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

Authentication, Reserved Sharing and Fuzzy Keyword on Cloud Platform

Radhika Bhati, Sridhar M A
Information Science and Engineering,
BMSCE, India

Abstract— Cloud computing has facilitated widespread businesses to communicate and share information on a common platform, along with which some commercial applications of cloud are gaining widespread acceptance for sharing files and data among stand-alone users. Although cloud computing allows us to share much freely and easily than before, it should not be done at the cost of losing the required privacy and authentications. In this paper, the authors explain how multiple level authentication must take in account various details from time to time and use these details in order to retain a constant secured environment. Along with this, they suggest how sharing data on a cloud platform should be implemented along with certain constraints for safety purpose, without hampering the advantages of the cloud computing principles. Lastly they mention approaches regarding the Biometric systems and Fuzzy keywords.

Keywords— Authentication, Authorization, Audit, Biometric Systems, Fuzzy keyword

I. INTRODUCTION

Cloud computing as we all know can be generalized as an internet centric platform providing a range of services on demand. The major services provided by cloud can be categorized as IaaS (Infrastructure as a Service), SaaS (Software as a service), PaaS (Platform as a Service) and DSaS(Data Storage as Services).

Weaknesses in the system and reduce the effect of an attack. The cloud security and privacy is a big concern today. Security, Privacy and secure storage of data are barriers which are preventing the organizations and users from adopting the cloud computing. Emphasis must be given on security, privacy and stability on the cloud based technologies and computing to make them admirable among the corporate multitenant environment. Malicious and Abusive attacks are proliferating cloud security. The data leakage and security attacks can be caused by insufficient Authentication, Authorization, and Audit(AAA) controls, inconsistent use of encryption and software keys, operational failures, persistence and reminisce challenges: disposal challenges, risk of association, jurisdiction and political issues, data center reliability and disaster recovery. Some of the risks in cloud computing are well known in traditional computing models.

Most Cloud platforms contain a single level security system, and the ones which are currently working with the multilevel structure need to make their platforms more robust. The single level authentication could be of the various following types:

- String password
- Biometric
- Graphical password
- 3D password object

Each of these approaches have their pros, as well as their cons. Let us see each of these one by one [1]. The simple String password, is the brute force method of providing security, it is simple, fast, and does the job. However these very properties make it extremely easy to be hacked. The Biometric system is a guaranteed way of providing security. However there are various questions raised about invading the physical and biological characteristic of an individual and also about the fact that this method cannot be used everywhere, for it would mean providing the hardware scanning device to detect authenticity in various locations, which is not very cost effective[1]. Graphical passwords take too much time and require much more space.

II. PROBLEM DEFENITION

The issue we see in current cloud platforms is firstly, that single level authentication is inadequate. Once a malicious user has logged in into account, they have full permission to access and modify data. Also user can upload and share their data with other registered user or unregistered user with help of email id. User can grant access control by which he/she can give permission to other users on the uploaded individual data to view or read and edit document. But the security measures applied is not enough.

Secondly, there should be certain methods to prevent even the authorized users to lay hands on data which is not meant to be used by them specifically. Let us illustrate this using an example. Say user A shares some data with user B;

we keep in mind that the content originally belongs to user A and user B is only accessing this on his or her consent. Let us assume this content, has text, files of various types say images, videos, etc. The cloud platform should contain a provision to ask user A before he or she shares the data whether user B should only be allowed to 'View' the data, or if it would they are allowed to download this data on their machine as well.

Considering the "Bring your own device to work" trend gaining acceptance due to its convenience , companies must ensure that data within their enterprise remains confidential, as in our example earlier, if user B just saved the data locally on his device and left the company, user A being the company would have lost data to an outsider. There is serious issue in sharing scheme. Security measure applied to protect shared file are not up to the mark. Once the file is shared with the other user, it sends a link to other user so that he can access the file but this link is universal. It's not user specific i.e. anyone can access shared file with this link. No measures are applied to check whether the user who has requested this file is genuine or not.

III. PROPOSED WORK

The first section we explain how a multilevel authentication during the first attempt in adding a user is mandatory, then we describe all the factors that the cloud security system must take in consideration each time a user logs into his or her cloud account. Lastly we propose various suggestions on how to improve on the security among registered and authenticated users within the environment.

A. Security Measures when registering a new user.

On the user's first attempts to create an account, the system asks the user for details as name, password, phone number and email-id and the mandatory fields among various other details as required by the company.

Along with explicit details which the user mentions, the system also perform a check on the machine the IP user is using based on IP address or MAC address. Along with this it would gather information on the system time in user's machine to determine the user's
time-zone. These details are necessary for safer log-ins as we will see in the next section.

Once the user has filled the details and the system has gathered the other information that is required, any encryption algorithm on the user's password is used to get an encoded version of the password, the ASCII values of the encrypted password are added and sent to the users assigned phone number and/or email as a One Time Password. The user is asked to enter the same on a prompt. If the user is able to specify what was sent correctly and within the time period of say, one hour, then the user would be registered as a new authorized user of the cloud platform.

B. Measures to be taken while logging in.

During an attempt to log into a user account, the platform again does a check on this user's system time and the Mac address. Firstly if the MAC address does not match with the address which was obtained during the registration of the user, then the time zone is scrutinized. Now if this Time zone is the same as before, the system again generates an OTP and sends this to the user's assigned email or phone number in order to allow the user the discretion of using a new device. This new MAC address is registered until the next login, to see if this may also be an additional device the user uses regularly. If it is, on the next login, it would be stored permanently.

However, if the time zone too happens different from the one gathered at the time of login, along with a completely new mac address, the system will disallow this login attempt and send the user an email stating what was done and if it was in fact the same user then we provide a link for logging in again along with registering a new login.

Along with these measures the cloud platform must perform the technique of authorizing access to user as was done during sign up after a time period of every six months or so, to retain the integrity constraints of the system.

C. Managing activities of authorized users as well.

This section proposes that sharing must be done in a reserved fashion. Let's restate the example mentioned earlier.

Say user A shares some data with user B; we keep in mind that the content originally belongs to user A and user B is only accessing this on his or her consent. Let us assume this content, has text, files of various types say, images, videos, etc. The cloud platform should contain a provision to ask user A before they share the data whether user B should only be allowed to 'View' the data, or if they are allowed to download this data on their machine as well. Depending of what the user A mentions, action would be taken accordingly.

If this content is only for viewing then what we are essentially doing is creating a link for user B to reference what is present with user B, and by reference here, we mean that user B will literally be capable of only viewing. Nothing more than this like copying the text is permitted.

This provision is done so that suppose at a later point in time user A decides that this data is not to be shared or perhaps irrelevant now, he can choose to cancel the sharing which would result to disconnecting this link that was provided to user B for referencing user A's data. This method is highly useful in holding integrity of the author's data and work to themselves, without hampering the ability of sharing it on a cloud platform.

IV. DESCRIPTION ON BIOMETRIC SYSTEMS

Every user has too many password-account pairings, authentication is the main problem. This leads to forgetting or using the same username and password for multiple Sites. Biometrics provides solution to these problems. In this technique, a person's physiological or behavioural traits are used for validation. Deployment domains of biometric

technology, such as forensics, law-enforcement also encounters the same issues.

By moving the existing Biometric technology to a cloud platform, we can solve these issues by ensuring appropriate scalability of the technology, sufficient amounts of storage, parallel processing capabilities, and with the widespread availability of mobile devices, an accessible entry point for various applications and services that rely on mobile clients can be provided [2]. Hence, cloud computing is capable of addressing issues related to the next generation of biometric technology and also offers new application possibilities for the existing generation of biometric systems simultaneously.

Identification and Verification are the two tasks involved Biometrics [2]. Identification involves matching of one among many users who have their data in the cloud. Verification involves validating the identity claim of the user. When a user sits in front of the system, his image is captured for authentication purpose. Then pattern recognition techniques are used to derive the template from the data inputted. The users must have enrolled in the cloud for this process to be valid. Then template derived from the image taken with the appropriate templates soared in the database is compared by a matching component and the outcome of this comparison decides the identity of the user currently presented to the system.

V. FUZZY KEYWORD

The growth of Cloud computing is rapid. Users today can store sensitive information like emails or their personal details in it. However, a major concern in this is the owners of the data and the cloud servers are not present in the same trusted domain. Hence data is at risk and the server cannot be considered to be fully trustworthy. This can be overcome using Data encryption which involves data to be encrypted prior to out-sourcing for data privacy and combating unsolicited accesses. Also when user wants to retrieve data from the cloud, there are few ways to do so. One of the most popular ways is the Fuzzy Keyword search. Users can retrieve files of their need with the help of keyword-based search techniques and has been applied in many plaintext search scenarios like Google search etc.

Unfortunately, data encryption restricts user's ability to perform keyword search and thus makes the traditional Plaintext search methods not suitable for Cloud Computing. Since keywords usually contain important information related to the data files, data encryption also demands the protection of Keyword privacy. Although encryption of keywords can protect keyword privacy, it further renders the traditional plaintext search techniques useless in this scenario. Searchable encryption techniques have been developed in recent years [3] to securely search over encrypted data.

Searchable encryption schemes usually build up an index for each keyword of interest and associate the index with the files that contain the keyword. By integrating the trapdoors of keywords within the index information, effective keyword search can be realized while both file content and keyword privacy are well-preserved. The existing searchable encryption techniques do no suit the cloud computing scenario despite allowing performing searches securely and effectively because they support only exact keyword search. Minor typos and format inconsistencies are not considered. Sometimes users input word keywords or typos, (such as typewriter and typewriter) in her lack of the exact knowledge of data. This is when Fuzzy keyword performs simple spell check mechanisms to correct it using spell check algorithms and fetches the information the user desired. In another instance, user accidentally types some other valid keywords by mistake (for example, search for "fame" by carelessly typing "game"), the spell check algorithm would not even work at all, as it can never differentiate between two actual valid words. Thus, the drawback of existing schemes signifies the important need for new techniques that support searching flexibility, tolerating both minor typos and format inconsistencies [3].

VI. CONCLUSION

A single level of data security on any sort of cloud platform is far from inadequate. A multilevel authenticity is required; certain single level authenticity like the biometric system continues to be the best case of checking integrity of the user due to its robustness, but remains to be a debatable issue. Sharing on a cloud platform beings its greatest strength as well as weakness, must be done cautiously with attempts of reserved sharing. Platforms such as the IaaS, SaaS or PaaS platforms require easier and more effective methods for searching for individual users. In order to facilitate and improve on the basic simple string match idea which does not fetch correct results majority of the times, to obtain what the users usually require fuzzy keyword is a good approach to consider.

REFERENCES

[1] Yogesh Patel , Nidhi Sethi "Enhancing Security In Cloud Computing Using Multilevel Authentication.

[2] Peter Peer,Jernej Bule,Jerneja Žganec Gros, Vitomir Štruc1 ,"Building Cloud-based Biometric Services" on December 4, 2012.

[3] Jin Li, Qian Wang, Cong Wang, Ning Cao, Kui Ren, and Wenjing Lou ," Fuzzy Keyword Search over Encrypted Data in Cloud Computing ".

.

