Security Approaches and Implementation for Data Protection over Cloud

Amit Wadhwa
Assistant Professor
Department of Computer Science and Engineering
Amity University Haryana, India

Abstract: In Cloud Computing domain data and its protection is a sensitive matter of concern as data is available with the third party cloud vendor. Over the years many algorithms have been proposed to cater to the problem of sensitive data and its protection and still solutions are coming in form of different approaches employed to find an effective solution to the problem. In earlier works related to this MLBAAC model has been presented catering to some of the issues of data security and sensitive data protection. This paper focuses on discussing and detailing the approaches used to handle the issue of data protection and specifically sensitive data protection of users over cloud. Further in addition to that, this paper discusses the actual implementation and design of the system used in MLBAAC[5][7] model for implementation of such approaches.

***Keywords* – Cloud Computing, Data Protection, Sensitive Data, Cryptography**

I. INTRODUCTION

Cloud computing and its security has been a major concern and focus area for users over the years. As the data is with cloud administrators so trust has always been an issue for cloud users as sensitivity of the information varies across users using cloud for data storage[1,2][3].

Many security algorithms have been proposed in recent time and implemented to prevent attacks to critical or non-critical data, to provide trust among cloud users. Although the need for more effective and suitable techniques to handle data related attacks have always been open for researchers to work out. Access control is also needed to be done for the purpose of controlling the access to user data[4][6][8]. Malicious users attack by making unauthorized access to cloud storage, thereby accessing important user data leading to losses for the organizations and even damaging the reputation of stakeholders in the organization. This problem results into affecting or decreasing the customer base and trust also. Another problem arising out of this situation is related to data sharing among cloud users[4]. Sharing of data has been the most discussed and worked out operation among cloud users working in an organization[4][5].

Cloud users think about the concerns regarding storage space provision and privacy of its data present over cloud platform. Storage data over a cloud often provoke the malicious attackers to attack such system with vulnerabilities. They attack by making unauthorized access to cloud storage, accessing confidential data leading.[4][5]

This situation requires the CSP's (i.e. Cloud Service Providers) providing solutions so that these type of situations and vulnerabilities can be prevented[4]. There are some applications in the market like dropbox which uses various security algorithms like SHA, DES, AES etc to secure their data [2][4]. But to make this situation work trust should be established among data owners cloud providers. Apart from this the location to store data files is not provisioned to be specified by cloud service user. So, the main solution used generally for data protection in this type of scenario is important data files encryption and moving them to storage servers on cloud environment[2].

Problem arising out of this situation is related to data sharing among CSU's. Data sharing is one of the most common operation among cloud users associated with an organization[4]. So, problem with encrypted data present over cloud is as storage is done after encrypting the information which requires sharing of decryption keys [2],[9] it possess a security threat to the system.

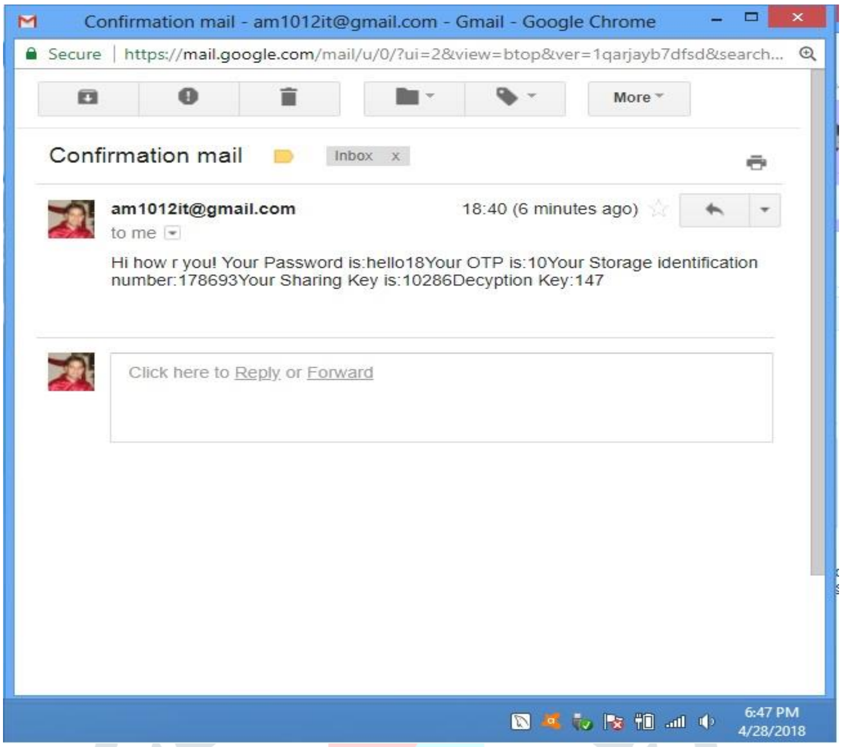
Another approach of preventing attackers invading the cloud platform security to affect the cloud service user's (CSU) data[5] is by providing low intensity honey traps or pots using technique of implementing some fake servers to deviate attacker from original production server[5]. This problem was catered to in the previous approaches worked out. Implementing a fake server over the network to prevent attacks over cloud is a costly solution in terms of the resources required to make it feasible by CSP [10] (cloud service provider)[11,12]. So, this opens a channel for providing some low interaction and less resource requiring honey pots to be deployed over cloud[5]. This paper works on the requirements of data protection mechanism using various approaches.

II. APPROACHES FOR CLOUD DATA SECURITY

Over the years many different approaches have been laid down by researchers for providing protection to data over cloud. These approaches work on different principles from using cryptography, securing network by providing restricted access etc. Still there is need to discover more techniques as attackers in network are keep on mending different ways to bypass any sort of layer in an network to access restricted or confidential data of users. Many different techniques have been presented by researchers over the past like:

(a) Digital Signature using SHA and AES

For securing cloud users data a model working on this technique have been implemented in the past named as "MLBAAC"[4][5][7], as per that in order to secure data over cloud a mix of both digital signature[13][14] with SHA and AES cryptographic algorithms [10] could be used. Implementation for the model suggest that it provided a successful way as employing security using the approach requires sub security procedures implemented as multiple levels of security represented in form of single and multi brakers[5][7] used to share different portions of the key required to access users data over cloud. MLBAAC[7] model implementing such approach provides a mechanism for sharing the service access key and other information with user over registered email id and the information shared as per implemented model as shown in Figure 1 here:


Confirmation mail - am1012it@gmail.com - Gmail - Google Chrome
Secure
https://mail.google.com/mail/u/0/?ui=2&view=btop&ver=1qarjayb7dfsd&search...
More
Inbox x
6:47 PM
4/28/2018

Confirmation mail

am1012it@gmail.com 18:40 (6 minutes ago)

to me

Hi how r you! Your Password is:hello18Your OTP is:10Your Storage identification number:178693Your Sharing Key is:10286Decyption Key:147

Click here to Reply or Forward

Figure 1: Service access key part 1 and other shared information

(b) Sensitive Data protection using Extension Changing Approach

Data over cloud storage could be categorized into various categories as per the sensitivity of the information or as per user who is storing the data over cloud storage or using the system. As per the general categorization of information two categories could be sensitive and non sensitive information [15]. For non sensitive information or less critical one any basic or less secure mechanisms could be employed for providing security but in order to secure critical or highly sensitive data one needs to find out secure ways of protection.

So in response to that requirement for securing cloud users critical or sensitive data a technique for changing the extension of files have been proposed as extended part of MLBAAC [5] , [7] model. This technique uses various steps used to provide implementation for sensitive data protection over cloud. As part of the initial step, the system provides a mechanism for the user to add or insert data files over his reserved cloud storage. Next step is, to access the storage area user will be asked to provide storage access key initially shared with him during registration process over email as storage identification number. As next step user needs to provide the correct pass key with which user would be able to insert and download his critical data files from its cloud storage area. The interface for the same is as shown in Figure 2 here:

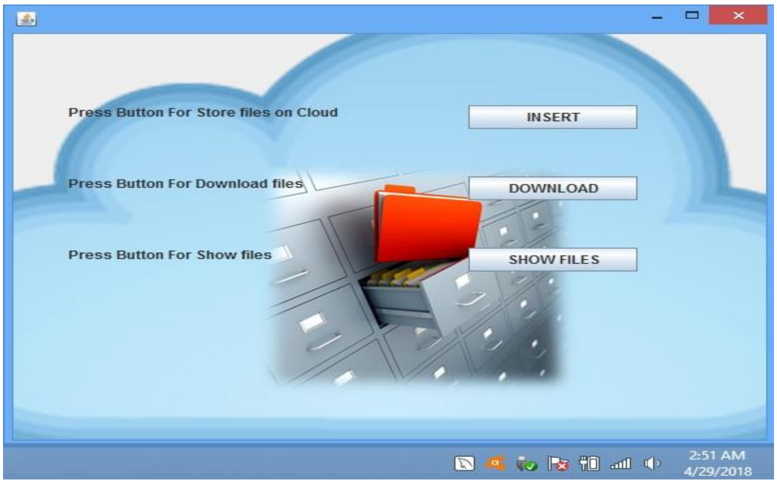

Press Button For Store files on Cloud
INSERT
Press Button For Download files
DOWNLOAD
Press Button For Show files
SHOW FILES
2:51 AM
4/29/2018

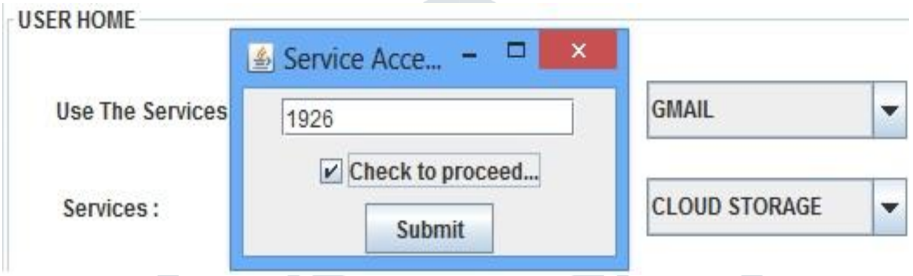
Figure 2: Interface Providing access to User's Cloud Area

This interface as shown in Figure 2 gives user three options as: first with a button supporting insertion of users critical data files over cloud storage, second using button to download these data files and further third using a button to associate correct extensions with files after downloading them on its local storage for access. Even if the critical data file of a user is accessed by malicious insider[16,17] by some means the extension would never be correct and that would prevent attacker to misuse the data as correct extension could only be associated with data file from user's protected cloud storage area by pressing show files button as shown in Figure 2.

(c) Data Protection using Honey Pots and Their Implementation

Another approach used in the literature is to prevent attacks using honey pots over cloud. As part of the technique the malicious attacker could be prevented from unauthorized access to cloud users data using honey pots which would be actually different duplicate preventive server implemented to disguise the attacker so as to protect actual data server[18,19].

Over the years many techniques were presented by researchers to deploy such honey pots but most of them are based on using expensive servers depicting as actual data servers so that attacker could not get access to original data. But in MLBAAC model [4],[5],[7] implementation system a less expensive technique was proposed to provide honey pot implementation[20] which proved to be less expensive and useful. It uses an alarm mechanism which would be raised and run in background as someone tries to access the information which he is not authorized to access otherwise. In order to simulate such mechanism an approach is designed and implemented using the interface shown here in Figure 3:



1926

☑ Check to proceed...

GMAIL

CLOUD STORAGE

Figure 3: Service Access Key insertion - Activating Honey Pot

In this Figure 3, to access the services of a cloud user, he needs to punch in the service access key as 1926 and as he checks the option saying "Check to proceed…" and presses submit button, a alarm would be raised internally in the system and current user would be moved to the honey pot system containing some bogus data or service interface so attacker could not differentiate or guess as his attack was successful and he is able to bypass the security later or not.

III. CONCLUSION AND FUTURE DIRECTIONS

In this paper various approaches used for implementation of security system have been discussed and implementation for the same have been detailed using the implementation scenarios as per given figures. The main focus was on the techniques implemented as part of the MLBAAC [5], [7] model whose practical implementation have been presented in our earlier work. Further the techniques discussed were implemented successfully using an interface designed along with implementation performed on CloudSim[16] framework. As per the simulations carried out in this respect the implemented model shoes the effectiveness of the system. In future one could predict the usage of this system to provide extensive security in different phases of cloud applications.

REFERENCES

[1] U. Somani, K. Lakhani, and M. Mundra, M. Implementing digital signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Computing. First International Conference On Parallel, Distributed and Grid Computing (PDGC 2010), Solan, India, pp. 211-216

[2] D. Singh and H. K. Verma, "A new framework for cloud storage confidentiality to ensure information security," in *Symposium on Colossal Data Analysis and Networking (CDAN)*, Indore, 2016.

[3] R. Kaur and R. P. Singh, "Enhanced Cloud Computing Security and Integrity Verification via Novel Encryption Techniques," in *International Conference on Advances in Computing,Communications and Informatics (ICACCI)*, Greater Noida, 2014.

[4] Amit Wadhwa , "Proposed Technique for Securing Critical Data Over Cloud," *Journal of Emerging Technologies and Innovative Research*, vol. 5, no. 5, pp. 592-595, 2018.

[5] Amit Wadhwa and V. K. Gupta, "Practical Implementation and Analysis of MLBAAC Model for Cloud," *International Journal of Computer Engineering & Technology*, vol. 9, no. 3, pp. 14-22, 2018.

[6] G. P. Kanna,, and V. Vasudevan, Enhancing the security of user data using the keyword encryption and hybrid cryptographic algorithm in cloud. International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), Chennai, India, 2016, pp. 3688-3693

[7] Amit Wadhwa and V. K. Gupta, "Proposed Framework with Comparative Analysis of Access Control & Authentication based Security Models Employed over Cloud," *International Journal of Applied Engineering Research*, pp. 15715-15722, 2017.

[8] S. Vishnupriya, P. Saranya, and A. Rajasri, Secure multicloud storage with policy based access control and cooperative provable data possession. International Conference on Information Communication and Embedded Systems (ICICES2014), Chennai, India, 2014

[9] Patil, D. H., Bhavsar, R. R., and Thorve, A. S. Data Security over Cloud. IJCA Proceedings on Emerging Trends in Computer Science and Information Technology (ETCSIT2012), 2012, pp. 11-14

[10] Amit Wadhwa , "Comprehensive Analysis of Security Issues and Solutions While Migrating to Cloud Environment," *International Journal of New Innovations in Engineering and Technology*, vol. 4, no. 4, pp. 127-130, 2016.

[11] R. Charanya, and M. Aramudhan, Survey on access control issues in cloud computing. International Conference on Emerging Trends in Engineering, Technology and Science (ICETETS), Pudukkottai, India, 2016, pp. 1-4

[12] S. Sajithabanu and E. G. Prakash Raj, "Data Storage Security in Cloud," *International Journal of Computer Science and Technology*, vol. 2, no. 4, pp. 436-440, 2011.

[13] Moghaddam, F. F., Karimi, O., and Hajivali, M. Applying a single sign-on algorithm based on cloud computing concepts for SaaS applications. IEEE 11th Malaysia International Conference on Communications (MICC), Kuala Lumpur, 2013, pp. 335-339

[14] Gadhavi, L., Bhavsar, M., Bhatnagar, M., and Vasoya, S. Design of efficient algorithm for secured key exchange over Cloud Computing. 6th International Conference - Cloud System and Big Data Engineering (Confluence), Noida, India, 2016, pp. 180-187

[15] Amit Wadhwa and V. K. Gupta, "Framework for User Authenticity and Access Control Security over a Cloud," *International Journal on Computer Science and Engineering*, vol. 06, no. 04, pp. 138-141, 2014.

[16] R. Buyya, "CloudSim: A Framework For Modeling And Simulation Of Cloud Computing Infrastructures And Services," The Cloud Computing and Distributed Systems (CLOUDS) Laboratory. [Online]. [Accessed 18 May 2018]

[17] V. Nirmala, R. K. Sivanandhan and R. S. Lakshmi, "Data confidentiality and integrity verification using user authenticator scheme in cloud," in *International Conference on Green High Performance Computing (ICGHPC)*, Nagercoil, 2013.

[18] G. Raj and S. Setia, "Effective Cost Mechanism for Cloudlet Retransmission and Prioritized VM Scheduling Mechanism over Broker Virtual Machine Communication Framework," *International Journal on Cloud Computing: Services and Architecture (IJCCSA)*, vol. 2, no. 3, pp. 41-50, 2012.

[19] V. Khedekar, G. Mane, S. Khanvilkar and S. Karade, "Study of Cloud Setup for College Campus," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 2, no. 10, pp. 251-255, 2012.

[20] N. Jose and C. K. A, "Data Security Model Enhancement In Cloud Environment," *IOSR Journal of Computer Engineering*, vol. 10, no. 2, pp. 01-06, 2013.