International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 05 | May 2019 www.irjet.net p-ISSN: 2395-0072

An Implementation of Secured Data Integrity Technique for Cloud Storage through 3DES Algorithm

Ms Amrita Nagda[1], Mr Nikhil Karale[2], Dr S.S. Dhande[3]

[1]M.E II yr, DRGITR, SGBAU University, Amravati, Maharashtra, India.
[2]Assistant Professor, DRGITR, SGBAU University, Amravati, Maharashtra, India.
[3]HOD,Dept of Computer Science & Engineering, SIPNA College, SGBAU University, Amravati, Maharashtra , India.

Abstract - *Cloud Computing is a set of IT Services, for example network, software system, storage, hardware, software, and resources and these services are provided to a customer over a network. The IT services of Cloud Computing are delivered by third party provider who owns the infrastructure. Benefits of cloud storage are easy access means access to your knowledge anyplace, anyhow, anytime, scalability, resilience, cost efficiency, and high reliability of the data. Because of these benefits each and every organization is moving its data to the cloud, means it uses the storage service provided by the cloud provider. So there is a need to protect that data against unauthorized access, modification or denial of services etc. To secure the Cloud means secure the treatments (calculations) and storage (databases hosted by the Cloud provider).In this project, we have proposed to make use of 3DES algorithm which is a well-known symmetric cryptosystem and is widely used for secure data transmission, along with that we will blend it with Random Key Generator and Graphical Password to add an extra security measure. This proposed architecture of three way mechanism and the use of symmetric method of encryption make it tough for hackers to crack the security system, thereby protecting data stored in cloud. This Cipher Block chaining system is to be secure for clients and server. The security architecture of the system is designed by using DES cipher block chaining, which eliminates the fraud that occurs today with stolen data. There is no danger of any data sent within the system being intercepted, and replaced. The system with encryption is acceptably secure, but that the level of encryption has to be stepped up, as computing power increases. Results in order to be secure the system the communication between modules is encrypted using symmetric key*.

Key Words: Cloud, Cloud Security, Cryptosystem, 3DES, Random Key Generator, Block Cipher Chaining, Symmetric Techniques.

1. INTRODUCTION

Cloud computing is an emerging computing technology that uses the internet and central remote servers to maintain data and applications. Basically cloud computing is the idea of accessing files, software and computing services through the Internet instead of on our personal computer. The primary benefits of Cloud Computing are the ability to create, update and store your files through any computer that has access to the Web. It has the ability to rent a virtual server, load software on it, turn cloud services on and off at will, or clone it ten times to meet a sudden workload demands. It can be storing and securing immense amounts of data that is only accessible by authorized applications and user. Cloud computing has the ability to use applications on the Internet that store and protect data while providing a service.

Cloud Computing moves the application software and databases to the large data centres, where the management of the data and services may not be fully trustworthy. This unique attribute, however, poses many new security challenges which have not been well understood. In this project, we focus on cloud data storage, encryption of data as well as security of the data, which has always been an important aspect of quality of service

1.1 CLOUD WITH CRYPTOGRAPHY

Whenever we save our valuable information on our phones and desktops or on our notebooks, we always get worried about the security of data. .The main aim of ours is to save that information from the third party vendor or from the

Unauthorized user. So security is the major concern which we have to keep in our mind. This is the biggest issue of today's world. To save our data on the cloud we use various techniques and cryptography is one of them. We use various cryptography algorithms to keep our data more secure from the unauthorized access. Whenever we have to send our data from one network to another network over the internet, there are so many possibilities to get our data leaked by the third party. So while sending our data to the destination from the source we simply perform two operations the first one is encryption and another one is decryption. Encryption is also used to protect our data and plays a vital role for the security of data. Encryption can be defined as a technique of securing our data from the intruders in which a plain text is converted into the cipher text and cannot be readable by them.

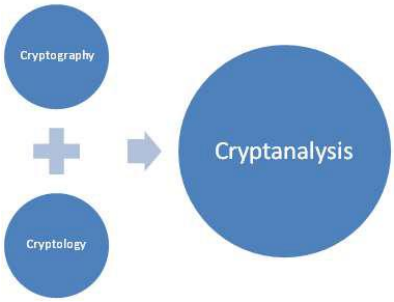

Fig -1: Cryptography

In cryptography, there are many algorithms which are used for the security of data. Cryptography can be basically divided into two parts. One of them is symmetric cryptography and an other one is asymmetric cryptography. In symmetric cryptography we only use one key for both encryption and decryption process. The algorithms used in symmetric key cryptography are AES, DES, and 3DES. On the other hand asymmetric key cryptography we use two keys one for he encryption and one for the decryption process. By using the asymmetric cryptography we can provide the authentication and nonrepudiation.The algorithms used in asymmetric key cryptography are RSA and Elliptic Curve Cryptography.

1.2 3DES

Sample 3DES is developed by IBM in 1978. It is the successor of DES algorithm which uses 168 bits key size. The key size of 3DES algorithm is 3 times bigger than the key size of DES algorithm i.e., (3*56 bits) and the block size of 3DES algorithm is 64 bits. 48 rounds are used in 3DES algorithm for the encryption process. There are three main steps are in the 3DES algorithm and which are as follows:

1.1 Encryption process is done with a key K1.

1.2 Decryption process is done with a key K2.

1.3 Encryption process is done with a key K1.

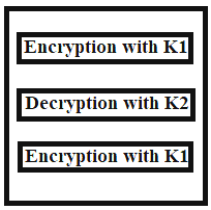

Fig -2: Steps in 3DES Algorithm

2. RELATED WORK

Juels et al. [1] described a formal ―proof of retrievability‖ (POR) model for ensuring the remote data integrity. Their scheme combines spot-checking and error-correcting code to ensure both possession and retrievability of files on archive service systems. Shacham et al. [2] built on this model and constructed a random linear function based homomorphic authenticator which enables unlimited number of queries and requires less communication overhead. Bowers et al. [3] proposed an improved framework for POR protocols that generalizes both Juels and Shacham's work. Later in their subsequent work, Bowers et al. [4] extended POR model to distributed systems.However, all these schemes are focusing on static data. The effectiveness of their schemes rests primarily on the preprocessing steps that the user conducts before outsourcing the data file F. Any change to the contents of Feven few bits, must propagate through the error-correcting code, thus introducing significant computation and communication complexity. Ateniese et al. [5] defined the ―provable data possession‖ (PDP) model for ensuring possession of file on entrusted storages. Their scheme utilized public key based homo-morphic tags for auditing the data file, thus providing public verifiability. However, their scheme requires sufficient computation overhead that can be expensive for an entire file. In their subsequent work, Ateniese et al. [6] described a PDP scheme that uses only symmetric key cryptography. This method has lower-overhead than their previous scheme and allows for block updates, deletions and appends to the stored file, which has also been supported in our work. However, their scheme focuses on single server scenario and does not address small data corruptions, leaving both the distributed scenario and data error recovery issue unexplored. Curtmola et al.

3. PROPOSED METHODOLOGY

Proposed trusted computing system model is categorized in two parts. First part describes the functions that can be performed on cloud for storage and management of files and the other part describes the security algorithm applied on the cloud to make it secure. Cryptography is the practice and study of techniques for secure communication in the presence of third parties.

Modern cryptography is heavily based on mathematical theory and computer science practice; cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in practice by any adversary. It is theoretically possible to break such a system but it is infeasible to do so by any known practical means. These schemes are therefore termed computationally secure; theoretical advances

A. Hardware and Software Requirements for Development

1.Minimum 1Gz dual core AMD BRAZO CPU or Equivalent.

2. Minimum 50 GB storage space on Hard Disk for User Storage.

3. 4 GB DDR3 RAM or Above

4. Integrated Network Adapter

5. High Speed LAN Cable

6. Windows 7 Professional or Above

7. Visual Studio 2010

8. MySQL v5.5.3

9. ODBC Connector v5.5.3

10. Heidi SQL

11. IIS Management Server

12. Microsoft Dot-Net Framework v4.0 or above

4. ACTUAL IMPLEMENTATION

We have developed a cloud storage system where a user would first have to register him on the cloud by creating an account. We have made use of symmetric key encryption for data, and for authentication of the user we make use of the technique of 2-step verification which will contain Graphical password in its second step.

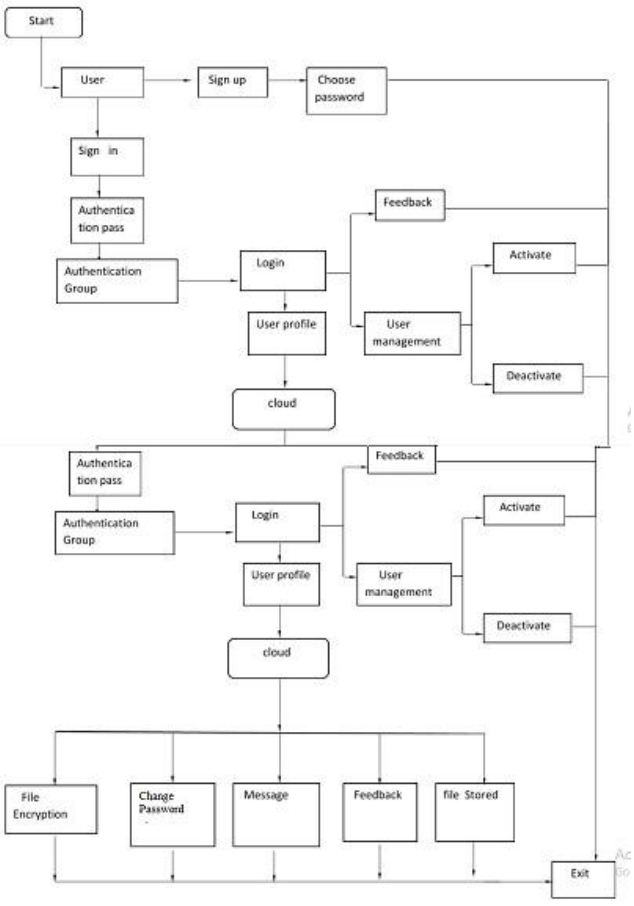

Fig- 3 : flowchart and working of project

We use the front-end as C# language to create the application while we use MySQL as back-end technique to handle the technique of data storage. We have designed the prototype model which has the desired features which we had earlier mentioned in our objectives of 2 step verification process of using a alphanumerical password in the initial stage and graphical password in the next stage for the authentication of the user.

Due to the time constraints we have managed to implement encryption algorithm on textual content only. However it is feasible to encrypt images, audio video in future.

The designed prototype will be subjected to three well know globally used penetration testing tools viz. KBG Key-Logger, Dark Comet-RAT, High Ion Orbit Canon.

The analysis will be consisting of series of test to verify the security level to which the password can be obtained using tools. We can say that the project appears as per planned however the prototype designed gives the glimpse of the implementation of our objectives. The two step verification process provides an added layer of authentication of the user by asking him to perform two task of writing password and choosing appropriate images. Using 3DES algorithm we have successfully encrypted the .txt files while other multimedia files are safeguarded by key generation policy. Also the generated key being sent on the users email id only registered users of that email id can access the key.

1) KBG Key logger Output:

Given below are the screenshots of the KGB Key logger software which was tested on our project. As shown in the screen shot the first level of password which consists of alphanumeric characters is captured by the software however, it failed to capture the next level of authentication which is graphical password. This result ensured that the KBG Key logger was unable to crack the authentication procedure of our project completely.

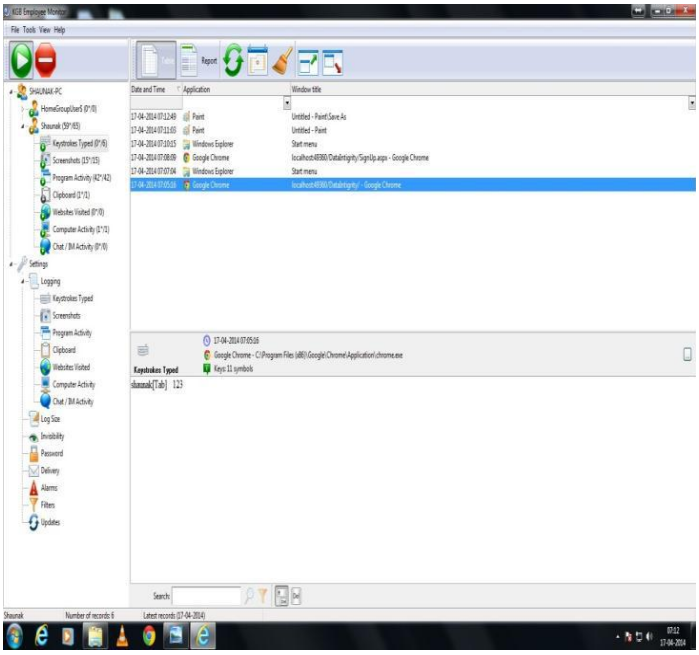

Fig-4 : Snapshot of the software tested KGB Key logger

2) 4.7.2 Dark Comet (R.A.T)

To verify that the KBG Key logger output were verified we made use of another famous Trojan Generation tool known as the Dark Comet which is the Remote Administration Tool (R.A.T). The Key logger failed to log the graphical password of the project.

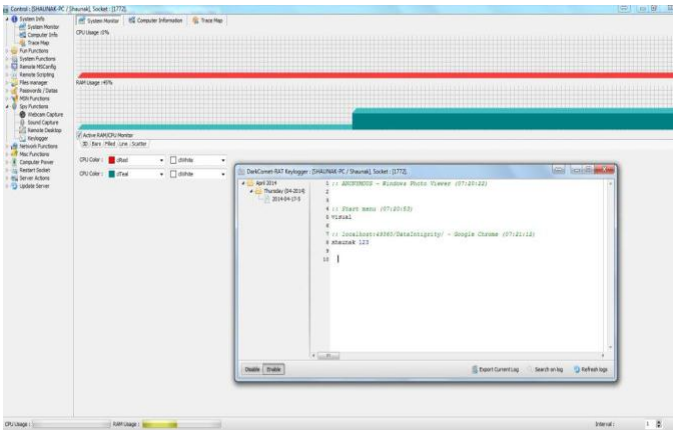

Fig-5: Snapshot of the software tested Dark Comet Key logger

However our project failed to provide security if a client has already been affected with a Trojan which has the feature of remote viewing the desktop activity. In such a scenario the graphical password can be viewed of the section of the password made.

5. CONCLUSIONS

The developed project achieved the goals of authentication and providing security on cloud storage since during our analysis the tools failed to identify the graphical password thus failing to proceed further in our project. Also we achieved data encryption during the storing of the textual data files. This ensured that the content to be safe and secure during a scenario of breach-of-data.

This concludes us in saying that the goals that were set during the development of the project have been achieved as desired and the project is ready for large scale implementation or for commercialization.

REFERENCES

[1] A. Juels and J. Burton S. Kaliski, —PORs: Proofs of Retrievability for Large Files,|| Proc. of CCS '07, pp. 584–597, 2007.

[2] H. Shacham and B. Waters, —Compact Proofs of Retrievability,|| Proc. of Asiacrypt '08, Dec. 2008.

[3] K. D. Bowers, A. Juels, and A. Oprea, —Proofs of Retrievability: Theory and implementation,|| Cryptology ePrint Archive, Report 2008/175, 2008, http://eprint.iacr.org/.

[4] K. D. Bowers, A. Juels, and A. Oprea, —HAIL: A High-Availability and Integrity Layer for Cloud Storage,|| Cryptology ePrint Archive, Report 2008/489, 2008, http://eprint.iacr.org/.

[5] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, —Provable Data Possession at Untrusted Stores,|| Proc. Of CCS '07, pp. 598–609, 2007

[6] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, —Scalable and Efficient Provable Data Possession,|| Proc. of SecureComm '08, pp. 1

[7] Mrunalini Motilal Shete, Pragati Damodar Hipparkar, "Data Secure in Cloud Computing Using Encryption Algorithms ",International Journal of Science and research (IJSR), Volume 4 Issue 3, pp- 1497-1499, March 2015.

[8]. Rohit Bore, Dr. Rahila Sheikh, "International Journal of

Computer Science and Network", Volume 5, pp-171-176,

February 2016.

[9]. Dr. S. S. Manikandasaran, "Security Attacks and Cryptography Solutions for Data Stored in Public Cloud Storage",International Journal of Computer Science and

Information Technology & Security (IJCSITS), Vol.6, pp- 498-503, Jan-Feb 2016.

[10]. Shaunak S.Ganorkar:" An Information Security Scheme for Cloud based Environment using 3DES Encryption Algorithm", International Journal of Recent Development in Engineering and Technology (ijrdet) (ISSN 2347 – 6435) (Online) Volume 2, Issue 4, April 2014