THINK INDIA JOURNAL ISSN: 0971-1260

Vol-22-Issue-17-September-2019

Survey Paper on Authorization and Authentication In Security Aspect of Cloud Computing

Shailja Sharma
Department of Computer Science & Engineering
Lovely Professional University
Phagwara, Punjab, India.
Shailja.22209@lpu.co.in

Subhita Menon
Department of Computer Science & Engineering
Lovely Professional University
Phagwara, Punjab, India
subhita.20260@lpu.co.in

Gurleen Kaur
Department of Computer Science & Engineering
Lovely Professional University
Phagwara, Punjab, India.
Gurleen.22742@lpu.co.in

Abstract

Cloud computing is storage over internet. The cloud user store there data on the cloud and once data is uploaded over the cloud by a particular user then they can access it from anywhere with secure login with the help of internet connection. Cloud can store every type of data such as images, text and video data in an enormous amount. With the ease of data access, it has some security issues. Over the cloud storage, Authentication and Authorization of user is the area where improvement needs to be done. In that, if the user wants to access the data over cloud from any other place, he needs to login before get the access to data or services. After correct login details, he will only be authorized to use the cloud data, if he is authenticated user. There are numerous authentication procedures together with outmoded and biometric but has some downsides on which further work can be done in research.

1. INTRODUCTION

The Cloud Computing now a days is in latest trends, it is the technology useful for all the companies which works over internet and stores it data on cloud. Cloud computing has number of advantages over other storage such as efficient in cost , easy to back up the data and unlimited storage, easy access to information automatic software integration but secure access management to cloud is an area we are lacking in . The Cloud coordinates with technologies like memory management, management of huge database sets and networking.

Authentication: In terms of Cloud security the mainly important factor is authentication. Authentication can be viewed as a process to verify the identity of a user for its identification. Authentication deals with valid identity of the individual for which he is claiming. Authentication can be achieved on the basis of Personal ID and Password, Fingerprints or Voice Patterns etc.

Now various researchers are focusing to find new technologies to check the authentication of user such as Face Recognition System

Authorization: The other main aspect of Cloud security is authorization. Authorization is next step of secure data access over cloud after authentication , it is viewed as a process of allowing the authenticated user to access the data or services over cloud .

2. Literature Survey

To find out new methods of authentication and authorization in cloud computing on which the researchers are working. In this section the work done in the field of cloud security is divided into different categories.

2.1 Authentication Architectures And Models

Chow et.al. The model of Authentication for a particular user is predicted. It is done by going through the history of website the user has visited on the. But this method becomes vulnerable in the sectors of high risk such as banking. One of the other researcher developed the method of authentication that was implemented through mobile phones i.e. during the login phase, the Out of Box substantiation lying upon Public Key Infrastructure. This infrastructure is a collection of machinery such as hardware and also include software, protocols, policies to follow, measures to consider and it is also dependent on group of set of people waged together.

It has a drawback of absence of secure credential protocol. The smart card inserted in terminal and ID password is entered. System validates the request made by user and send the request to the server. In response, server generate One Time Password (OTP) which will be sent over the users' registered mobile phone. The user access that OTP from the mobile and add it to the interface which is further sent the OTP mentioned by user to server. The server authenticate the client by matching the sent and received OTP . If it matches access to the cloud storage is provided to the user. The advantage of this framework is session key agreement of users and server of cloud, identity management.

2.2 Passwords With Smart Card based Authentication

A. Celesti et al. The model of Authentication was based on what has possessed by a user. Base of this model is Tokens. Authentication has two types of tokens –software and hardware. The model which uses tokens also works on mobile devices. The physical devices that helps to generate a one time password are called hardware tokens.OTP can validate the authentication only one single time. It has disadvantage of security. So to overcome that the software Tokens came into existence. In distributed servers ,the gaugability of the defined server linked to smartcard grid system is considered which manages the execution of occurrence of user's accesses in terms of sessions.

2.3 Biometric Authentication Methods

Akshay A. Pawle et. Al. All the Bio-metric authentication techniques depend on the physical characteristics of the user.

The most commonly considered characteristics to use in bio-metric authentication scheme includes finger prints, face recognition, palm prints, thumb impression, voice recognition, hand geometry, retina acknowledgement. Biometric recognition scheme can be investigated on factors such as time, acceptability, uniqueness, consistency. The highlighted bottleneck of these techniques is the need of a particular scanning system to authenticate the users, who is not even feasible to apply for internet users remotely. Thorough dedicated research is conceded out in order to abridge biometric based authentication approaches for the users who use cloud for storage. In this fiels many important work related to research is discussed. The user authentication system works in two phases. The enrollment phase and the matching phase. The best preferable model is the one which employs both the phases i.e. old password security and biometric based security attribute for cloud client's authenticity .

Additional biometric technique for cloud computing is face recognition. In face recognition security system, on entering the username, instead of numeric password, the face of cloud user is clicked by the camera and the image acts as an password , which is clicked through camera . This approach of authentication is achieved in following four steps i.e. face capture , then face detection, then alignment of face structure, then the last step is feature mining. It is one of the best method to implement in the terms of security of a dedicated individual cloud account. But the one vulnerability it has is that ,camera is required to recognize the face features. The other disadvantages are that the capturing of structures may vary contingent on illumination, presence of accessories on the face, beards, time of the day, surgeries and changes in face with ageing.

3. Problem Definition in various techniques available

Authentication in the Clouds: Authentication framework is a very useful application to mobile users. Authentication is prepared on the clients conduct, so if the device is stolen, it is not a threat. Authentication is maintained parallel to a crisp value of threshold. Henceforth, the better result relies on applications' flexibility provision to latest and developing systems related t cloud authentication .

Two factor Authentication: Two factor authentication is vigorous and efficient alongside phishing and attacks through replay. But in this case, if the users mobile is lost , then it leads to breakage of security. There is a requirement to design an approach which will check the authenticity of the user depending on the attribute instead of level of possession for mobile devices.

A better user authentication design approach for cloud computing: Under this process , Identity management, then Mutual authentication and another way is Session key agreement Password and smartcard authentication is done by the local system recital and by providing formal security proof.

Consolidated authentication mode: protocols designed to maintained security allow the user's credentials detail to easily float in the environment of cloud computing. Credential hoard is name given to the overall repository maintained for credentials, posturing various affective threats of the cloud data to be hacked.

Single Sign On: In every smart device connected to internet, there is a dedicated central server. It is the responsibility of central server to supply credentials of users floating in cloud to the dedicated application server. Therefore, multiple authentication for different applications is not required. In this case the bottleneck is ,if the centralized server, which maintain the repository, is hacked then the server and all of its client will be affected. So instead of acting as a centralized server , data should be distributed equally to various servers. Therefore, the measures of security for centralizing the server for authentication needs to be reconsidered and be converted into distributed environment where the control of cloud to various servers instead of one main server.

Multidimensional Password Generation: In this technique the passwords are in the form of 3-dimensional structural pattern. In Multidimensional Password Generation the authentication overheads are more due to multiple levels of authentication. Security levels need to be strengthened.

Voiceprint biometric authentication: The algorithms used to implement the voice security over the clouds make the voiceprint data invertible. Size of codebook database to store all voiceprint depends on the number of users. Therefore, if number of cloud user will increase it will causes an enormous increase in the overhead of codebook.

Remote authentication on secret splitting. Biometric data harmonizing is done at the terminal end. But Remote authentication on secret splitting a threat of the template leakage remain there. More recent trend of biometric trait which include face recognition or 3-dimensional security could be used for authentication. Matching the credentials using smart card technology can be implemented.

Face Recognition as an User Authentication System : Face recognition technique is very simple and its implementation is also easy. The vulnerability is if you do not have camera then this technique comes as a failure for authentication in cloud computing . Other thing is that the effectiveness of features of face may vary with the environment conditions such as lighting conditions, time of the day, makeup etc.

Leak Prediction Model for Authentication in Cloud Computing: This can be employed as an solution for the problem of authenticity preservation by using the redacted trees which takes the help of previous available privacy patters . The bottleneck of this approach is that is dependent on the information which is priority available, so it is unable to detect the attack patters whose information is not available already . The documents which are clustered are initially arranged in the form of trees and it may extended to the use of graphs and forests as well.

4. CONCLUSION

The paper provides a review on the progression of authentication. It shows the step by step development in Authentication field of cloud computing from the application of hardware tokens to multi model biometrics. Research is still being under progress to find new techniques and schemes to authorize and authenticate the user in order to contest the security threats found in Cloud as well as to eradicate those threats. These new approaches by researchers in this field provide a better way for additional research plus expansion in the arena of Cloud security.

REFERENCES

[1] NIST Computer SecurityHandbook,http://csrc.nist.gov/publications/nistpubs/800-12/

[2] Chow, Markus Jocobsson,RyusukeMasuoka, JesusMolina, Yuan Niu, Elaine Shi, Zhexuan Song,"Authentication in the Clouds, 2010.A Framework andits Application to Mobile Users. CCSW‟10, October 8,2010, Chicago, Illinois, USA.

[3] A. Celesti, F. Tusa, M. Villari, APuliafito, 2010. Securityand Cloud Computing: InterCloud Identity ManagementInfrastructure. 19th IEEE International WorkshoponEnablingechnologies: Infrastructures forCollaborativeEnterprises (WETICE), 2010 , pp 263-265.

[4] J. Kim and S. Hong, 2011. One-Source Multi-UseSystem having Function of Consolidated UserAuthentication, YES-ICUC, 2011.

[5] AmlanJyotiChoudhury, PardeepKumar,MangalSain,Hyotaek Lim, Hoon Jae-Lee, 2011. A Strong UserAuthentication Framework for Cloud Computing. Asia -Pacific Services Computing Conference, 2011, IEEE.

[6] Sanjeet KumarNayak,SubasishMohapatra,BanshidharMajhi, 2012.AnImproved Mutual Authentication Framework for CloudComputing.International Journal of ComputerApplications, Volume 52, issue. 5, August 2012.

[7] Akshay A. Pawle, Vrushsen P. Pawar, 2013. FaceRecognition System (FRS) on Cloud Computing for UserAuthentication. International Journal of Soft Computingand Engineering (IJSCE), Volume-3, Issue-4, September2013.

[8] http://blog.kaspersky.com/biometric-authentication.