can be decrypted back into their original forms.

E. *Maintenance*

The maintenance stage of the Waterfall model involves modification of the system and improving the performance. These improvements are done based on the user request. However, the maintenance part is not applicable at this stage to the proposed system.

V. CONCLUSION ANDFUTUREWORK

This paper presents a system which combines DES algorithm with RSA which is used for key generation for encrypting and decrypting of data. By using this technique we can provide highly secured data which is a main concern of placing data in cloud. It also describes the organization of cloud structure. Four stages in Waterfall method has been explained for the proposed system. This method is designed by combining two cryptographic techniques which are implemented using an USB device. Whenever this device is plugged it is detected automatically and keys are generated which are used for both encryption and decryption purpose.

REFERENCES

[1] Dr A.M. Gonsai and L.M. Raval, "Evaluation of Common Encryption Algorithm and Scope of Advanced Algorithm for Simulated Wireless Network,", Int. Journal of Computer Trends and Technology, vol.11(1), pp. 7-12, May 2014

[2] T. Chou, "Security Threats on Cloud Computing Vulnerabilities," International Journal of Computer Science & Information

Technology, vol. *5*(3), pp. 79–88, 2013.

[3] J. Strickland, "How Cloud Computing Works," Howstuffworks.com. Retrieved from http://computer.howstuffworks.com/cloudcomputing.htm, 2011.

[4] K.Hashizume, D.G. Rosado, E. Fernandez-Medina, and E.B. Fernandez, "An analysis of security issues for cloud computing," Journal of Internet Services and Application, 4:5, Feb 2013.

[5] Beckham, The top five security risks of cloud computing, Available on internet: http://blogs.cisco.com/smallbusiness/the-top-5-securityrisks-of-cloud-computing, 2011.

[6] T. Laukkarinen, J. Suhonen, and M. H¨annik¨ainen, "A survey of wirelesssensor network abstraction for application development," *InternationalJournal of Distributed Sensor Networks*, vol. 2012, 2012.

[7] C. Kirsch, E. Pereira, R. Sengupta, H. Chen, R. Hansen, J. Huang, F. Landolt, M. Lippautz, A. Rottmann, R. Swick *et al.*, "Cyber-physical cloud computing: The binding and migration problem," in *Proceedings of the Conference on Design, Automation and Test in Europe*. EDAConsortium, 2012, pp. 1425–1428.

[8] S. Ravi, A. Raghunathan, and S. Chakradhar, "Tamper resistance

mechanisms for secure embedded systems," in *VLSI Design, 2004. Proceedings. 17th International Conference on*. IEEE, 2004, pp. 605–611.

[9] J. Archer, D. Cullinane, N. Puhlmann, J. Reavis, P. Kurtz and B. Alan,"Security Guidelines for critical areas of focus in cloud

computing v3.0," Cloud Computing Alliance, 2011.

[10] "International Telecommunication Union, X-509| ISO/IEC 9594-8, The directory: Public-key and attribute certificate frameworks, ITU, XSeries," 2001.

[11] "Cloud Security Alliance," [Online]. Available: https://cloudsecurityalliance.org/download/the-notorious-nine- cloudcomputing- top-threats-in-2013/.

[12] D. A. B. Fernandes, L. F. B. Soares, J. V. Gomes, M. M. Freire and P.R. M. Inacio, "Security issues in cloud environments: a survey,"
International Journal of Information Security, vol. 13, no. 2, pp. 113-
170, 2014.

[13] LC.l oCuodl uCmobmupsu, t"iCngo manpdu tAernwaloyrtlidc'ss w20il11 5l eFaodr eITca sspt ePnrdeidnigct,s" 2S0ec1u4r. ity,

[14] T. Steiner and H. Khiabani, "An Indroduction to Securing a Cloud
Environment," 2012.

[15] "Security for Cloud Computing," Cloud Standards Customer Council,2012.

[16] "Security On Demand," [Online]. Available: https://www.securityondemand.com.