International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-2, Issue-7)

Research Article

July 2013

Graphics Based Cloud Security

Ankush Narkhede*, Dr. Pankaj Dashore, Prof Dhanraj Verma
Dept. of CSE
Oriental University Indore, India

Abstract:

In this article, I focus on cloud secure data storage, which has always been an important aspect of quality of service (QOS). "Cloud computing may be the only way to handle vast, unstable query loads differentiated data in any number of formats and with any number of relationships" Data Security is considered as major aspect in cloud environment while using an application. This Data security can be implemented with respect to user authentication and authorization using cryptography system. Data security involves encrypting the data as well as ensuring that appropriate policies are enforced for data sharing. In this way, Data security becomes more and more important in cloud computing.

Keywords— Security, Cloud, Graphical, Authentication and Encryption

I. INTRODUCTION

In this topic I will general overview about how to provide cloud "Cloud computing is a compilation of existing techniques and technologies, packaged within a new infrastructure paradigm that offers improved scalability, elasticity, business agility, faster start-up time, reduced management costs, and just-in-time availability of resources". Generally, in the text-based password, the password is easy to guessing the others user. The one user is easily find out the password of second user and easily login her\his account. So, there is the need to finding the more secure password and to generate the graphical password. Graphical secrets present lots of advantages and can increase the level of security without a significant change in the user's habits. For that, we need to possess strong ways to convert them into strings that will feed the implemented passwords systems. Cloud computing is a computing model, where resources such as computing power, storage, network and software are abstracted and provided as services on the internet in a remotely accessible fashion. User authentication plays important role in securing cloud as it is done before both processes either storing data or retrieving data.

II. LITERATURE SURVEY

There are different techniques to provide authentication. The text-Based password flaws in the aspects of usability and security issues that bring problems to users. Hence, there is a need for alternative mechanism to overcome these problems. The difficulty in remembering the text Based password. To overcome this problem, we need the graphical password system. Passwords that are easily remembered for example pet's name, first name and street address. Unfortunately, these passwords can be easily guessed or broken. According to an article in Computerworld, the security team at a large company tested and ran a network password cracker and surprisingly within 30 seconds, they manage to crack approximately 80% of the passwords. Pictures are generally easier to be remembered or recognized than text, especially photos, which are even easier to be remembered than random pictures. In user description of the concept an image would appear on the screen, and the user would click on a few chosen regions of it. If the correct regions were clicked in, the user would be authenticated. Efficiency is important in password systems because users want to have quick access to systems.

III. PROPOSED METHODOLOGY OF ENSURING CLOUD SECURITY

Cloud is a computing model providing web-based software, middleware, computing resources on-demand, and capabilities of Information Technology (e.g. applications, storages, communication, virtualization, collaboration, and infrastructure). That derives cloud computing environments to the software that runs in virtual appliances that can be used to assemble applications in minimal time. Its service has ubiquitous access through a web browser or mobile device with APIs or special desktop applications developed by cloud service provider. Cloud computing now provides organizations with new ways to organize and maintain applications allowing for greater flexibility and reduce complexity. Fully understanding the range of potential cloud computing benefits requires a broad perspective that recognizes that real computing resource optimization aligns computing capabilities with business needs. So, in addition to uptime, organizations can now achieve agility, integration, scalability, accelerated deployment, better utilization, and transparent cost accounting. Cloud computing promises to increase the velocity with which applications are organized, increase innovation, and lower costs, all while increasing business agility.

Cloud computing environment are multi domain environment. Among which different domain can use security, privacy and trust requirements in a different manner. So as far as cloud computing is newly idea developing, security has made commercial Internet possible. Cloud can be secured only when proper user authentication can be done. Till today many technologies had been used to provide user authentication. [1]Different biometrics are used to provide security. It consists of three cloud including customer relationship management (CRM) , storage cloud service and separate

decryption/encryption cloud service. These entire components plays different role during data retrieval and data storage process. A proposed three tier cloud architecture is explained below:

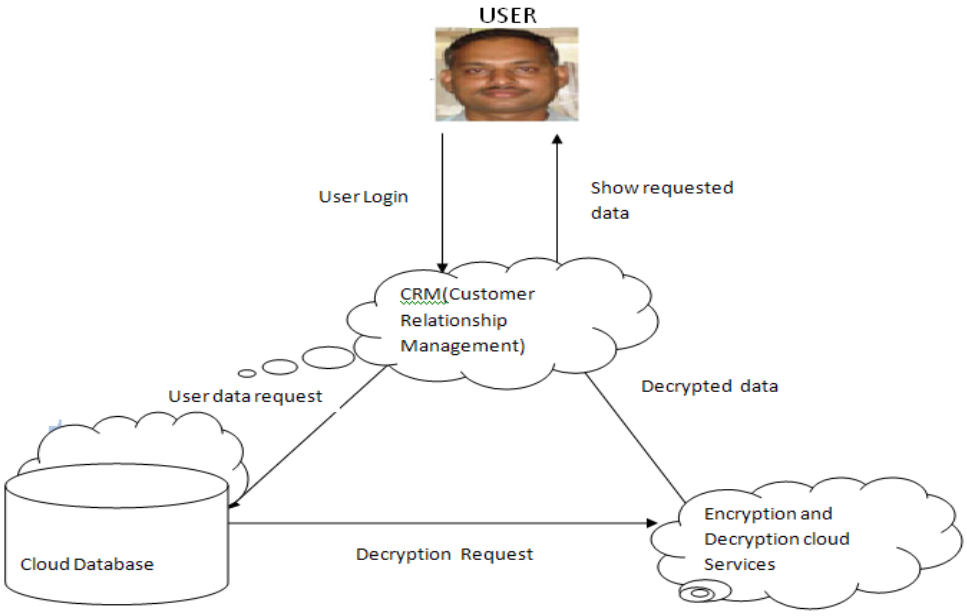

Fig 1: A Three tier Cloud Architecture

Encryption and decryption of data can be done to maintain data confidentiality. Beyond of all these things CRM plays most important role. If user is authorized then only he can store or retrieve data from cloud database. We proposed that authentication can be provided by using graphics keys. The image is combination of pixels arranged according to fixed dimension. In this methodology, each pixel has equal importance.

Password can be generated by arranging sequence of pixel. After this overall process completes at that time, the encryption or decryption service must delete all encrypted and decrypted user data. In addition to this, data storage and decryption of user data works independently. This means that those working with data storage cloud system will have no access to decrypted user data. In short here we are just dividing and separating the encryption or decryption cloud service from the storage as service. For enhancing the security and privacy in an organization, the concept of dividing authority is applied in business management.

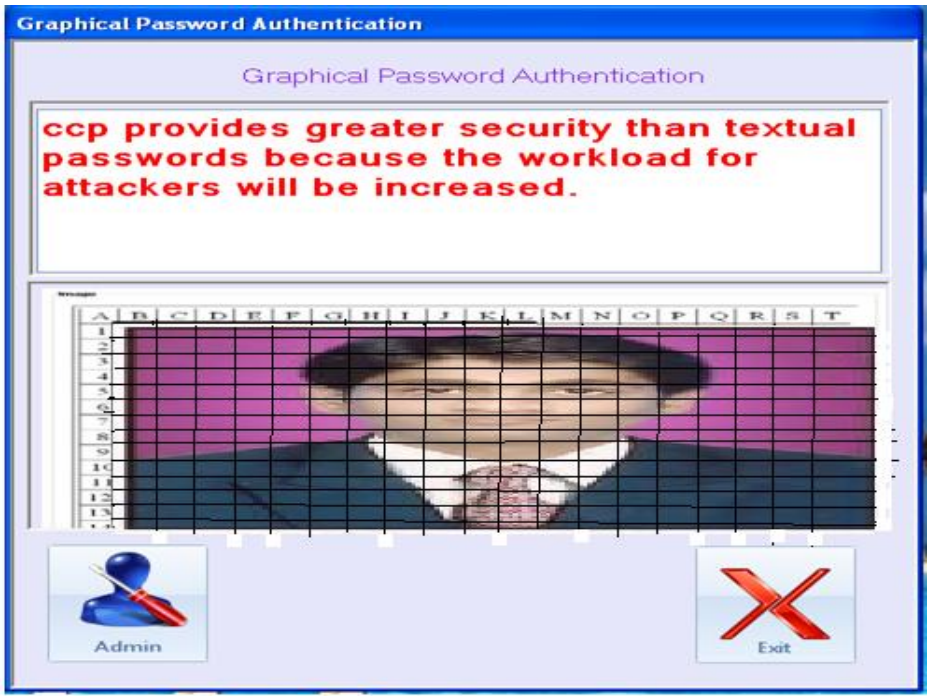

Fig 2: Graphical Password Authentication

If the user had decided to provide access to some of the operator of an organization to decrypt the data while some of them will work on storage service only. So, it's up to user for deciding the concept of dividing the authority. Consider an example of motor garage system organization, the user will supposed to divide the authority in the billing department as one of the factor named as, accountant operator and another factor is cashier.

Due to this, the accountant is responsible for keeping records and making billing of various Motors while cashier is responsible for making payment to the customer. So, by keeping the two sections separately the company prevents from fraud if an accountant makes any. Because as accountant has authority of making billing section only and not to provide payments to the customer and the employee. This example of division of authority is design to avoid the operational risk factor. In cloud computing environment the user ties to uses effective and efficient services provided by the cloud with some of specific function. Data generated while using these services is then stored on the storage cloud service. This study related to the business model provides division as per the responsibility for data storages and data encryption or decryption. In cloud computing, Customer relationship management application can be replaced with some other services ex.ERP cloud service, account software cloud services etc. In this manner these three clouds can put separately for insuring security. The interesting point is that the SaaS provider the dose not stored the unencrypted user data.[4,5,6] This ensure security and privacy to the user and reduces discloses of the data. Because when the user requests for encrypt or decrypt of the data to the encryption or decryption as service, and when all this process conversion completes and then handled it CRM application. After this overall process completes at that time, the encryption or decryption service must delete all encrypted and decrypted user data. In addition to this, data storage and decryption of user data works independently. This means that those working with data storage cloud system will have no access to decrypted user data. In short here we are just dividing and separating the encryption or decryption cloud service from the storage as service. For enhancing the security and privacy in an organization, the concept of dividing authority is applied in business management. If the user had decided to provide access to some of the operator of an organization to decrypt the data while some of them will work on storage service only. So, it's up to user for deciding the concept of dividing the authority.

A. Access to data for data retrieval system

Data retrieval system consists of following steps:

- To access data from cloud database, user authentication is must. So firstly authentication of user can be done.
- After authentication process, CRM cloud accept any kind of request from user to process further. Every user associated has its own identity.This identity plays unique role during data retrieval system.
- Then CRM sends request to cloud storage ,where user data is present in encrypted form. Decryption of required data takes place to fulfill the user requirement because user cannot read data in encrypted format.

B. Appropriate access to data for data storage system

The data storage system methodology is exactly opposite to the data retrieval. Here this process is also conducted in three main steps.

- To store data in cloud database, user verification is must. Unless and until user verification is confirmed the CRM cloud service will not proceed further. After successfully login the user will firstly send the request for storing data to be stored to the CRM system.
- Then CRM will forward the user request to the Encryption and Decryption cloud services. Presently data is in decrypted form. So in encryption and decryption cloud services, conversion of decrypted data gets into encrypted form takes place. The user identity is very important while encrypting or decrypting the data as there are multiple users accessing the service. The encryption and decryption cloud service had no authority to store the data either in the encrypted form or decrypted form on the same cloud service. So this cloud automatically deletes the data after sending it to its proper designation. This will increase the data security. After data send to the Storage Cloud Service, here the data is stored in the encrypted form along with the user Id. This will help in future to identify and differentiate among the data of multiple users.
- Finally this Storage Cloud Service Provider will send request to user that the data is stored in the encrypted form. After sending confirmed request of data stored in the encrypted form to user then only the Encryption and Decryption Cloud Services will delete the data which is stored there as on temporary process for encrypting or decrypting data for completing the data storage process will delete the data. This would help in reduce the risk factor of getting data hacked due to some unauthorized persons. Thus the data storage process is completed successfully.

IV. CONCLUSION

To ensure the correctness of user's data in cloud data storage, We proposed an effective and flexible graphics based password. We believe that data storage security in Cloud Computing, an area full of challenges and of paramount importance, is still in its infancy now, and many research problems are yet to be identified. There are several security challenges including security aspects. There believes that due to the complexity of the cloud, it will be difficult to achieve end-to-end security. So security issues for cloud are important. These issues include storage security, data security, network security and application security. The main goal is to securely store and manage data that is not controlled by the owner of the data. Then there is focused on specific aspects of cloud computing. This kind of structured

security will also be able to improve customer satisfaction to a great extent and will attract more investors in this cloud computation concept for industrial as well as future research farms.

REFERENCES

[1] M. Christodorescu, R. Sailer, D. L. Schales, D. Sgandurra, D. Zamboni. Cloud Security is not (just) Virtualization Security, CCSW'09, Nov. 13, 2009, Chicago, Illinois, USA.

[2] L. Litty and D. Lie. Manitou: a layer-below approach to fighting malware. In ASID '06: Proc. of the 1st workshop on Achitectural and system support for improving gsoftware dependability, pages 6-11, New York, NY, USA, 2006. ACM.

[3] B.D. Payne, M. Carbone, M. Sharif, and W. Lee. Lares: An architecture for secure active monitoring using virtualization. Security and Privacy, IEEE Symposium on, 0:233-247, 2008..

[4] M. A. Rahaman, A. Schaad, and M. Rits. Towards secure SOAP message exchange in a SOA. In SWS '06: Proceedings of the 3rd ACM workshop on Secure Web Services, pages 77–84, New York, NY, USA, 2006. ACM Press.

[5] Meiko Jenson, Jorg Schwenk, Nils Gruschka, Luigi Lo Iacono. On Technical Security Issues in Cloud Computing. IEEE International Conference on Cloud Computing 2009. [8] D. Kormann and A. Rubin, ―Risks of the passport single sign on protocol,‖ Computer Networks, vol. 33, no. 1–6, pp. 51–58, 2000.

[6] Nilesh N. Kumbhar, Virendrasingh V. Chaudhari, Mohit A.Badhe "The Comprehensive Approach for Data Security in Cloud Computing: A Survey" International Journal of Computer Applications (0975 – 8887) Volume 39– No.18, February 2012 23