Encryption & Fingerprint Based Security in Cloud Computing

AZAZ KHAN & NASIB SINGH GILL
Department of Computer Science & Applications, Maharshi Dayanand University,
Rohtak, Haryana, India.

Received: May 17, 2018 Accepted: June 30, 2018

ABSTRACT *A cloud user can utilize different computing resources (e.g. network, storage, software application), whenever required, without being concerned with the complex underlying technology and infrastructure architecture. The most important feature is that the computing resources are available whenever they are needed. Additionally, users pay only for the resource they actually use. By using cloud-based solutions, companies do not need to have their own hard ware infrastructure to host their application. Thus, they eliminate the need for a large capital investment to purchase this hardware. However, there is often a lack of security when realizing such cloud-based solutions. In the longer term, the problems caused by this lack of security might inhibit companies from taking advantage of cloud-based solutions. This paper aims to strengthen the security of the cloud-based data storage for various clients by encryption and fingerprint mechanism.*

Keywords: *Cloud computing Security, Blowfish Algorithm, Cryptography*

I. INTRODUCTION

Cloud computing [1] can be considered as a service provided by a service provider. The user of this service does not need to know or worry about how the service (e.g. network, storage, application) is provided or maintained. Instead, the user is only concerned that the service is available whenever the user needs this service. The cloud computing approach relieves companies from needing to have their own data centers. It avoids purchase, management, and updating costs for hardware, cooling systems, storage, and power supplies. As a result, the use of the cloud computing enables companies to quickly start up a new business and to scale their business efficiently.

Cloud computing is a growing area of concern in the IT security community because cloud architectures are literally popping up all over [2]. Public clouds are available from Google, Amazon, Microsoft, Oracle, Eucalyptus, and many other vendors. The basic concerned with cloud computing is about security. While there is no "ultimate security" solution, security experts will try to minimize the potential for security threats as much as possible. Although they have tried to minimize security risk as much as possible, cloud computing still possesses many security risks. Some of these security risks are well known and some of them are new.

Confidentiality, integrity, and availability are the three key aspects of security [3]. Ensuring confidentiality means that no one can read our data unless we want them to read it, integrity ensures that no one can modify our data without the modifications being detected, and availability means that we can access our data at any time. Cloud computing also needs to deal with security risk/threats just as any other service.

In this work a security solution for data storage in cloud computing is examined. The solution encompasses confidentiality and integrity of the stored data, as well as a secure data sharing mechanism in the cloud storage systems. This paper aims to strengthen the security of the cloud-based data storage for various clients by encryption and fingerprint mechanism.

II. SECURITY ISSUES FACED BY CLOUD COMPUTING

Cloud allows users to achieve the power of computing which beats their own physical domain. It leads to many security problems. The cloud service provider for cloud makes sure that the customer does not face any problem such as loss of data or data theft. Cloud computing infrastructures use new technologies and services, most which have not been fully evaluated with respect to security. There is also a possibility where a malicious user can penetrate the cloud by impersonating a legitimate user, there by infecting the entire cloud. This leads to affects many customers who are sharing the infected cloud. The security issues faced by cloud computing are discussed below [5].

1. Data Access Control*:* Sometimes confidential data can be illegally accessed due to lack of secured data access control. Sensitive data in a cloud computing environment emerge as major issues with regard to security in a cloud based system. Data exists for a long time in a cloud, the higher the risk of unauthorized access.

2. Data Integrity*:* Data integrity comprises the following cases, when some human errors occur when data is entered. Errors may occur when data is transmitted from one computer to another otherwise error can occur from some hardware malfunctions, such as disk crashes. Software bugs or viruses can also make viruses. So at the same time, many cloud computing service consumer and provider accesses and modify data. Thus there is a need of some data integrity method in cloud computing.

3. Data Theft: Cloud computing uses external data server for cost affective and flexible for operation. So there is a chance of data can be stolen from the external server.

4. Data Loss: Data loss is a very serious problem in Cloud computing. If banking and business transactions, research and development ideas are all taking place online, unauthorized people will be able to access the information shared. Even if everything is secure what if a server goes down or crashes or attacked by a virus, the whole system would go down and possible data loss may occur. If the vendor closes due to financial or legal problems there will be a loss of data for the customers. The customers won't be able to access those data's because data is no more available for the customer as the vendor shut down.

5. Data Location: Consumers do not always know the location of their data. The Vendor does not reveal where all the data's are stored. Cloud Computing offers a high degree of data mobility. The Data's won't even be in the same country of the Customer, it might be located anywhere in the world. They may also wish to specify a preferred location (e.g. data to be kept in the USA) then requires a contractual agreement between the Cloud service provider and the consumer that data should stay in a particular location or reside on a given known server.

6. Privacy Issues: Security of the Customer Personal information is very important in case of cloud computing. Most of the servers are external, so the vendor should make sure that is well secured from other operators.

7. Security issues in provider level*:* A Cloud is good only when there is a good security provided by the vendor to the customers. Provider should make a good security layer for the customer and user and should make sure that the server is well secured from all the external threats it may come across.

8. User level Issues: User should make sure that because of its own action, there shouldn't be any loss of data or tampering of data for other users who are using the same Cloud.

9. Infected Application: Service provider should have the full access to the server with all rights for the purpose of monitoring and maintenance of server. So this will prevent any malicious user from uploading any infected application onto the cloud which will severely affect the customer and cloud computing service.

III. PROPOSED WORK

The cloud storage providers claim that they supply the stored data with necessary security solutions. The truth is that users would not feel secure, because they have to trust the servers, while they do not exactly know what is going on inside the servers. Users lose their trusts even more, especially when they hear some news about, or become a victim of a security glitch. In this paper a cryptographic access control mechanism [4] is applied for data confidentiality and integrity. In order to provide the needed security for the stored data in the cloud, we ensure that the data is provided with cryptographic protection in terms of client centric solution.

For confidentiality of data, encryption of the data at the client side is carried out. The encryption must be performed just before storing/uploading it to the cloud. Also the data needs to be decrypted after retrieving it from the cloud. We propose one of famous symmetric cryptography algorithm namely Blowfish for encryption and decryption of user's data.

Blowfish a public domain encryption algorithm with a block size of 64 bits, and it uses a variable key length. Blowfish was invented by an American cryptographer, Bruce Schneier, and it was introduced in 1993. It is mainly designed for large microprocessors. Its main design criteria are to be fast, compact, simple and having variable security. Its key length can be op to 448 bits long. Blowfish makes use of cycles/rounds. It consists of 16 rounds, and in each round transpositions and substitutions are used. However it is said to suffer from weak key problem, but with a full 16 rounds implementation, no ways are known to break the security of the algorithm until now.

For integrity of the data, we use finger print based security mechanism. The fingerprint of users are taken as images and stored in the database. The user's whose fingerprint matches with database's fingerprint are allowed to access and store the data from cloud storage.

IV. PROPOSED ALGORITHM

In this work, we applied two algorithms for providing security of client's data on the cloud server. The authentication security is provided by

biometric traits with fingerprint and a cryptographic access control mechanism is applied for data confidentiality and integrity. Both these security concepts are applied from the client side.

A. **Authentication security using Biometrics traits (Fingerprint)**

Biometrics refers to the use of unique physiological characteristics to identify an individual. A number of biometric traits have been developed and are used to authenticate the person's identity. The idea is to use the special characteristics of a person to identify an individual. In this dissertation we use fingerprint biometric traits. A general impression of fingerprint is shown in figure 1 below.

Figure 1: Impression of Finger Print [6]

When using biometrics as an authentication tool, a cloud user, during Enrollment for a service, registers with his unique traits (finger prints, tongue, face, iris etc.). These get stored as templates at the cloud service provider's end. Every time when an access is made, the cloud user is prompted to provide his enrolled trait that is compared against the template and authenticated accordingly.

B. **Confidentiality and Integrity security using Cryptography Technique**

Cryptography uses encryption and decryption concepts for providing confidentiality and integrity related security. Encryption is the conversion of data into a form that cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so it can be understood. For enhanced security, the text/images from user's end can be encrypted for storing in cloud data storage. By doing so, even if a hacker gains access to an image/text, he may not be able to decrypt it back to the original image, provided, the underlying encryption algorithm is very complex to decrypt. There are number of encryption algorithms that are used for the finger print images. One such algorithm is Blowfish algorithm that is used in this thesis.

Blowfish is one of the most public domain encryption algorithms [7]. Blowfish was designed in 1993 by Bruce Schneider as a fast alternative to existing encryption algorithms. Blowfish is a symmetric key block cipher that uses a 64 bit block size and variable key length. It takes a variable-length key from 32 bits to 448 bits. Blowfish has variants of 14 rounds or less. Blowfish is one of the fastest block ciphers which has developed to date. No attack is known to be successful against it, though it suffers from weak keys problem.

The algorithm has two parts, key expansion and data encryption. Key expansion consists of generating the initial contents of one array (the P-array), namely, eighteen 32-bit sub keys, and four arrays (the S boxes), each of size 256 by 32 bits, from a key of at most 448 bits (56 bytes). Blowfish also incorporated two exclusive-or operations to be performed after the 16 rounds and a swap operation. Blowfish can have a key that ranges from 32 to 448-bits. It is suitable and efficient for hardware implementation and no license is required. Blowfish is a cipher based on Feistel rounds. No attack is known to be successful against this. It is suitable for applications where the key does not change often, like a communications link or an automatic file encryptor. It is significantly faster than most encryption algorithms when implemented on 32-bit microprocessors with large data caches.

Algorithm: There are 16 rounds in blowfish; input is a 64-bit data element, x. x is divided into two 32-bit halves: xL, xR. Then, for i = 1 to 16 XL = xL XOR Pi, xR = F(xL) XOR xR And Swap xL and xR After the sixteenth round, xL and xR are has to swap again to undo the last swap. Then, xR = xR XOR P17 and xL = xL XOR P18. Recombine xL and xR to get the cipher text.P1, P2,..., P18 are used in the reverse order to decrypt [8].

The basic algorithm for Blowfish is illustrated as follows:

1. Divide X into two 32-bit halves XL and XR
2. For i=1 to 16:
3. XL = XL $\oplus$ Pi
4. XR = F (XL) $\oplus$ XR
5. Swap XL and XR
6. End for

7. Swap XL and XR
8. XR = XR ⊕ P17
9. XL = XL ⊕ P18
10. Recombine XL and XR
11. Output X (64-bit data block: cipher text)

For decryption, the same process is applied, except that the sub-keys Pi must be supplied in reverse order. The nature of the Feistel network ensures that every half is swapped for the next round.

The flowchart for above algorithm is shown in figure 2 below [9].

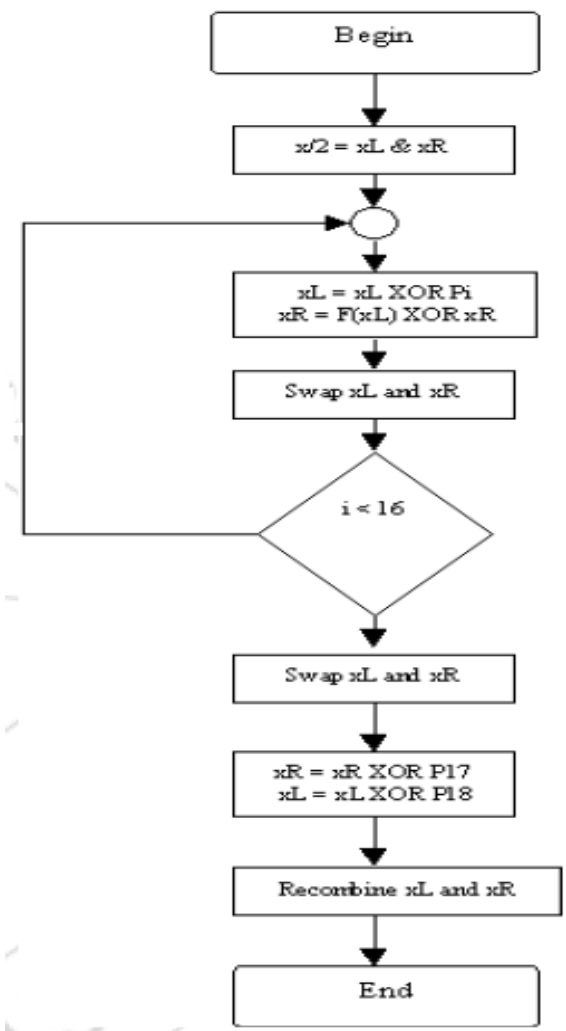

Figure 2: Flowchart for Blowfish Algorithm

V. IMPLEMENTATION

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective. The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

Modules

Our Implementation of Security in Cloud Data Storage consists of multiple modules as described below:

1. Cloud Server Module:

In this module the cloud server administrator starts the server process for providing data storage and retrieval services. For this administrator must authenticate the server by issuing login name and password. The authenticate administrator can view the list of registered users/clients and their resources available on the cloud storage. Finally the admin can start the server process for communication with different clients.

2. Client Module:

In this module, the client sends the query to the server. Based on the query (storage or retrieval) the server sends the corresponding file to the client. Before this process, the client authorization step is involved. The client authentication step requires user name, password and fingerprint information. On the server side, it checks the client name, password and matches the fingerprint image already registered with the server for authentication. If it is satisfied then server displays the list of resources to the client. The client can view any resource, modify the resources and save back the modified file. The client can also create new file and save it to the server for future reference.

If client is not already registered with server then he can registered with the cloud server by filling the registration form provided with client module. In the registration form client fills the necessary details and authentication information such as login name, password and fingerprint image. After successfully registration the client can login with server and do necessary processing.

3. Cloud data storage Module:

With cloud data storage, a user can store his data on a set of cloud servers, which are running in a simultaneous. The user interacts with the cloud servers via Cloud Service Provider (CSP) to access or retrieve his data. The user can stores new files and modify the existing files whenever required. The cloud data storage stores the data in encrypted form so that only authorized user can access the resources stored on the cloud storage.

VI. CONCLUSION

Cloud computing can be considered as a service provided by a service provider. The user of this service does not need to know or worry about how the service (e.g. network, storage, application) is provided or maintained. Instead, the user is only concerned that the service is available whenever the user needs this service. The cloud computing approach relieves companies from needing to have their own data centers. The basic concerned with cloud computing is about security. While there is no "ultimate security" solution, security experts will try to minimize the potential for security threats as much as possible. In this work a security solution for data storage in cloud computing is examined. The solution encompasses confidentiality and integrity of the stored data, as well as a secure data sharing mechanism in the cloud storage systems. This paper aims to strengthen the security of the cloud-based data storage for various clients by encryption and fingerprint mechanism.

REFERENCES

1. J. W. Rittinghouse, Cloud computing: implementation, management, and security. Boca Raton: CRC Press, 2010.
2. P. Mell and T. Grance, "The NIST definition of cloud computing (draft)," NIST special publication, vol. 800, no. 145, p. 7, 2011.
3. G. Anthes, "Security in the cloud," Communications of the ACM, vol. 53, no. 11, p. 16, Nov. 2010.
4. M. E. Whitman, Principles of information security, 4th ed. Boston, MA: Course Technology, 2012.
5. ZiyuanWang, "Security and privacy issues within the Cloud Computing", International Conference on Computational and Information Sciences, 2011.
6. D.Pugazhenthi, B.Sree Vidya, "Multiple Biometric Security in Cloud Computing", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 4, April 2013.
7. Pratap Chandra Mandal, "Evaluation of performance of the Symmetric Key Algorithms: DES, 3DES ,AES and Blowfish", Journal of Global Research in Computer Science, Volume 3, No. 8, August 2012.
8. S. S. Sudha, S. Divya, "Cryptography in Image Using Blowfish Algorithm," International Journal of Science and Research (IJSR), Volume 4 Issue 7, July 2015.
9. Pia Singh, Prof. Karamjeet Singh, "Image Encryption and Decryption Using Blowfish Algorithm in Matlab", International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013.
10. A. Singh and M. Shrivastava, "Overview of Attacks on Cloud Computing," International Journal of Engineering and Innovative Technology (IJEIT), vol. 1, no. 4, Apr. 2012.
11. "Security and Privacy in Cloud Computing - 600.412.lecture02.pdf." [Online]. Available: http://www.cs.jhu.edu/~ragib/sp10/cs412/lectures/600.412.lecture02.pdf. [Accessed: 02-May-2013].
12. Nidal Hassan Hussein, Ahmed Khalid, "A survey of Cloud Computing Security challenges and solutions", International Journal of Computer Science and Information Security (IJCSIS), Vol. 14, No. 1, January 2016.