Advanced Identity & Access Management Mechanisms for Cloud Computing

Himanshu V. Taiwade¹, Dr. Prakash S. Prasad², Ashish S. Sambare³, Ketan D. Bodhe⁴

¹Department of Computer Technology, PIET, Nagpur, India
Email: himanshu.taiwade@gmail.com
²H.O.D, Department of Computer Science & Engineering, PIET, Nagpur, India
Email: prakashprasada56@gmail.com
³H.O.D, Department of Computer Technology, PIET, Nagpur, India
Email: ashishsambare@gmail.com
⁴Department of Computer Technology, PIET, Nagpur, India
Email: ketanbodhe@gmail.com

Abstract—Cloud based services and always increasing popularity of related services is not new to anyone but neither are any security related threats that exits with them. There are many countermeasures which are introduced with the purpose of minimizing the threats; it is still found that security breaches are always imminent. It is observed that emphasis has been extensively given to the security of Cloud services; the outcome is still not satisfying.

In this paper we present advanced Identity & Access Management Mechanisms for Cloud Computing that generates high level of security for Clients as well as an encryption technique to further improvises the existing structure its clients.


I. INTRODUCTION

The recent success of cloud based services and its ever increasing popularity are not unknown to anyone and neither are the security threats which persist in parallel with its growth. Cloud computing has the potential to change how organizations manage information technology and transform the economics of hardware and software at the same time. Introduction of Cloud initially promised it’s users to help the new entrepreneurs by helping them start their new ventures without any investment. But this was not the case and as the things progressed, security concerns also went up. Possibility of a secure cloud computing scenario that to especially for public cloud is now overshadowed because of the security breaches [5].

There have been number of countermeasures which are introduced for minimizing threats; but there are regularly security breaches occurring at large. We can consider some difficulties of clients who wish to access services of cloud; for that they should have browser on their system. In this case we can discuss about attacks made on clouds that make data insecure on these systems but there are many more attacks also that can affect the data. Many approaches are proposed for the solution that through a cloud storage server. The sender here needs the basic information like identity of the receiver. The receiver also needs to possess few more things which are his/her own secret key stored in the computer and a unique personal security device which can easily be used to connect to the computer [1]. Some of the other basic preliminary overview is confidentiality, accountability, revocation, secure access control, and collision resistance of the data [2].

Another threat is related to the Identity and access management which looms at large. It is always very difficult to manage multiple numbers of accounts for customers and that to when the user can leave the organization and their account remains active. This case increases risk of data exposure that can lead to the Identity and access related problems especially in SaaS [7]. In the past the cloud services that faced security breach was never expected to come down due to security concerns. Consumers should try and make sure that the contract which they want to sign should always be able to serve the need of security which should be considered as a main factor [6]. It is a bit difficult to manage number of accounts of customers and especially when a user leaves the organization then in that case their account can remain active that increases the risk of data exposure that can lead to Identity and access related problems [8]. It can be hence said that to have a secure Cloud, important objectives are needed which are still be totally achieved.
II. SOLUTIONS AND LIMITATIONS

The problem of malicious insider in the cloud infrastructure which is also the core of cloud computing is illustrated and explained that IaaS cloud providers can provide its users with multiple sets of virtual machines from which the user can be benefitted as they can run their software’s on them. To ensure data confidentiality using data encryption is not sufficient because of the fact that user’s data requires to be manipulated with the help of virtual machines and it not easily possible if the data is encrypted [18]. In addition, it is always assumed that if the data is processed while being accessed by different clients, data privacy cannot be assured in the cloud.

Some other solutions are also available for the users with a motive to protect different types of security threats such as Data confidentiality where Data is encrypted by the data owner before uploading to cloud. Fine-grained access control that provides secure accessibility to the resources. Scalability, User revocation is other method where if any user wants to quit the system, then the system revokes access rights and then the user has no access to his data. The performance of the system is not affected if the number of authorized users increases. Collision resistance is an example where its users cannot decipher encrypted data just by combining attributes at it is because each of the existing attribute is related to a random number [2].

Some other issues which need to be considered are Natural disasters which can range from a lightning bolt to an earthquake which can wipe out power for an entire state. There are also some human-induced disasters including network misconfiguration or a shut down for any number of issues. Although most of these cases are extremely unlikely, it is not suggested to take risks. Luckily, there are a broad range of extremely effective technologies and techniques available to both SaaS providers and end users to ensure their data is safe and secure including backups and multiclouds [8].

If a SaaS application’s data is hosted in just one data center, this means there is a single point of failure that could, potentially, make the entire application unavailable. Geographic redundancy takes advantage of multiple, geographically distributed data centers [8].

To overcome above difficulty, User Backups is one of the most common way, as a risk-mitigating precaution, making regular backups of data from the SaaS provider is a good strategy. Additionally, some bar associations require their members retain on-premises copies of their practice’s data. For this it should be taken care that, our SaaS provider allows for a full export of your data from their system.

III. PROPOSED SOLUTION

Keeping an eye on Client side security, we proposed a solution through which the Client’s Identity can be secured with higher level of security mechanism. By having the record of Client’s logins and MAC address the server will maintain a database and generate a random token by the use of Gold number generator for uniquely matching that token with the MAC address. Sensing the change in MAC address the server asks the user to enter the 2nd level password and randomly generates the 4-digit code and forwards the code to the already registered mobile number of the Client which was registered at the registration process.

The code is received on the Client’s mobile and notifies him of a possible attack if in case the user attempting the login is not authenticated, if the Client is authenticated, the code received can be entered as required by the Server and allows user to access the account else the access is denied.

We can also increase the security for the available data, the data can be encrypted by using some easily available encryption algorithm which will further improve the security.

IV. CONCLUSION AND FUTURE WORK

The paper provides us a detailed survey of existing threats on Cloud Computing and related solutions for overcoming them. Through this paper we can conclude that there are still possibilities for improvement of security mechanisms available on Cloud but by ensuring some of the basics are followed the threats can be averted. In this paper we have proposed a higher level security mechanism which provides the two levels of passwords. For future work, there can be few more enhancements that can be used for securing the Cloud based services by providing a more command use of more advanced encryption algorithms.

REFERENCES


ACM SIGACT News, 40, 2009, pp. 81-86.


[17] “Microsoft says lost sidekick data will be restored to users”, D. Sarno, Los Angeles Times, October 2009.
