ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 3, March 2015

Security in Cloud using Implicit Security Model and OTP

Akanksha Rana

M.Tech Student, Computer Science Department, Galgotias University, India

Abstract: Cloud computing is considered to be one of the burning topic nowadays. Some of its excellent features attracts the confidence of the users but at the same time some of its uncertainties results in lack of faith of user. This survey paper gives a brief review of implicit security techniques, used in cloud computing. Traditionally explicit techniques are used in cloud computing but storing the data implicitly may provide more secure and balanced storage of data.

Keyword:Cloud Computing, Explicit Security, Implicit Security, OTP

I. INTRODUCTION

Cloud computing is in great demand today. It shifts the burden of securing and storing data from client side to server side. Users can simply store their data on servers and now it's the job of the servers to ensure integrity, confidentiality etc. of the data available with them. The excellence of the cloud storage services lies in the fact that it avoids the costly expenses on software, and maintenance. Apart from this, there are many other advantages that can be taken into concern while thinking of cloud computing. But dealing with data in such an open environment, which is prone to many attacks it sometimes is not an easy task. This survey discuss over existing cloud storage frameworks and helps to identify the potential areas to be worked upon in order to increase reliability of the storage techniques in cloud. The main focus in on implicit security mechanisms used to store data over multiple servers by partitioning it and OTP is used to tighten the security framework.

Why Implicit Security Model?

Past researches done in the area of cloud security has mainly focused on securing the communication of the information. But securing the storage of the information has been overlooked. Traditionally explicit techniques are used to secure data on servers. A data is stored and backed up on a single server. Data is secured by passwords and user may access data by providing the same. Disadvantages of this technique is that

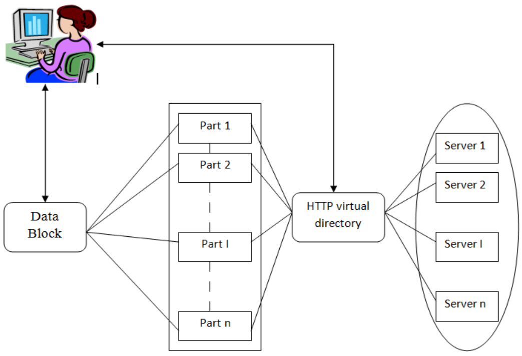
- Brute force attacks are very common on passwords.
- It's never a good option to store a complete data at a server because if in any case the attacker managed to surpass the imposed security mechanisms then complete data will be easily accessed.

In such scenario, implicit security techniques may be proved to be beneficial .The data is partitioned into pieces and the partitions are stored over multiple servers. The main advantage of this technique is that there is no need to encrypt the data because these partitioned pieces will not provide any information to the attacker. Original data can be reconstructed from these partitioned pieces or subset of these pieces whenever user wants to access complete data.[1][2]

Possible variations in the Implicit Security Model

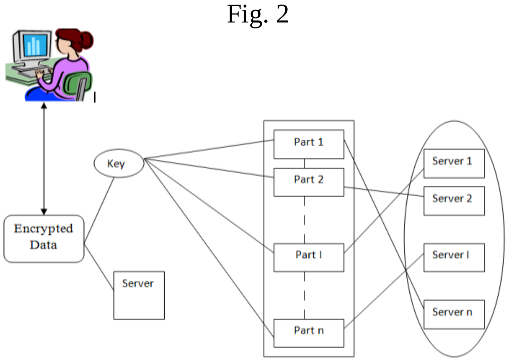
Implicit techniques are mainly used with two variations that depends on the size of the data to be stored online. If the size of data to be stored on server is small, then the data may be simply partitioned into n pieces and then stored over multiple servers.[2]

Fig. 1



If the size of data to be stored on server is large, and it becomes quite tough to deal with large partitions then the data may be first encrypted and the key is partitioned into n pieces and then stored over multiple servers.

Fig. 2



DOI 10.17148/IJARCCE.2015.43133

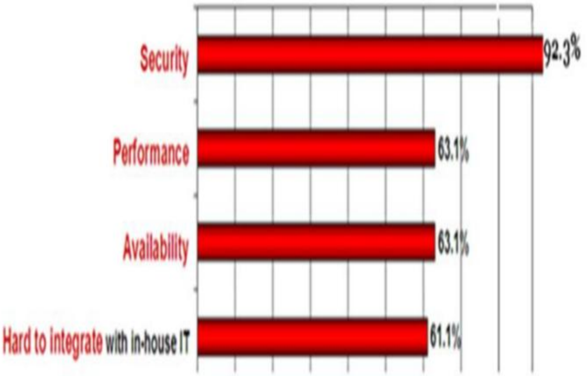
II. SECURITY IN IMPLICIT MODEL

In modern era, security is major issue to secure any information. A data partitioning scheme is proposed for online data storage that involves the finite field polynomial root [3]. The partitioned pieces are stored on randomly chosen servers. In order to access the partitioned data, the user must have knowledge of the password and servers on which the pieces are stored. This information is mentioned in the HTTP virtual directory. The partitioned pieces do not contain any complete information and thus they are implicitly secure. The original data from the partitioned pieces can be reconstructed whenever desired by the user [4]. This will enable better load balancing as it will be easy for servers to manage and store small partitioned pieces of data [5].

III. RELATED WORK AND SOLUTION

Implicit security techniques are new to cloud computing and are vulnerable to many attacks. These techniques simply provides services to the cloud by introducing new methods for partitioning the user's data and storing it in various other servers but it can be made more secure if some existing security techniques can be used along with them. OTP (One Time Password) can be thought of such a solution that may pave a way towards using implicit techniques in a more reliable way. Reason behind focusing mainly on security is the following figure.

Fig. 3



Source: IDC Enterprise Panel, January 2012

There are many reasons which favors the use of OTP in cloud computing. [6]. There are various algorithms that may be used to generate a new One Time Password that may be mailed to the user and then the user may get access to data only when the OTP is entered. After using OTP once, it will not be of any use for next time and again a new OTP is mailed to the user [7]

IV. PROPOSED MODEL

The proposed model is as follows:

i. First of all user will be asked to enter his mobile number.

ii. An OTP will be sent to his mobile no. and he can proceed only after entering that OTP.

iii. If he enters correct OTP, he will be able to proceed and a login page will appear that will ask for user's id and password.

iv. Only after he enters correct id and password, he will be able to get access to his data.

v. Various phases are included in this proposed model such as registration and login phase, that will be done in the traditional manner [8]

vi.

V. CONCLUSION

The proposed technique may be proved useful in terms of security as well as it will save bandwidth of network as using OTP prior to login page will ensure legitimacy of the user to a great extent and further login page will serve the security purpose.

REFERENCE

[1] HOW TO SHARE A SECRET: Communications of the ACM, Volume 22 –No. 11 November 1979. (Adi Shamir)

[2] ONLINE DATA STORAGE USING IMPLICIT SECURITY: journal in information sciences 179(2009)3323-3331. (Abhishek parakh, Subhash kak).

[3] A SURVEY ON SECURE STORAGE IN CLOUD COMPUTING: Indian Journal of Science and Technology, Volume 6 –No. 4, April 2013 (A. Rajathi and N. Saravanan).

[4] IMPLICIT SECURITY ARCHITECTURE FRAMEWORK IN CLOUD COMPUTING BASED ON DATA PARTITIONING AND SECURITY KEY DISTRIBUTION: International Journal of Emerging Technologies in Computational and Applied Sciences, Volume.3- No.1,February.2013 (S.Hemalatha, Dr.R.Manicka Chezian)

[5] EFFICIENT DISPERSAL OF INFORMATION FOR SECURITY, LOAD BALANCING, AND FAULT TOLERANCE: Journal of the Association for Computing Machinery. Vol. 36-No. 2, April 1989, pp. 335-348. (Michael O. Rabin)

[6] AN APPROACH TOWARDS SECURITY IN PRIVATE CLOUD USING OTP: International Journal of Emerging Technology and Advanced Engineering, Volume 3, Issue 3, March 2013 (Vishal Paranjape, Vimmi Pandey)

[7] ONE TIME PASSWORD SYSTEM FOR SECURITY OVER CLOUD: International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 7, July 2014 (Neha Sharma, Kiran Gautam , Praveen Nagar)

[8] SECURING THE CLOUD ENVIRONMENT USING OTP: International Journal of Scientific Research in Computer Science and Engineering, Volume 1, Issue 4, 30 June 2013 (Vimmi Pandey).

DOI 10.17148/IJARCCE.2015.43133