Data Leakage Protection for Cloud Computing

Vansh Verma [1], Waqar Ahmad [2], Vishal Malhotra [3], and Rohan Gupta [4]

[1]B.Tech Student, Dept. Computer Science and Engineering, IMS Engineering College, Ghaziabad
[2]B.Tech Student, Dept. Computer Science and Engineering, IMS Engineering College, Ghaziabad
[3]B.Tech Student, Dept. Computer Science and Engineering, IMS Engineering College, Ghaziabad
[4]B.Tech Student, Dept. Computer Science and Engineering, IMS Engineering College, Ghaziabad

ABSTRACT

In today's virtual world, the process of sharing important data from one party to another is occurring frequently. It is necessary to ensure the security and durability of data as per users need. Generally, the sensitive data are leaked by the agents, and the specific data has to be protected at every stage. Thus, the protection of data from the distributor to agents is mandatory. This project presents a data leakage protection system using various allocation strategies and which assess the likelihood that the leaked data should not be real data that an unauthorized user accepting.

For a safe transaction of data, we will allow only authorized user to access sensitive data. And under control policies, the data should be protected through adding a fake record in the data set. This project uses the AES, DES and Blowfish algorithm to encrypt data. User can select any one of the algorithms for encryption and decryption. The project uses the three-way security model. With more advance strategies and features, we can implement this mechanism on a cloud server.

Key Words: **Data Security, AES DES and BLOWFISH Algorithm, Cloud Environment.**

1. INTRODUCTION

The company's Information security depends on employees by learning the rules through training and awareness-building sessions. However, security must go beyond employee knowledge and cover the following areas such as a physical and logical security mechanism that
is adapted to the needs of the company and to employee use than the procedure for managing updates and finally it needs an up to date documented system.

Data leakage happens every day when confidential business information such as customer or patient data, source code or design specifications, price lists, intellectual property and trade secrets, and forecast and budgets in

spreadsheets are leaked out. It leaves the company unprotected and goes outside the jurisdiction of the corporation.

This data leakage puts the business in a vulnerable position. The company is at high risk as once the data is not under the domain of the company. To address this problem, we have developed a model for assessing the guilt of agents. The distributor will intelligently give data to agents in order to improve the security by providing the corrupt file to unauthorized user as a fake file. The main aim of this project is to provide triple security to the user in the form of a combination of three different encryption algorithms – Advanced Encryption Standard, Blowfish and Data Encryption Standard. User is allowed to choose a specific algorithm for encryption purpose and the same algorithm has to be used by the user on the other hand in order to decrypt the file. Else a wrong selection of algorithm on another side will result in a corrupt file.

In this paper, we are dealing with the term data leakage when the transaction of information takes place on an online server and analyzing how the encrypting algorithms help in minimizing the data leakage problem. The study is performed as case research on Data Leakage Protection.

2. CRYPTOGRAPHY: OVERVIEW

Cryptography means “Hidden Secrets”, now-a-day concerned with encryption. Cryptography is the study of techniques for secure communication. Cryptography is used for analyzing protocols, which are related to various aspects in informationsecurity such as data confidentiality, data integrity, authentication and non-repudiation.

2.1 Cryptography Goals

We have discussed the goals behind using cryptography. They are as follow:

Authentication: It means that the data sender and data receiver must be authenticated before sending and receiving data.

Confidentiality: It means that the user who is authenticated, can only access the messages or data of other authenticated users.

Integrity: It means that the data is free from any kind of modification between sender and receiver.

Non-Repudiation: This function prevents the sender and the receiver to falsely deny that they have sent a certain message.

2.2 Symmetric and Asymmetric encryptions

There are commonly two types of techniques that are used for encrypting/decrypting the secured data i.e. Asymmetric and Symmetric encryption techniques.

2.2.1 Symmetric Encryption

In the case of Symmetric Encryption, same cryptography keys are used for encryption of plaintext and decryption of ciphertext. Symmetric key encryption is simpler and faster but their main drawback is that both the users need to transfer their keys in a secure way.

2.2.2 Asymmetric Encryption

In the case of Asymmetric encryption, two keys are used. It is also known as Public Key Cryptography (PKC) because users tend to use two keys: a public key, which is known to the public and a private key which is only known to the user.

In Asymmetric key Encryption, there are different keys that are used for encryption and decryption of data i.e. Public key and Private Key.

3.SET OF ALGORITHMS

3.1 AES Algorithm

AES algorithm is a block cipher-based algorithm with a block length of 128 bits. It uses three different key lengths: 128, 192 or 256 bits. With purposeof using a key length other than 128 bits. The main thing that brings change in AES is how you generate the key schedule from the key.

For encryption, this algorithm performs 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256- bit keys. All rounds are identical except the last round in each case. Every round has one single byte-based substitution step. It performs a row-wise permutation step, mixing step as column-wise and then performs addition of the round key. In more general sense AES algorithm uses Substitution Permutation Network. Here, each round of processing involves byte-level substitutions followed by word-level permutations. This nature of substitutions and permutations in AES allows for a fast software implementation of the algorithm.

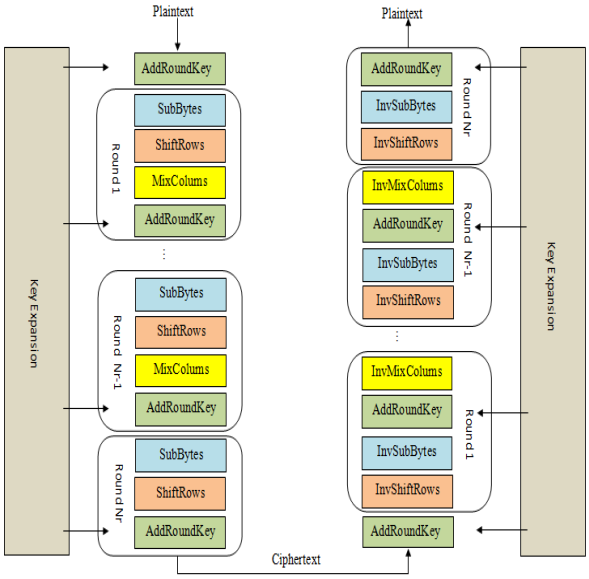

Figure: 3.1

3.2 Blowfish Algorithm

Blowfish algorithm is based on Feistel network block cipher with 64-bit block size and a variable key size up to 448 bits long. It is free to use for everyone and every situation. The number of subkeys that can be used is 18 [P-array] with number of rounds 16. Blowfish requires 4 substitution boxes each having 512 entries of 32-bits each. The entire encryption process can be shown in Fig. 3.2 as a block diagram.

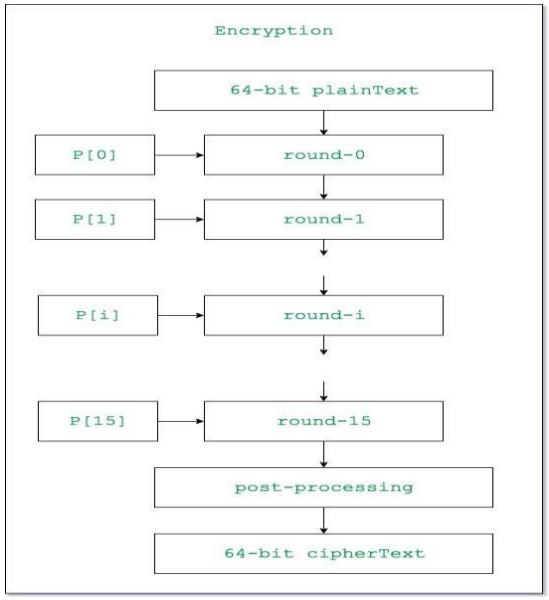

Figure: 3.2

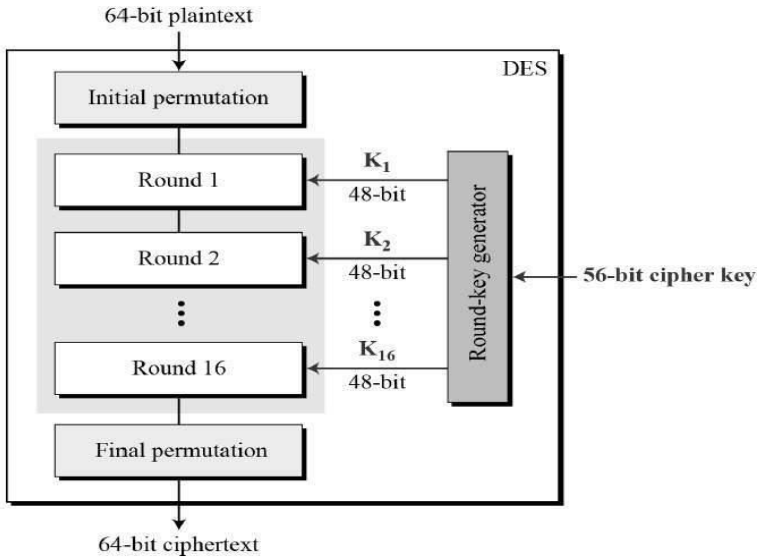

Figure: 3.3

3.3 DES Algorithm

The Data Encryption Standard (DES) is a symmetric-key block cipher algorithm based on Feistel Cipher. This Feistel structure is of 16 rounds with block size if 64 bits. DES only has an effective key length of 56 bits, as 8 of the 64 bits of the key are not used by the encryption algorithm. They work as check bits only.

The fundamental attributes of cryptography used by DES are-

- Substitution
- Transposition

4. THE CONCEPT

The project consists of three different encryption algorithms. It allows the user to select any algorithm from the given one for the purpose of encryption. As a result, the data is encrypted by the selected algorithm. As on the other hand to decrypt the data provided by the user, another user has to select the same algorithm as that of used for encryption. And by the selection of algorithm, it is necessary to fill the correct key generated by the system. If the user fails to fulfil any of the criteria then respected data will get corrupt and the user will receive an undesired data.

5. COMPARITIVE ANALYSIS

In this paper, the popular algorithms including DES, Blowfish, and AES were implemented, and their performance was compared by encrypting input files of varying contents and sizes. The algorithms were implemented in the project,

using their standard specifications, and were tested using the following parameters.

Comparision between AES,Blowfish and DES

Factors	AES	Blowfish	DES
Key Length	128, 192, or 256 bits	(k1,k2 and k3) 168 bits (k1 and k2 is same) 112bits	56 bits
Cipher Type	Symmetric block cipher	Symmetric block cipher	Symmetric block cipher
Block Size	128, 192, or 256 bits	64bits	64 bits
Developed	2000	1978	1977
Cryptanalysis resistance	Strong against differential, truncated differential, linear, interpolation and square attacks	Vulnerable to differential, Brute Force attacker could be analyze plaint text using differential cryptanalysis.	Vulnerable to differential and linear cryptanalysis; weak substitution tables
Security	Considered secure	one only weak which is Exit in DES.	Proven inadequate
Possible Keys	2^{128}, 2^{192}, or 2^{256}	2^{112} or 2^{168}	2^{56}
Possible ASCII printable character keys	95^{16}, 95^{24}, or 95^{32}	95^{14} or 95^{21}	95^{7}
Time required to check all possible keys at 50 billion keys per second**	For a 128-bit key: 5×10^{21} years	For a 112-bit key: 800 Days	For a 56-bit key: 400 Days

Figure: 5

6. RESULT

Our results revealed that AES is the better algorithm in terms of performance and security although its time consumption for encryption and decryption is on the higher side. In case of power consumption, AES has higher power consumption but it is way less than Blowfish, only DES has less power consumption than AES but on the security front, DES is the most vulnerable and can be easily broken by brute force attack is merely fifteen hours. In comparison to the Blowfish strength of a 128-bit, AES key is roughly equivalent to 2600-bits.

Through data leakage protection we can secure our sensitive data from getting leaked. Encryption algorithms use several rounds of shifting of rows, columns and mixing of columns with XORing to encrypt and decrypt data. Safety of sensitive data is important. Thus, this

research paper helps to increase the safety of data transfer and allows to store data securely on remote servers. As it is low a weighted approach to secure data more easily.

Hence, the main aim of the project is to store data securely on remote cloud servers and retrieving data only if all control policies are matched.

Encryption and decryption time in Figure: 6.1 and Figure: 6.2 respectively.

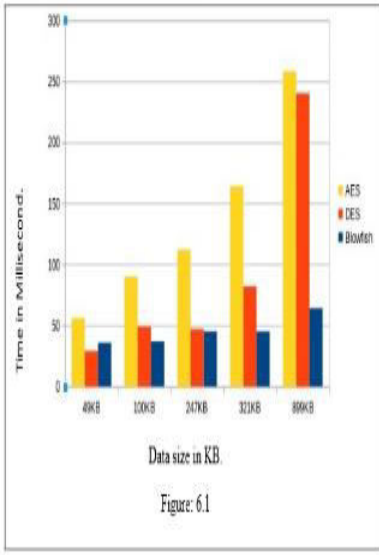

Figure: 6.1

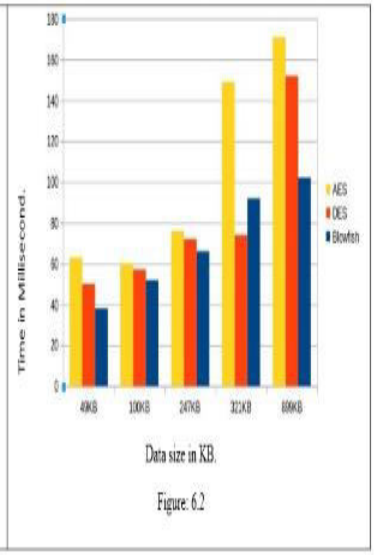

Figure: 6.2

7. CONCLUSION

The project aims to bridge the trust gap between the sender and the receiver. The methodologies used in the project encrypts data into three different forms as selected by the difficulties forms as selected by the sender. The project reduces difficulties of firms, agents and normal

users of data insecurity. In comparison to the existing systems, our project allows user to select how he/she wants to protect the data and our project is device friendly.

This system describes the design and working of a system which is useful for firms and even for the personal use to store data in a secured way for security purpose. Generally, data is secured only with the private or public key. But we are providing few extra securities for the user in the form of a selection of algorithm to encrypt data. This system converts data into different types of algorithm encrypting data is secured.

By implementation of this system, we can help firms and people who want to secure their data from third parties and want to not letting others use our data without our consent. It also reduces the risk of data leaking and storing it on remote cloud servers. It also reduces the risk of data leaking and storing it on remote cloud servers.

8. ACKNOWLEDGEMENT

The project was a great opportunity for us as senior students to evaluate our capabilities and Engineering skills, but also to apply the concepts learnt during our bachelor at IMS Engineering College to a concrete example. We would like to express my sincere gratitude to the people who helped me during my final project. First of all, we would like to thank MrSuveg Modgil who supervised us very carefully throughout our project. He was patient, comprehensive and very helpful. We are very grateful to him for sharing his knowledge with us and giving us the support that we needed. His precious advice guided us from the beginning to the end.

9. REFERENCES

[1] AviKak "AES: Advanced Encryption Standard Lecture Notes on Computer and Network Security." March 6, 2014

[2] .Xiaowei Yan, Xiaosong Zhang, Ting Chen, Hongtian Zhao and Xiaoshan Li "The Research and Design of Cloud Computing Security Framework."

[3] MehrnooshMonshizadeh, ZhengYan, Leo Hippelainen, Vikramajeet Khatri, "Cloudification and security implications of Taas", Computer Networks and Information Security (WSCNIS) 2015 World Synposium on, pp. 1-8, 2015.

[4] Omar G. Abood, Shawkat K. Guirguis, "A Survey on Cryptography Algorithms", International Journal of Scientific and Research Publications, Volume 8, Issue 7, July 2018.

[5] Ramaswamy Chandramouli, Michaela Lorga, Santosh Chokhani, "Cryptographic Key Management Issues and Challenges in Cloud Services."

[6] Sushilkumar N. Holambe, Archana U. Bhosale, Ulhas B. Shinde "The Guilt Detection Approach in Data Leakage Detection" ,International Journal of Computer Applications (0975 – 8887) Volume 119 – No.8, June 2015

[7] LekshmiR ,Sajan Xavier, FPGA Based Design of AES with Masked S-Box for Enhanced Security", International Journal of

Engineering Science Invention, Volume 3 Issue 5‖ May 2014.

[8] N.Meenakshi and G.Sasikala Department of CSE, Valliammai Engineering College, "Cloud Storage Auditing With Key Generation Using Blowfish Algorithm" International Journal of Computing Academic Research (IJCAR) ISSN 2305-9184, Volume 5.

[9] Bijayalaxmi Purohit, Pawan Prakash Singh "Data leakage analysis on cloud computing" International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 Vol. 3, Issue 3, May-Jun 2013, pp.1311-1316

[10] Youssof Mahamat Koukou, Siti Hajar Othman, Maheyzah MD Siraj, HerveNkiama "Comparitive Study of AES, Blowfish, CAST-128 and DES Encryption Algorithm" IOSR Journal of Engineering(IOSRJEN), Vol. 06, Issue 06 (June, 2016).