Volume 4, Issue 10, October 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Novel System to Enhance Cloud Data Security

Shekhar Anand, Poonam Ingale, Mehul Pande, Keshav Gangopalwd

Computer Department, Pune University,

Pune, India

Abstract— Cloud computing, even though known to have a malicious behaviour, is an environment which enables convenient, efficient, and ready to use on demand network access to a pool of shared data resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud is basically a centralized database where the clients or the organisation store their data, retrieve data and possibly modify the data. To overcome challenges from cloud security, many state-of-the-art technical solutions, e.g., continuation protection mechanism, IDM, data security, and virtualization security have been adopted but due lack of users loss control of data dynamic operations on cloud have not been implemented. Varieties of Algorithms have been referred before this literature and the system is proposed to ensure that the data transfer between client and cloud is made secure.

Keywords— Cloud Computing, Data Security, Asymmetric key generation, Advanced Encryption Standard (AES), Session Layer

I. INTRODUCTION

What is Cloud Computing? Going literally by the word cloud, it denotes enormous unending space. Actually the word "cloud" is a synonym used for the "Internet", so cloud computing in that sense means "Internet-computing". Actually cloud computing is a service provided over the internet to the customer on a leased basis. All that the customer requires to avail these services is an internet connection. The customer can use the enormous storage space of the cloud to store his applications and can use them on-a-go. However there are some security issues related to Cloud Computing which is why the customers are reluctant to use these services. The customer stores his important data on the cloud and so if the security is not optimum, he will obviously be thinking twice before saving any of his data on the cloud. In today's age Cloud Computing has come a long way from being just a brilliant concept to one of the fastest growing technologies. But as more and more individual as well as company data is being stored on the cloud, concerns have started growing about the security the cloud can provide. As we discussed earlier, customers are still very hesitant about storing their data on the cloud. In fact security issues are placed at the first position in the "challenges list" of Cloud Computing. The customers are reluctant because there's a sense of lack of control over the data they store on the cloud. The customer's data, their applications and all the other resources are with the third-party provider. So there's a loss of control over their data once it is stored in the cloud. So as the customers no longer possess their own data, security measures cannot be adopted at the customer's side directly.

II. RELATED WORKS

Authentication has always been the first line of defence. The application must determine if the user is who he/she claims to be or if the entity, a server or program, is what it claims to be. This is the "I recognize who you are." stage. The most common form of authentication is the user id and password. Many new and upcoming websites and applications struggle to provide security to their users. We as a third party will be able to meet their needs and help them out. All they need will be to just download our software and install it on their Operating Systems. The scheme could achieve the integration of storage correctness insurance and data error localization, i.e., whenever data corruption has been detected during the storage correctness verification across the distributed servers, Could almost guarantee the simultaneous identification of the misbehaving server(s) through detailed security and performance analysis. John Harauz, described the Security Content automation protocol (SCAP) and benefits it can provide with latest cloud computing paradigm with reference to the latest report released by NIST, giving insight as to what SCAP is trying to do, It states that many tools for system security, such as patch management and vulnerability management software, use proprietary formats, International Journal of Computer Applications. Balachandra Reddy, described some of the security issues that have to be included in Service Level Agreement (SLA), SLA is a document which defines the relationship between service provider and the recipient, typical Service level agreement contents includes Definition of services, Performance management, Problem Management, Security, Disaster recovery, proper termination of transaction also they have stated a methodology to standardize SLA.

III. SYSTEM APPROACH

For the cloud security system, there are three important modules: firstly user, one who is going to store huge amount of data on cloud. Data stored on cloud needs to be secured from unauthorized access. Secondly Trusted Third Party (TPA-

Third party auditor), which will be used for accessing the cloud storage service. And Cloud server, which provides storage space and resources. Cloud server is handled by administrator of the organization. User can access data stored on cloud. In order to do that, trusted third party helps to reduce the burden of online user authentication and save resources.

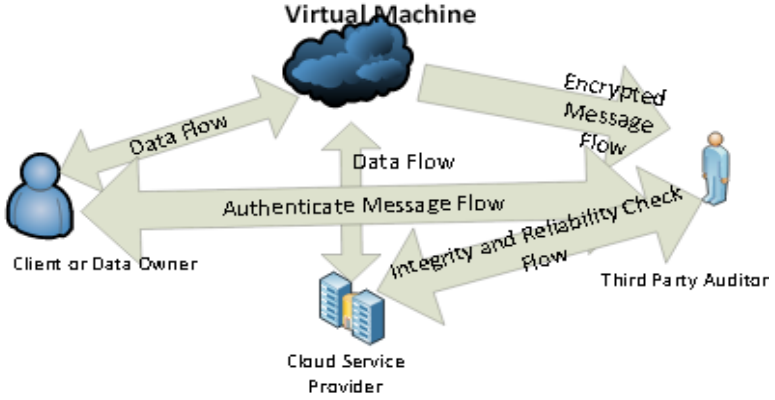

Figure 1: System Architecture

Design Goals:

1. Ensuring the correct storage of data on cloud.
2. Ensuring no retrieval information of client in process by TPA.
3. Allowing TPA for verification of data in order to reduce resources.

IV. IMPLEMENTATION

Client requests service to server and Server grants the request through a response. Client has to first

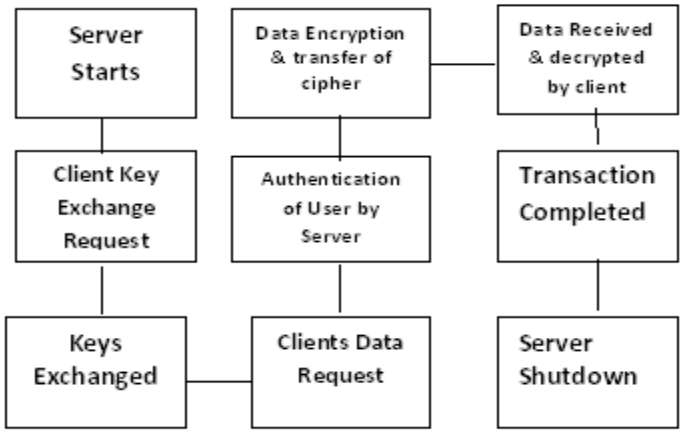

Figure 2: System Flow

register himself in the server to begin with. Server stores the password and client is registered. Then at the time of login, Username and password are verified, welcome message is prompted. Client sends a request to server; server creates a key and forwards it to the corresponding client for its use in encryption and or decryption. Client request for data which is encrypted by the server and then sent to it. Client later decrypts it to obtain the plaintext.

Module 1

This proposed system can be mainly divided into two parts: Server and Client

This project is mainly depended on client/server model. The client requests the server and server responses by granting the clients request. The proposed system should provide both of the above features along with the followed ones:

a) Server - The server should be able to perform the following features:

The first and foremost problem is to find the server. We should identify the program in the server which processes the client's request. Authentication of users' generation of keys encryption of data files

b) Client: The client should be able to perform the following features: authenticate itself from server request for keys decrypt data files

Module 2

This module involves testing the users for their authenticity by carrying out username and password verifications. There maybe two type of clients logging on to the server:

1. New Users
2. Existing Users

New Users shall give a required username and password which will be added to the database on the server side. Existing users shall verify their identity by providing their unique username and password. Once authenticated they can run the next module which provides the keys to clients.

Module 3

This module handles key generation by the server side. The server generates unique keys for users once they authenticate themselves with the server. The key is generated using instances of AES key generator class. This key is then transferred to the client via the LAN connection which receives and stores a copy for it for decrypting purpose. The key is a 16 byte or a 128 bit key.

Module 4

Once the keys are exchanged, the client requests for a data file to be transferred to it. The server then encrypts the data file with AES algorithm explained below and sends the cipher text to the client. In cryptography, the Advanced Encryption Standard (AES) is a symmetric-key encryption standard. Each of these ciphers has a 128-bit block size, with key sizes of 128, 192 and 256 bits, respectively. The AES ciphers have been analysed extensively and are now used worldwide, as was the case with its predecessor, the Data Encryption Standard (DES). The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plaintext into the final output of cipher text. Each round consists of several processing steps, including one that depends on the encryption key. A set of reverse rounds are applied to transform cipher text back into the original plaintext using the same encryption key.

Module 5

Client After the keys are received and the cipher text is sent to the client by the user, the client uses the reverse process of the AES encryption .AES decryption to obtain the original plaintext that was transferred by the server. Hence the client receives the intended file in a secure manner over the LAN.

V. CONCLUSION

After this proposed system, we can conclude that the process of the securing the data is now easy and that it helps not only the user but also the organization in reducing the time spend on the system or waiting for the response. In this approach, the future work will be mostly done developing the system for multiple users and with added greater security The TPA will not have any idea about the data which is being shared.

REFERENCES

[1] Mandal Pratap Chandra, "Superiority of Blowfish Algorithm" IJARCSSE, volume 2, Issue 9, September 2012, pp. 196-201.

[2] M. A. Shah, M. Baker, J. C. Mogul, and R. Swaminathan," Auditing to keep online storage services honest," in *Proc. Of HotOS'07*. Berkeley, CA, USA: USENIX Association, 2007, pp.1–6.

[3] Sujit Tilak, Dipti Patil "A Survey of Various Scheduling Algorithms in Cloud Environment "International Journal of Engineering Inventions Volume 1, (September 2012) PP: 36-39.

[4] Stallings William, "Cryptography and Network Security Principles and Practice", Fifth Edition, Pearson Education, Prentice Hall, 2011.

[5] Thakur Jawahar, Kumar Nagesh. "DES, AES and Blowfish Symmetric Key Cryptography algorithm Simulation Based Performance Analysis", IJETAE, vol. 1, Issue 2, DEC. 2011, pp. 6-12.

[6] (2002) The IEEE website. [Online]. Available: http://www.ieee.org/

