INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

GRAPHICAL PASSWORD AND DATA SLICING: NEW TECHNIQUES FOR DATA SECURITY IN CLOUD COMPUTING

ASHWINI G. RAUT[1], PROF. C. M. MANKAR[2]

1. ME (Fourth Semester), Computer Engineering, SSGMCE Shegaon, Sant Gadge Baba Amravati University.
2. Computer Science & Engineering, SSGMCE Shegaon, Sant Gadge Baba Amravati University.

Accepted Date: 15/03/2016; Published Date: 01/05/2016

Abstract: Cloud computing allows us to create, configure, and customize applications online. Cloud computing promises lower costs, rapid scaling, easier maintenance, and service availability anywhere, anytime, a key challenge is how to ensure and build confidence that the cloud can handle user data securely. As cloud providers have priority access to data, so it is difficult to guarantee the confidentiality and integrity of user's data. Many multinational organizations are interested in cloud computing and its wonderful features but they are worried about the security, privacy and availability of data as it rest in the cloud. For this reason this paper proposed a model to solve the problem of data security in cloud computing. The model adopts efficient data division mechanisms to protect user's data. This model suite provides security of data using encryption, logging with key management, Third Party Auditor technology and Graphical Password technology. In this paper we explore data protection as a service as a suite of security primitives offered by a cloud platform, which enforces data security and privacy and offers evidence of privacy to data owners, even in the presence of potentially compromised or malicious applications and the slicing as a new technique for privacy preserving data security given here. Slicing has several advantages when compared with general data saving techniques such as CSV file. It preserves better data utility than general techniques of packet delivery ratio, throughput, normalized routing load, delay and control overhead.

Keywords: Cloud Computing, Data security, Encryption, Graphical Password, Key Management, Slicing, Third Party Auditor, CSV file.

Corresponding Author: MS. ASHWINI G. RAUT

Access Online On:

www.ijpret.com

How to Cite This Article:

Ashwini G. Raut, IJPRET, 2016; Volume 4 (9): 126-132

PAPER-QR CODE

1. INTRODUCTION

As cloud providers have priority access to data, so it is difficult to guarantee the confidentiality and integrity of user's data. Cloud computing promises lower costs, rapid scaling, easier maintenance, and services that are available anywhere, anytime. A key challenge in moving to the cloud is to ensure and build confidence that user data is handled securely in the cloud. For this reason this paper proposed a model to solve the problem of data security in cloud computing. The model adopts efficient security mechanisms to protect user's data. Experimental results show that the model can better ensure data confidentiality and integrity.

On the other hand, user data protection while enabling rich computation is challenging. It requires specialized expertise and a lot of resources to build, which may not be readily available to most application developers. The most common method used for authentication is textual password. The vulnerabilities of this method like eavesdropping, dictionary attack, social engineering and shoulder surfing are well known. Random and lengthy passwords can make the system secure. But the main problem is the difficulty of remembering those passwords. Studies have shown that users tend to pick short passwords or passwords that are easy to remember. Unfortunately, these passwords can be easily guessed or cracked. The alternative techniques are graphical passwords and biometrics. But these two techniques have their own disadvantages. Biometrics, such as finger prints, iris scan or facial recognition have been introduced but not yet widely adopted. The major drawback of this approach is that such systems can be expensive and the identification process can be slow [5].

Many organizations have implemented encryption for data security, they often overlook inherent weaknesses in key management, access control, and monitoring of data access. If encryption keys are not sufficiently protected, they are vulnerable to theft by malicious hackers. Vulnerability also lies in the access control model; thus, if keys are appropriately protected but access is not sufficiently controlled or robust, malicious or compromised personnel can attempt to access sensitive data by assuming the identity of an authorized user [2].

Proposed system

We use a new cloud computing paradigm, data protection as a service (DPaaS) is a suite of security primitives offered by a cloud platform, which enforces data security and privacy and offers evidence of privacy to data owners, even in the presence of potentially compromised or malicious applications.

Secure data techniques using logging, key management, graphical password authentication, Slicing of data which is stored by user and is sliced into different data tables, for this slicing algorithm which divides data from comma separated value that is CSV file which is a xls file containing user's data on first basic work that is slicing for privacy preserving data security is used here. My contribution includes the following. First, introduction of slicing as a new technique for privacy preserving data security given here. Slicing has several advantages when compared with general data saving techniques. It preserves better data utility than general techniques.

With Slicing and key authentications we used Graphical password authentication. Slicing can slice data stored and uploaded in cloud by user for which user as well as admin can generate challenge and check integrity of uploaded data, for user and admin we provide Key or better say an alphanumeric password technique, to make it more advance and secure graphical password technique also provided for more securely logging into account [4].

There are many graphical password schemes that are proposed in the last decade. But most of them suffer from shoulder surfing which is becoming quite a big problem. There are graphical passwords schemes that have been proposed which are resistant to shoulder-surfing but they have their own drawbacks like usability issues or taking more time for user to login or having tolerance levels. Personal Digital Assistants are being used by the people to store their personal and confidential information like passwords and PIN numbers. Authentication should be provided for the usage of these devices. For user and admin login it is necessary to give a strong protected password options which helps to keep data secure in the database saved by user and checked through administrative department. Slicing concept will work in background and after slicing the CSV file which we use as an example to show the concept will work in cloud, it save it in two different tables. Third party auditor has capabilities that users do not have and it is trusted to assess and expose risk of cloud storage services on behalf of the users upon request. Cloud service provider is always online and assumed to have abundant storage capacity and computation power. The third party auditor is invariably online too. It makes every data access to be in control.

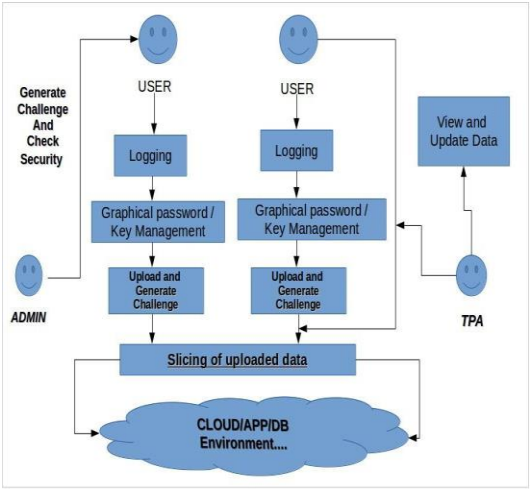

Figure 1: Workflow of the Model

2. MATERIALS AND METHODS

2.1 CSV file

A CSV file is a text file that has a specific format which allows for the saving of textual information/data in an organized fashion. The format, known as a flat table, is very simple. Each row (paragraph) contains one record of information; each record can contain multiple pieces of data (fields) each separated by a character. The character used to distinguish each piece of data within each record is most commonly a comma, but can be any character

2.2 TPA (Third Party Auditor)

The auditor is one who audits the overall performance of the system. He can track the transactions and logins of users with correct time and date. Here auditor is software that is capable of tracking the transactions. Cloud storage offers movement of data into cloud. For well organization of data it is very essential that cloud that allows checking from a single party, audit the outsource data to ensure the data security and save the user's computation and data storage. It is very important to provide public auditing service for cloud data storage, so that the user trust an independent third party auditor (TPA).TPA checks the integrity of data on the cloud on the behalf of the users, and it provides the way for the users to check the validity of data in the cloud.

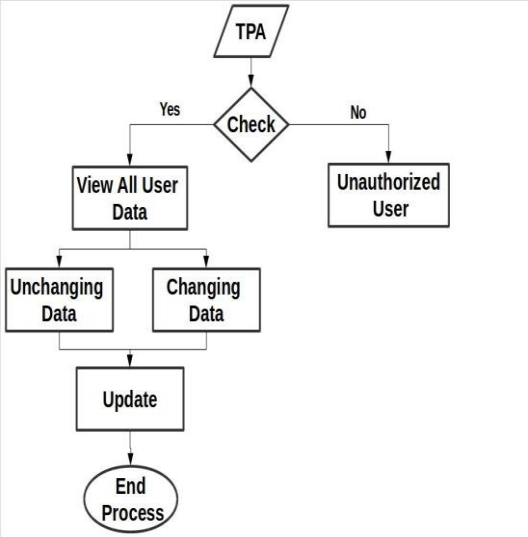

Figure 2: TPA model

2.3 Slicing of a data

This technique partitions the data both horizontally and vertically. We show that slicing preserves better data utility than generalization and can be used for membership disclosure protection. Another important advantage of slicing is that it can handle high-dimensional data. We show how slicing can be used for attribute disclosure protection and develop an efficient algorithm for computing the sliced data that obey the ℓ-diversity requirement. Our workload experiments confirm that slicing preserves better utility than generalization and is more effective than bucketization in workloads involving the sensitive attribute[4].

2.4 Graphical Password

Graphical password is one of the solutions. A graphical password is an authentication system that works by having the user select from images, in a specific order, presented in a graphical user interface (GUI)[11]. For this reason, the graphical password approach is sometimes called graphical user authentication (GUA).

2.5 Encryption

Here the concept of AES is used for more security. I used the High level Design for key management .The concept of key come from the branch of science called cryptography. There are basically two types of keys.

- Public key
- Private key

A public key known to everyone and a private or secret key known only to the recipient of the message. When X wants to send a secure message to Y, X uses Y's public key to encrypt the message. Y then uses X's private key to decrypt it. In this system I encrypt the file using a key and stored in the cloud. The user should enter the key to decrypt the file. So multiple protection mechanisms are used here for protecting the files in the cloud.

3. RESULTS AND DISCUSSION

More advantages for individual users to store their data redundantly across multiple physical servers so as to reduce the data integrity and availability threats. Thus,

Distributed protocols for storage correctness assurance will be of most importance in achieving robust and secure cloud storage systems.

4. CONCLUSION AND FUTURE SCOPE

4.1 Conclusion

Many of cloud users think that cloud is secure and easier. However, most of the IT experts feel that the cloud has lots of problems in the field of data security and privacy issues towards the growth of cloud computing. No user will transfer their data to the cloud until the trust is built between the cloud service providers and consumers. The main contribution in this project is a new approach of data security solution, which contains slicing of data and graphical password verification for authentication purpose. The trusted third party provides security services, secures user data and made more intractable which is important and can be used as reference for designing the complete security solution. It allows the clients to verify the integrity of the data stored on download or retrieval of its own stored data in cloud. The client can store the data securely without any overhead of key management [8].

4.2 Future Scope

In cloud, the data security idea can enhance with a third party auditor to verify the cloud server that stores the users data on cloud. The slicing of data will be applied to all the files existing in the cloud. The TPA concept will be more system dependent and graphical password can be used with more secured features which helps to:

- To enhance the security more, a mechanism to secure the keys in security cloud can be a area of research.
- To reduce the overhead of network traffic can be another area of research.

5. REFERENCES

1. Dawn Song, Elaine Shi, Ian Fischer, and Umesh Shankar. ”Cloud data protection for the masses". IEEE Transactions in Computer Society, 45(1):39-45, 2012.
2. Derek Tumulak. “Data security in the cloud protecting business-critical information in public, private, and hybrid cloud environments". Gartner Inc. Worldwide Cloud Services Market Is Expected to Surpass 2012, pages 01-04, 2012.
3. IBM Corporation.”Cloud-based data protection services for managed service providers". pages 01-07, 2012.
4. Tiancheng Li, Ninghui Li, Jian Zhang, and I. Molloy. “Slicing: A new approach for privacy preserving data publishing ". IEEE Transactions on Knowledge and Data Engineering, 24(3):561-574, 2012.
5. Ashwini G. Raut and prof. C.M. Mankar. “Unassailable and streamlined operations to provide data protection in cloud computing”. International Journal of pure & applied research in engineering & technology, pages 183– 187, 2014.
6. Hakan Hacigumus, Bala Iyer, Chen Li, and Sharad Melhrotra. “Executing sql over encrypted data in the database-service-provider model". pages 216-227, 2002.
7. A. Juels and B. A. Kaliski Jr. “Proofs of retrievability for large files". Proc of the 14th Conf on Computer and Communications Security (CCSO7), pages 136-149,2010.
8. S. Kamara and K. Lauter. “Cryptographic cloud storage". LNCS Fina.Cryp. and Data Sec, pages 584-597, 2007.
9. Sunumol Cherian and Kavitha Murukezhan. “Providing data protection as a service in cloud computing ". 3(6):01-05, 2013.
10. Jin Li, Qian Wang, Cong Wang, and Ning Cao. “Fuzzy keyword search over encrypted data in cloud computing ". IEEE Transactions on INFOCOM, 2010, 3,2010.
11. Ms. Sneha Vasant Thakare and Ms. Dipali V. Gore. “3d security cloud computing using graphical password". Int. Journal of Adv. Rese.in Comp. and Commun.Eng. 2(1):945-949, 2013.