Framework for User Authenticity and Access Control Security over a Cloud

Mr. Amit Wadhwa
Research Scholar
Computer Science & Engineeriung
JaganNath University, Jaipur
Email: amit87_wadhwa@yahoo.co.in

Dr. V. K. Gupta
Research Supervisor
JaganNath University, Jaipur

***Abstract*—Cloud computing has emerged as a computing paradigm bringing forward many new challenges for data security and access control when users outsource sensitive data for sharing on cloud servers, which are not within the same trusted domain as data owners. Considering the user access control part, in recent years many new findings have been worked upon to provide better user access control while accessing services over a cloud. But the problem still remains unresolved and if resolved by some encryption/decryption methods are problematic in some way or the other. Here security issue related to user authentication and access control is addressed and given an insight into it, along with providing some valuable inputs which if implemented according to the plan proposed might come up with better solutions to user authentication and CSP's critical data security issue. This paper mainly considers various points, like securing access to services of cloud users, protecting user credentials data files stored with CSP and other critical information related with CSP and cloud users.**

Keywords- Cloud Computing; Access Control; Authentication; Digital Signature

I. INTRODUCTION

Cloud computing is a dream of computing as a utility. It makes software more attractive as a service and shaping the way as information technology hardware is designed and purchased. By combining a set of existing and new techniques from research areas such as Service-Oriented Architectures (SOA) and virtualization, cloud computing is regarded as such a computing paradigm in which resources in the computing infrastructure are provided as services over the Internet [1]. It basically shifts all computing infrastructure to the network with the aim to outsource the provision of computing infrastructure required to host services (which were earlier made available to its users through internet based interfaces). As more business is accomplished using cloud computing technology, many companies are developing a higher comfort level with these advanced systems and are willing to entrust more of their operations to professional cloud computing providers. Cloud computing provides three service models [4] that provide different levels of control and security, as explained below:

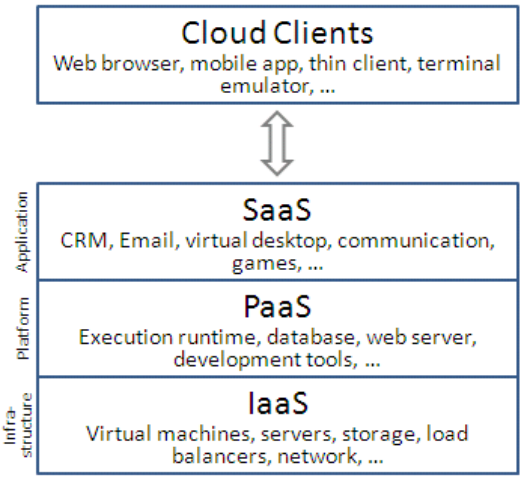

Figure 1. Service Models in Cloud Computing

In practical, though a cloud is basically a combination of data center hardware and software [2]. So, while adopting this cloud for providing services to users, a cloud service provider (CSP) has to be responsible for providing a secure access to the data of users accessing those services over a network. Owner of data in starting days of the cloud technology is not much aware or concerned about providing its own level of security to its data made open to CSP working with a cloud. But as time progresses and more adoption of cloud comes into picture in global market, then a new emerging set of attacks and security breach are made aware of.

This leads to data owner's to think other way around about providing their own level of security to its data made available over a cloud. Along with it CSP's also start thinking of securing user credential related data over a cloud for accessing a service, to be made secure. Because as if that information is threatened then user's privacy over a cloud is compromised. Cloud computing paradigm also brings forth many new challenges for data security and access control when users of cloud outsource sensitive data for sharing on cloud servers, which are not within the same trusted domain as data owners. So, their security needs to be handled properly, and it is the responsibility of CSP (Cloud Service Provider) to make different user's areas un-accessible by un-intended and unauthorised other users of the same cloud.

II. ACCESS CONTROL AND AUTHENTICITY

Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. In private and public computer networks (including the Internet), authentication is commonly done through the use of login passwords. Knowledge of the password is assumed to guarantee that the user is authentic. To start with each user registers him/her using an assigned or self-declared password. On each subsequent use, the user must know the previously declared password. The weakness in this system for transactions that are significant (such as the exchange of money) is that passwords can often be stolen, accidentally revealed, or forgotten. These systems and techniques are not optimized enough to make any authentication secure enough to withstand every type of security breach, which points towards the necessity of more secured and fool proof authentication technique.

A. Ways of Authentication

The ways in which someone may be authenticated fall into three categories, based on what are known as the factors of authentication:

1. Something you know
2. Something you have, or
3. Something you are

Each authentication factor covers a range of elements used to authenticate or verify a person's identity prior to being granted access [3]. These three factors (or categories) and some of elements of each factor are:

- The ownership factors: Something the user has (e.g., wrist band, ID card, security token, software token, phone, or cell phone).
- The knowledge factors: Something the user knows (e.g., a password, pass phrase, or personal identification number (PIN), challenge response (the user must answer a question)).
- The inherence factors: Something the user is or does (like fingerprint, retinal pattern, DNA sequence), signature, face, voice, unique bio-electric signals, or other biometric identifier).

Even these represent general scenario of authentication covering basic definition. Over the years many different methods have been proposed to solve this problem or to reduce it to a considerable extent, but still some flaws always occur in each one of them. So to provide a better insight into this problem of secured authentication, we propose a technique which might put an enormous hold over the topic of secured user authentication and access control. Basically user authentication is not the only step or process, it incorporates three A's i.e. Authentication, Authorization and Auditing. In this work our main stress is toward these three A's and towards the security of critical data associated with CSP (like password storing files or access control files etc).

B. Methods Providing Secured Access Control

1. Message Authentication and one time password generation
2. Authentication using Private-key Ciphers
3. Hashing Functions and
4. Digital Signature Scheme

Important points to be stressed upon in this research is related to secured user authentication and making sure that the intended hacker or cryptanalyst acting as intended/genuine customer is not able to access any of critical data/information belonging to CSP (such as passwords file or access control related information). And approach used to make it happen is elaborated in proposed schemata.

III. DIGITAL SIGNATURE AND RSA ENCRYPTION ALGORITHM FOR ENHANCED DATA SECURITY IN CLOUD

In cloud computing platform there are many problems of security like host security, network traffic, backups and critical user data security. A digital signature scheme is a mathematical based scheme for demonstrating the authenticity of a digital message or document encrypted with either RSA algorithm or any other algorithm like MD5/SHA etc. If a digital signature is valid it gives an impression to the recipient that message or document was created by a known and legitimate sender and was not altered in between the process of transferring.

One can use digital signature and RSA scheme combined together to ensure the data security over cloud. RSA is the most recognizable asymmetric (i.e. requiring two different keys) algorithm. RSA was created by Ron Rivest, Adi Shamir, and Leonard Adleman in 1978 [8]. In digital signature technique the process is that the data is crunched down in few lines using some kind of hashing algorithm which is a called as message digest. Then message digest is encrypted with private key and decrypted using pair of recipient's private key and public key of sender. Digital signature scheme can be used for distributing data over a network just like cloud where it is important to detect forgery and tampering as cloud provides services like pay per use basis and on demand access to services of CSP. So it might prove to be an asset to implementing better security methods over a cloud.

IV. PROPOSED SCHEMATA

Basically it requires a user over a cloud need to be registered for accessing various available services. During registration process with a mix of Digital signature technique and other related encryption technique or algorithm the user related critical information is securely stored over the cloud and is made available with the CSP. Which as is in encoded form, not readable by CSP itself.

The initial step of the proposal made can be represented with the help of diagram depicted here as under:

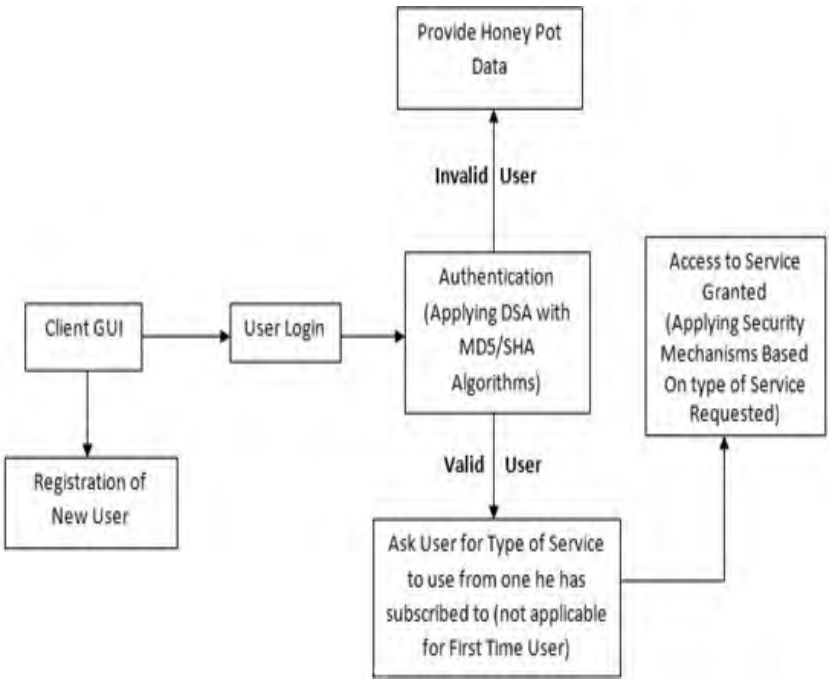

Figure2. Basic Layout of Proposed Technique

Another thing after making the critical data secure, the file with access control detail is transformed into a new form using a secured method of encryption. And when next time user logs in over the cloud after authentication process, a secured key (generated using a chosen digital encryption algorithm and is made available to the user through a medium chosen by him/her at time of registration) needs to be entered by user to further access various different services available at his/her disposal.

This specifies a two way secured communication to take control of the secured authentication process. For further security at internal level after successful login procedure there can be provision for barring of various services based on criteria chosen for different users is made. Along with it a new technique for storing the information of CSP is proposed, to provide a better level of security.

V. IMPORTANCE, RELEVANCE AND POSSIBLE OUTCOMES OF PROPOSED TECHNIQUE

The main focus of this study is towards providing security while authenticating users of cloud for accessing services provided by respective clients of the cloud. This is one of the common and important issues related to security concerns that various organizations would look after before moving over to this emerging and widely growing technology i.e. cloud computing. Main question that a client planning to use a particular cloud for his computation or storage needs ask is:

- "What is the level of security you would provide us if we use your services and at What Price?"
- Basically how different user's areas are separated from others using the same services provided by a client?
- How different users account are managed, starting from login into system to accessing services?

Here this study is basically focuses on the second and third perspectives mentioned above i.e. separation of different user's area and authentication related issues of users accessing their personal regions over a cloud as well as how critical data (like login credential and access rights file of users) of CSP is maintained secure. This technique if implemented as per the proposal made could result in further development of various standards to be implemented by a CSP in order to make its service set work and function as a cloud.

VI. CONCLUSION AND FUTURE CONSIDERATION

This paper presents a proposed technique pertaining to secured user authentication. Along with it making the critical data of CSP secure in its own way of encrypting the critical data file or record with a different algorithm and storing it over a cloud in an altered format which is not easily traceable by the un authorised user or attacker. It also highlights the issues and requirement of a secured user authentication and better access control over a cloud. Further in future a problem still left untouched a bit over a cloud can be resolved, of setting up various standards to be followed by any anonymous CSP for making its services available to its users over a cloud.

REFERENCES

[1] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing," in Proc. of IEEE INFOCOM 2010, 2010

[2] Pardeep Sharma, Sandeep K. Sood, and Sumeet Kaur : "Security Issues in Cloud Computing" (Book review): Springer-Verlag Berlin Heidelberg 2011 pp. 36–45, 2011

[3] L. M. Vaquero, L. Rodero-Merino, J. Caceres, M. Lindner, "A Break in the Clouds: Towards a Cloud Definition," in Proc. Of ACM SIGCOMM Computer Communication Review, 39(1), Jan 2009, pp. 50-55

[4] Oracle.com, Software Architecture for High availability in the cloud http://www.oracle.com/technetwork/articles/cloudcomp/jimerson-ha-arch-cloud-1669855.html

[5] Ristenport, T., Tromer, E., Shacham, H., and Savage, S., "Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds" Proceedings of the 16th ACM conference on Computer and Communication Security, 2009

[6] D.H. Patil, R. R. Bhavsar, A. S. Thorve, "Data Security over Cloud" , International Conference on Emerging Frontiers in Technology for Rural Area (EFITRA), 2012, proceedings in International Journal of Computer Applications® (IJCA)

[7] Boneh, D., and Crescenzo, G., D., "Public Key Encryption with Keyword Search" Proceedings of Advances in Cryptol- ogy, EuroCrypt 2004. Lecture Notes in Computer Science, Springer

[8] S. Uma, L. Kanika, M. Manish, "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing", 1st International Conference on Parallel, Distributed and Grid Computing (PDGC - 2010), proceedings in IEEE

[9] NIST, Guidelines on Security and Privacy in Public Cloud Computing, http://csrc.nist.gov/publications. 2011

[10] Reddy, K.K.M, Macko, P., and Seltzer, M., Provenance for the cloud. Proceedings of the 8th USENIX conference on File and storage technologies, 2010

[11] Lindell, Y., and Pinkas, B., "Privacy Preserving Data Mining" Proceedings of 20th Annual International Cryptology Conference. 2000

[12] Ateniese, G., Burns, R., and Curtmola, R., Provable Data Possession in Untrusted Stores, Proceedings of the 14th ACM conference on Computer and Communication Security, 2007

[13] Microsoft Windows Azure, http://www.microsoft.com/azure/

[14] Wikipedia: Cloud computing http://en.wikipedia.org/wiki/Cloud_computing

[15] Google App Engine, online at http://code.google.com/appengine/

[16] Amazon Web Services (AWS), online at http://aws.amazon.com

AUTHORS PROFILE

Mr. Amit Wadhwa has received B.Tech (Computer Science) degree from Kurukshetra University in 2008, DAC from Dr. D. Y. Patil Prathisthan, Institute for Advanced Computing and Software Development, C-DAC Pune in 2009 and M.Tech(Computer Science & Enginreering) from Kurukshetra University in 2011. Currently pursuing Ph.D. from JaganNath University, Jaipur and working as an Assistant Professor in Amity School of Engineering and Technology (Dept. of Computer Science & Engineering),Amity University Haryana. He has 3 years of experience in teaching and has guided M.Tech students and several B.Tech projects, working with Amity University Haryana. His areas of interest are Cloud computing, Big Data Analytics and Genetic algorithm. Currently 12 B.Tech students are doing final year projects under him.