Volume 5, Issue 7, July 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Enhanced Security Mechanisms for Cloud Computing

Himanshu V. Taiwade
Dept of Computer Technology, PIET,
Nagpur, India

Abstract: ***Cloud Computing and the advantages presented by it are well known and so are the threats persist with the technology. There are number of countermeasures which have been introduced for minimizing the threats; still the security breaches are always at large. The previous studies has shown that so far the emphasis has been given largely on security of Cloud services still there is no single security mechanisms which is alone adequate to deal with the threats which are present.***

In this paper a solution is presented which can be used to generate higher level of security to the Clients alongwith an encryption technique which can further improvise the existing structure of Cloud Computing.

Keywords:, Cloud Computing, Clients, Cloud Security, Threats.

I. INTRODUCTION

Cloud computing can be described as the facility of providing and using the IT infrastructure alongwith the platforms, and applications which can be made available in any form of services which are electronically available on the Web. An important factor of Cloud computing is that it promises to cut operational and capital costs also it helps in the IT departments by allowing them to focus on strategic projects instead of keeping the datacenter running. With all this factors, The cloud based services and its ever increasing popularity are hence known everyone and alongwith its popularity, the security threats which persist in parallel with its growth also presents great difficulties for people to fully trust clouds. Cloud computing has the potential to change how organizations manage information technology and transform the economics of hardware and software at the same time. Cloud computing promised to bring a new set of entrepreneurs who could start their venture with zero investment on IT infrastructure. However this captivating technology has security concerns which are formidable. The promises of cloud computing, especially public cloud can be shadowed by security breaches which are inevitable [4]. As an emerging information technology area cloud computing should be approached carefully.

Countermeasures have been introduced to minimize the threats; still the security breaches are always at large. Consider the Clients who want to access the services of cloud; they must have browser on their system to access the network. We always talk about attacks on clouds which make our data insecure on clouds system but there are so many attacks which can also affect our data. When any user login through interface on cloud site then they must take care to perform secure process. There are number of attacks which may hamper the data.

The Identity and access management is other threat which looms at large. It is difficult to manage multiple accounts of customers and the fact that when user leaves the organization their account remains active increases risk of data exposure which leads to the Identity and access related problems specially in SaaS [5].

To overcome this, every organization should thoroughly study the safety measures and policies followed by the provider and should make sure that it is aligned with the privacy and security requirements of the organization. In the past the cloud services that faced security breach was never expected to succumb to vulnerabilities and it‘s evident that cloud providers also face the security concerns faced by other organizations. Consumers should make sure that the contract they sign should be able to fulfil the needed security [4]. It can be hence said that to have a secure Cloud, important objectives are needed which are still be totally achieved.

II. DIFFERENT TYPES OF SECURITY RISKS IN CLOUD COMPUTING

It is understood that although cloud service providers offers tremendous benefits to users, security risks still play a major role in the cloud computing environment which may cause users to hesitate to trust on the service providers [8]. Server security, Client security, Password security are some of the most emphasized concerns related to the Cloud security.

Server Security

There exist many security concerns on server side. As a user, it is important to know what security measures are provided by server before using any of cloud computing services. To enhance the trust of the users, providers can get their system verified by external organizations or by security auditors. Aside from the security factor other issues that needs attention is about the data in the cloud, if at the provider goes bankrupt or being acquired by another business. Traditional data centres used to have regular security audit and mandatory security certifications which ensure the data security. Cloud providers should also incorporate these measures to assure secure transaction among its customers.

© 2015, IJARCSSE All Rights Reserved

Client Security

It is important to provide physical and logical safety to client machine as Client side security is equally important as the Server side. Built in security measures can be eluded by an erudite person without much difficulty. To maintain secure client, organizations should review existing security practices and employ additional ones to ensure the security of its data. Clients must consider secure VPN to connect to the provider. Web browsers are majorly used in client side to access cloud computing services. Cloud providers usually provide the consumers with APIs which is used by the latter to control, monitor the cloud services. It is vital to ensure the security of these APIs to protect against both accidental and malicious attempts to evade the security. The various plug-ins and applications available in the web browsers also causes a serious threat to the client systems used to access the provider. Many of the web browsers do not allow automatic updates which will append to the security concerns. To ensure secure cloud organizations should work on the existing internal policies and improvise its security strategies if necessary [2]. Other than these attacks some attacks are explained in the report generated by FAA in 2012 [15].

Password Security

Password security is used for authentication process, but once broken; the attacker can gain all the privileges provide for the authenticated user. It is also noted that the best SSL encryption and client/server security can all be undone by the choice of a weak password. Thus, it's important to choose a secure password for any website and it should be the case that a given password should be changed regularly.

Identity Thefts

As advised by, NIST need of secure and trusted identities and there efficient management by keeping users privacy protected and also protecting the individual groups of data present within the remote and distributed shared environment. It is difficult managing many accounts of customers and the fact that when user leaves the organization their account remains active increases risk of data exposure which leads to the Identity and access related problems especially in SaaS [6].

III. LIMITATIONS OF PRESENT SOLUTIONS

By having the survey on security issues on Cloud, it can be understood that with many approaches being applied still huge number of limitations are present which cannot be easily overlooked. The problem of malicious insider in the cloud infrastructure which is the base of cloud computing is well explained by Rocha and Correia [16]. It explains that, IaaS (Infrastructure-as-a-service) cloud providers provide the users with a set of virtual machines from which the user can be benefitted by running software on them. For this, the traditional solution is to ensure data confidentiality by data encryption but this is not sufficient due to the fact that the user's data needs to be manipulated in the virtual machines of cloud providers which cannot happen if the data has been encrypted. Administrators manage the infrastructure and as they have remote access to servers, if the administrator is a malicious insider, then he can gain access to the user's data. Van Dijk and Juels [18] presented some negative aspects of data encryption in cloud computing. In addition, it was being assumed that if the data is processed from different clients, data encryption cannot ensure privacy in the cloud.

Some other important questions which appeared were how the data can be used because when it comes to confidentiality of the client information, the privacy policy generally outlines how the cloud computing provider can or cannot use the data we enter into the application. As, it is known that all the information we enter into a cloud computing application should be treated as confidential and that private information should not be used by the cloud computing provider. Furthermore, the cloud computing provider should only be permitted to view any of our private information with our explicit consent. In many cases this seems to be the only obvious and fair way of treating private data, there have been some high-profile cases of very popular websites imposing less-than-fair privacy policies on their users. For example, Facebook recently caused a virtual firestorm with an update to its privacy policies that apparently granted the company perpetual control over content posted by its users.

Data Availability is other aspect which should be properly handled as, not only the case of server systems going down, also types of disasters that need to be contemplated in a data availability strategy are numerous. Natural disasters could range from a lightning bolt that causes a simple power outage at one data center to an earthquake that wipes out power for an entire state. Human-induced disasters could include a simple network misconfiguration or a situation where the SaaS provider must shut down for any number of issues related to business continuity. Although many of these scenarios are extremely unlikely, the value of the data that is being stored should require a comprehensive plan to mitigate the risk associated with potential disaster scenarios. 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 [6].

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 [6].

To overcome above difficulty, User Backups is one of 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.

© 2015, IJARCSSE All Rights Reserved

IV. PROPOSED SOLUTIONS

The presented solution focuses on Client side security; we propose 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. The figure 1 is used for showing the flow of sequence in the login process using the two level efficient password management systems. 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.

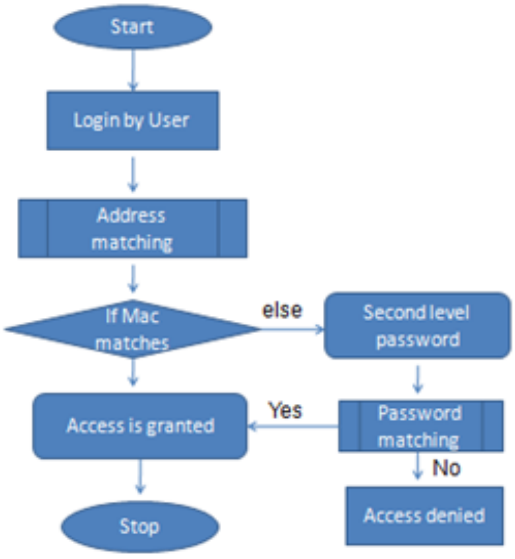

Fig. 1 The Data Flow Representation

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.

Further to increase the security of the data the entire data can be encrypted by the use of encryption algorithm for improving the security.

V. CONCLUSION AND FUTURE SCOPE

The study provided with the survey of existing threats for Cloud Computing and solutions available for overcoming them. We can conclude that still the possibility of secure Cloud is far from reach and huge amount of work is to be achieved for completely securing the cloud. For this we developed a higher level security mechanism by providing the two level passwords. For future work, we will try to provide a framework to supply a secure cloud database by encryption algorithms which can guarantee to prevent security risks faced by the cloud computing community. By the successful completion of the framework a more secure and enhanced Cloud security mechanism can be achieved.

REFERENCES

[1] "An Identity-Based Security Infrastructure for Cloud Environment" , by Christian Schridde, Tim Dornemann, Ernst luhnke, Bernd Freislebenl, Matthew Smith, *In 10th IEEE International Symposium on Cluster Computing and the Grid 2010*.

[2] "Security issues of Cloud Computing; Solutions and Secure framework" by Asha Mathew, *ZENITH International Journal of Multidisciplinary Research Vol.2 Issue 4, April 2012*.

[3] "Personal Cloud Computing Security Framework", by Sang-Ho Na, Jun-Young Park, Eui-Nam Huh, *In 11th IEEE International Symposium on Cluster Computing and the Grid 2011*.

[4] "A Layered Security Approach for Cloud Computing Infrastructure", by Mehmet Yildiz, Jemal Abawajy, Tuncay Ercan and Andrew Bernoth, *In 9th IEEE International Symposium on Cluster Computing and the Grid 2009*.

[5] "Privacy and Security Practices in the Arena of Cloud Computing - A Research in Progress", by Srilakshmi Ramireddy *2010 AMCIS 2010*

[6] "Cloud Computing Security: From Single to Multi-Clouds", by Mohammed A. AlZain, Eric Pardede, Ben Soh, James A. Thom, *45th Hawaii International Conference on System Sciences IEEE 2012.*

[7] "Survey: Some attacks on Client Side, Browser and Cloud", by Pragya Singh Baghel, *IJCSE Vol. 3 No.3 Jun-Jul 2012.*

[8] "Trusting the cloud", by C. Cachin, I. Keidar and A. Shraer, *ACM SIGACT News, 40, 2009, pp. 81-86.*

[9] "Dependable storage in the Intercloud", by C. Cachin, R. Haas and M. Vukolic, *Research Report RZ, 3783, 2010.*

[10] "Security in the cloud", by Clavister, *White Paper, 2008.*

© 2015, IJARCSSE All Rights Reserved

[11] "Security guidance for critical areas of focus in cloud computing", G. Brunette and R. Mogull (eds), *Cloud Security Alliance, 2009.*

[12] "Supporting Database Applications as a Service", by H.Mei, J. Dawei, L. Guoliang and Z. Yuan, *ICDE'09, 25thIntl.Conf. on Data Engineering, 2009, pp. 832-843.*

[13] "SiRiUS: Securing remote untrusted storage", E. Goh, H. Shacham, N. Modadugu and D. Boneh, *NDSS: Proc. Network and Distributed System Security Symposium, 2003, pp. 131–145.*

[14] "How to build a trusted database system on untrusted storage", U. Maheshwari, R. Vingralek and W. Shapiro, *by OSDI'00: Proc. 4thConf. on Symposium on Operating System Design & Implementation, 2000, p. 10*.

[15] "Lucy in the Sky without Diamonds: Stealing Confidential Data in the Cloud", F. Rocha and M. Correia, *Proc. 1stIntl. Workshop of Dependability of Clouds, Data Centers and Virtual Computing Environments, 2011, pp. 1-6.*

[16] "FAA Cloud Computing Strategy", Final - Version 1.0 May 2012.

© 2015, IJARCSSE All Rights Reserved