IMPLEMENTING ENCRYPTION ALGORITHMS TO ENHANCE DATA SECURITY OF CLOUD IN CLOUD COMPUTING

Jagriti Dhamija, Shalini Soni
M.Tech Student, Assistant Professor,
Computer Science Department,
JNCT, Rewa, Madhya Pradesh, India

Abstract- In Cloud computing technology there are a set of important policy issues, which include issues of privacy, security, anonymity, telecommunications capacity, government surveillance, reliability, and liability, among others. But the most important between them is security and how cloud provider assures it. Generally, Cloud computing has several customers such as ordinary users, academia, and enterprises who have different motivation to move to cloud. If cloud clients are academia, security effect on performance of computing and for them cloud providers must find a way to combine security and performance. For enterprises the most important problem is also security but with different vision. For them high performance may be not as critical as academia. This paper discusses to which degree this skepticism justified, by presenting the Cipher Cloud. The Cipher Cloud is a framework that lets users keep their data confidentially on public cloud frameworks. To achieve this, the Cipher Cloud uses a two-step encryption process, in by which all the data sent from a client to a cloud server or vice versa is kept totally encrypted and confidential. The most thorough security controls needed to protect the most sensitive data may not be guaranteed in public cloud computing architectures, while they can be realized in private cloud computing architectures. As the most promising cloud computing approach, this paper suggests selective encryption techniques, which almost gives the data confidentiality just like private cloud models.

Keywords- Google App Engine, Eclipse IDE, Security, Asymmetric Algorithm, Symmetric Algorithms.

---

1. INTRODUCTION

Cloud computing proposes new model for computing and related issues like compute, storage, software. It provides development environment, allocation and reallocation of resources when needed, storage and networking facility Virtually. It satisfies the on-demand needs of the user. It facilitates the sharable resources "as-a-service" model. For the organization, the cloud offers data centers to move their data globally. It eliminates the responsibility of local nodes for maintaining their data and cloud supports customizable resources on the web. Cloud Service Providers maintains computing resources and data automatically via software. Need of the user. It facilitates the sharable resources "as-a- service" model. For the organization, the cloud offers data centers to move their data globally. It eliminates the responsibility of local nodes for maintaining their data and cloud supports customizable resources on the web. Cloud Service Providers maintains computing resources and data automatically via software.

1.1 Research motivation and objectives

Cloud computing users work with data and applications that are often located off-premise. However, many organizations are uncomfortable with the idea of having their data and applications on systems they do not control. There is a lack of knowledge on how cloud computing impacts the confidentiality of data stored, processed and transmitted in cloud computing environments. The goal of this paper is to create a framework that clarifies the impact of cloud computing on confidentiality preservation, by making stepwise recommendations on:

1. How data can be classified on confidentiality?
2. How data classifications relate to the security controls needed to preserve the confidentiality of data?
3. How the process of security control selection is negatively influenced in cloud computing environments?
4. How to cope with the negative influences of cloud computing on the protection of data confidentiality?

2. BACKGROUND STUDY

Cloud computing is basically broken down into three segments: "application" "storage" and "connectivity." Each segment serves a different purpose and offers different products for businesses around the world. The services themselves have long been referred to as Software as a Service (SaaS). There is an increasingly perceived vision that computing will one day be the 5th utility (after water, electricity, gas, and telephony). To deliver this vision, architecture was made for creating cloud. Cloud computing is the concept implemented to decipher the Daily Computing Problems, likes of Hardware, Software and Resource Availability unhurried by Computer users. The cloud Computing provides an undemanding and non-ineffectual Solution for Daily Computing. The prevalent Problem associated with Cloud Computing is the Cloud security and the appropriate Implementation of Cloud over the Network. With the help of different encryption algorithms like- DES, Users can enhance the data security of cloud computing.

3. OBJECTIVE OF WORK

The objectives of the application will be as follows:

1. Creating secure cloud architecture.
2. Cloud access control and key management.
3. Identification and privacy in cloud.
4. Remote data integrity protection.

5. Dynamic data operation security.
6. Software and data segregation security.
7. Secure management of virtualized resource.
8. Joint security and privacy aware protocol design.
9. Failure detection and prediction.
10. Availability, recovery and auditing.
11. Secure wireless cloud.

4.PROPOSED STEPS FOR WORK

In this different encryption algorithms are used like - AES, DES, RSA and Blowfish to ensure the security of data in cloud. For the perspective of different users, these algorithms are proposed. DES is developed in early 1970s; Blowfish is developed by Bruce Schneier, in 1993. AES is developed by NIST in 2001.These algorithms are symmetric key, in which a single key is used for encryption/decryption purposes. RSA is asymmetric key algorithm, created by Ron Rivest, Adi Shamir and Lenard Adleman in 1978. This algorithm is used for public key cryptography. In this, two public/private keys are used for encryption/decryption. In this there is an option to the users to choose any algorithm according to him/her need and accordingly encrypt/decrypt the data on cloud. Here the Java runtime of Google App Engine, i.e. JDK 1.6. Eclipse IDE. Google App Engine SDK 1.6.0 or higher. Google Plug-in for Eclipse, for creating, debugging and testing the application.

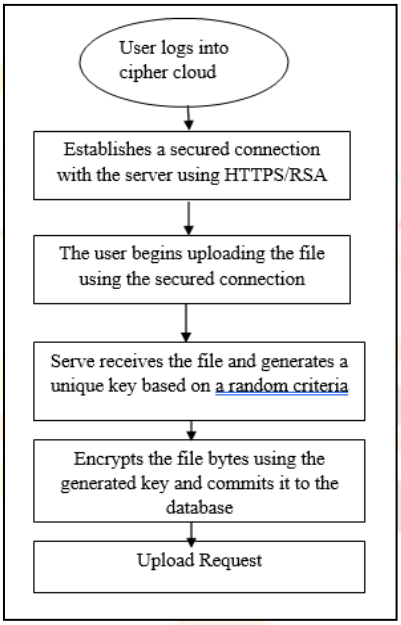

Figure 1: Proposed steps of the work

5.SECURITY ALGORITHMS

(a) RSA Algorithm
(b) DES Algorithm
(c) AES Algorithm
(d) Blowfish Algorithm

5.1 RSA Algorithm

Select two prime numbers. Calculate n = p*q.
Calculate f (n) = (p-1) (q-1)
Select e such that e is relatively prime to f (n) and less than f (n).
Determine d such that de congruent modulo 1 (mod f (n)) and d<f (n).
Public key = {e, n}, Private Key = {d, n} Cipher text c = message e mod n
Plain text p = cipher text d mod n

5.2 DES Algorithm

Triple DES uses a "key bundle" which comprises three DES keys, K1, K2 and K3, each of 56 bits (excluding parity bits). The encryption algorithm is:
Cipher text = EK3 (DK2 (EK1 (plaintext)))
i.e., DES encrypts with K1, DES decrypt with K2, then DES encrypt with K3.
Decryption is the reverse:
Plain text = DK1 (EK 2(DK3 (cipher text)))
i.e., decrypt with K3, encrypt with K2, and then decrypt with K1.
Each triple encryption encrypts one block of 64 bits of data.

5.3 *AES Algorithm*

1. Key Expansion—round keys are derived from the cipher key using Rijndael's key schedule
2. Initial Round
3. Add Round Key—each byte of the state is combined with the round key using bitwise x or

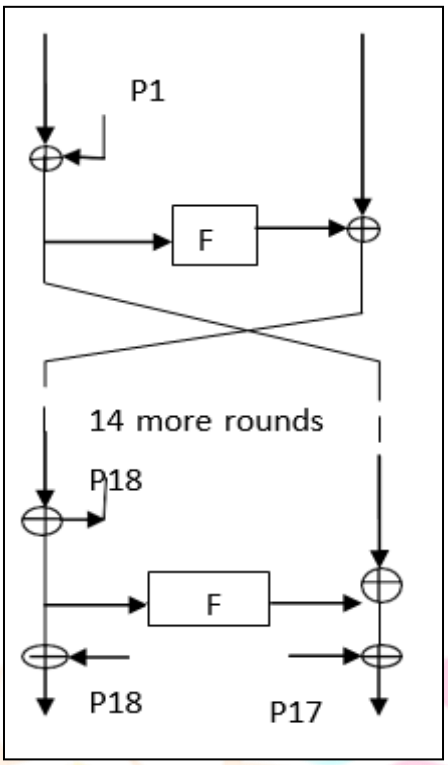

Figure 2: Feistel structure of Blowfish

4. Rounds
    1. Sub Bytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.
    2. Shift Rows—a transposition step where each row of the state is shifted cyclically a certain number of steps.
    3. Mix Columns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.
    4. Add Round Key
2. Final Round (no Mix Columns)
    1. Sub Bytes
    2. Shift Rows
    3. Add Round Key

5.4 Blowfish Algorithm

Blowfish has a 64-bitblock size and a variable key length from 1 bit up to 448 bits. It is a 16-round Feistel cipher and uses large key-dependent S-boxes. In structure it resembles CAST-128, which uses fixed S-boxes. Each line represents 32 bits. The algorithm keeps two sub key arrays: the 18-entry P- array and four 256-entry S-boxes. The S-boxes accept 8-bit input and produce 32-bit output. One entry of the P-array is used every round, and after the final round, each half of the data block is XOR ed with one of the two remaining unused P-entry.

Table 1: Specifications of encryption standards used

Algorithm name	Key size	Encoding	Padding	Initial vector size
DES ede/Triple DES	192 bits	CBC	PKCS5 Padding	64 bits
AES	128 bits	CBC	PKCS5 Padding	128 bits
Blowfish	64 bits	CBC	PKCS5 Padding	64 bits

6. ARCHITECTURE OF CIPHER CLOUD

Multi-layered architectures are must for any efficient design of a web application. To make the architecture flexible for Cipher Cloud there are five-layer designs. The design can be understood by referring to Figure 3.

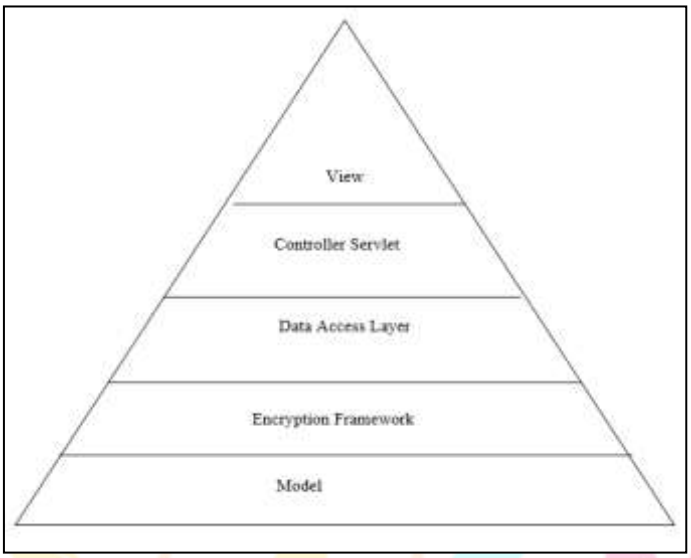

Figure 3: Layers of Cipher cloud

7. RESULTS AND DISCUSSION

The algorithm once chosen cannot be changed. First the home This will show the look and feel of Cipher Cloud and show how implanting the encryption standards have increased the security of cloud storage. In present architecture cloud is created. Then user login to the cloud with its id and password. After entering to the cloud user can see the contents of its account. In this user has following options: View files, download files, uploading files, Delete files. Once the user clicks the upload button, the file is transferred to Cipher Cloud via an encrypted connection using HTTPS and then again decrypted on the server side. After that it is again encrypted using a symmetric key algorithm chosen by the user. Once the file is uploaded and saved in encrypted form, it can then be downloaded by the user using the download button. The file received by this method will be in its decrypted form its Original form. Hence the Cloud Cipher framework can save the data in its encrypted form, and even retrieve it in its original form seamlessly and by using minimum possible CPU usage. The user is also given enough freedom to choose the encryption standard, he/she wishes to use and the framework works seamlessly with all the algorithms and standards, it supports. In case the user is new, Cipher Cloud asks for permission of the user to create a new account using the Google Account he/she had Logged in. It is on this page that the user has been offered a choice of the algorithm that he/she wishes to use for this account. The page for the cipher cloud is open. This shows the Gmail account in which this cipher cloud is resisted. In short this is the cloud in which all the processing is going to be done. After user successfully sign in to Cipher Cloud the user will be shown a link to open his/her account. The link has been highlighted in Figure 4.

Then user can upload, download the encrypted files in its account. In case the user is new, Cipher Cloud asks for permission of the user to create a new account using the Google Account he/she had logged in. It is on this page that the user has been offered a choice of the algorithm that he/she wishes to use for this account. The algorithm once chosen cannot be changed. Once the user clicks the upload button, the file is transferred to Cipher Cloud via an encrypted connection using HTTPS and then again decrypted on the server side. After that it is again encrypted using a symmetric key algorithm chosen by the user. There are three algorithms are used for the security of the data. User can choose the algorithm according to his/her choice, means choose algorithm according to its data. If message is small then RSA algorithm is used and for large message AES algorithm is better.

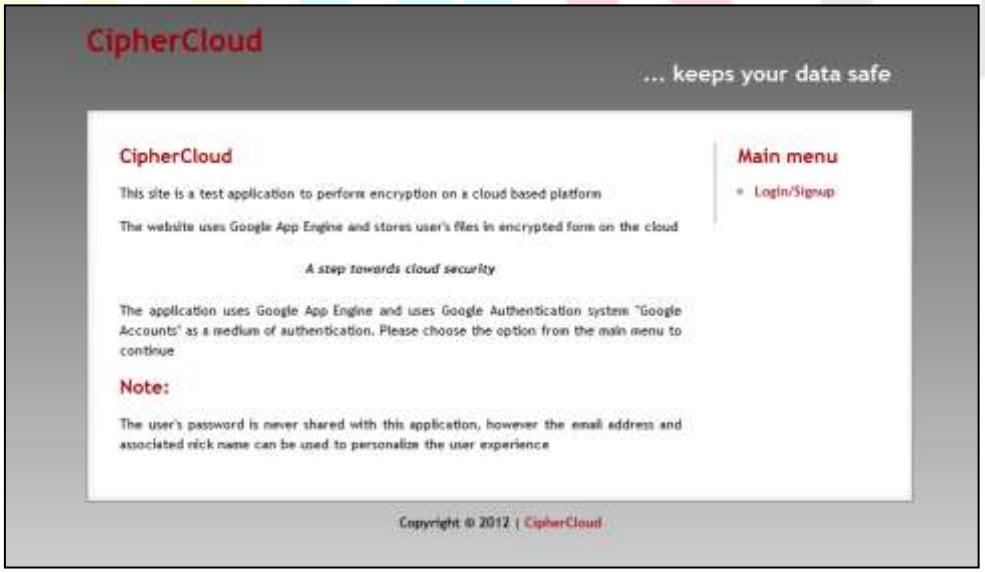

Figure 4: Home page after successfully signing in

Figure 5: New user creation

Figure 6: Uploading of a file on Cipher Cloud

8. CONCLUSION & FUTURE WORK

The investigation on confidentiality preservation and data classifications, started with a literature review. The literature view has been conducted to search all relevant scientific literature of top quality. The relevant academic and peer-reviewed information on the above topics is very limited at the time of writing. During the literature review, three concepts we are distilled that were related to the cloud computing paradigm in the form of dimensions. These dimensions relate to how data issued, where data is in relation to the data owner, and how data is protected. Each of these dimensions has been answered using the Cipher Cloud framework that has been developed. Cipher Cloud encrypts the data, making its ownership exclusive to its owner and makes it independent from the facts of where the data might be stored or who manages it. Even in cases of take over and change of ownership, only the user will be able to decrypt the given data. Additionally, the data is kept safe during transit using HTTPS TLS 1.0 standard making it difficult for anyone to sniff the data. Hence the objectives of the framework are fully achieved. Only technical privacy and encryption controls were analyzed and developed in this thesis paper. In future research on the topic of confidentiality preservation in cloud computing, the Cloud Computing Confidentiality Framework presented in this paper can be extended by adding the analysis of operational and management security controls. Such an investigation could lead to supplemental controls for limitations that might occur in cloud computing environments. As discussed in the previous section, hybrid cloud computing is a very promising cloud deployment model that can cope with the security limitations occurring in a public cloud environment, while still being able to support many of the economic advantages of public cloud computing. Hybrid clouds depend heavily on the gateway between the private part of the hybrid cloud and the public part of the hybrid cloud. The gateway between the private and public parts of a hybrid cloud is an interesting point for further research.

REFERENCES

[1] Andrzejak. 2010, Exploiting Non-Dedicated Resources for Cloud Computing, In Proceedings of 12th IEEE/IFIP Network Operations & Management Symposium (NOMS 2010), Osaka Japan.

[2] Bertino, R. Ferrini 2009, Privacy- Preserving Digital Identity Management for Cloud Computing vol.32- No.2, IEEE Data Eng. Bull.

[3] D L. Ponemon 2010, Security of Cloud Computing Users, vol. 34-No. 2, International Journal of Computer Theory and Engineering.

[4] Dawson 2002, Maximizing sharing of protected information, vol.64-No.3, Journal of Computer and System Sciences.

[5] Pieters, W. 2006, Acceptance of Voting Technology: Between Confidence and Trust. In K. Stolen (Eds.), I Trust., Computer science press.

[6] Sameer Raja 2011, Cloud Computing: The Fifth Generation of Computing, International Conference on Communication Systems and Networking.

[7] Sarathy, R, dhar, K. 2006, Secure and useful data sharing Decision Support System, vol.42-No.1, Computer Science press.

[8] Xing Zhou, Xiaofei Tang 2011, Research and Implementation of RSA Algorithm for Encryption and Decryption, Department of Computer Science and Technology Harbin, china.