© 2017 IJSRST | Volume 3 | Issue 7 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology

Secured Information Retrieval from Cloud Involving OTP and Human Voice

Lakshika Singh, Anuj Kumar
ITM, Aligarh, Karsua, Uttar Pradesh, India

ABSTRACT

Cloud computing is an emerging technological paradigm that provides a flexible, scalable and reliable infrastructure and services for organizations. Cloud data are stored and accessed in a remote server with the help of services provided by cloud service providers. There are enormous numbers of security problems associated with cloud computing but that is not resolved now. These security issues can be faced by cloud providers or by their customers. The cloud provider should make sure that whatever services they are offering to their customers are secure and their customer's data is safe while the customer should check that cloud providers are using security measures to keep their data safe. Cloud computing security is categorized from sub-domain of Information security In cloud security, dissemination of private data can be possible that requires stringent security policies with latest technology. Web Services are the essential feature of cloud computing. As web services helps in providing services easily to end users and manage cloud services, So, now-a-days all cloud providers support a large number of web services. But , some novice developers are making data unprotected that can be exploited by the attackers while deploying it on cloud service To combat dissemination of private data ,we are proposing secure information retrieval tactics that provides two level of authentication using OTP and voice recognition of the authorized person.

Keywords: Security, Cloud, Issues, Attacks, Risks, Computing, Availability, Platforms, Internet

I. INTRODUCTION

Data is the most significant entity to every being. It is the sole ingredient of human and non – human communication in all forms, be it electronic, digital, verbal or written. And because of its importance, we adopt stringent measures to secure the storage of data and ensure its authorized access at different levels so that its usability and integrity are maintained. Security of any data deals both with its storage and retrieval. We may apply robust cryptographic algorithms in order to encode the data and/or implement several authentication checks to verify the genuineness of user attempting to access it. In our implementation also, we shall make use of the newest technologies, i.e. Android and Cloud Computing. Android is an operating system that has software stack for mobile devices that includes an application framework, middleware and kernel at the bottom layer. Android is an open source operating system platforms that allows to install third party applications from Google play store. All the application are developed in java language and SDK contains tools and API that provides support for an application development.

II. LITERATURE SURVEY

In this paper the author vrushali Joshi et al. provides the solution to secure data stored on cloud using face fuzzy vault. The data on cloud is arranged in three layers according to CIA and accessed by authorized user of the particular layer. Hence, the data is protected from any modifications or misuse by the service provider as well as unauthorized user[33].

Himabindu Vallabhu at al. proposed that the data has to be stored in an encrypted format using cryptography on biometric for the security reasons. The protocol is blind in the sense that it reveals only the identity, and no additional information about the user or the biometric to the authenticating server or vice-versa. As the protocol is based on asymmetric encryption of the biometric data, it captures the advantages of biometric authentication as well as the security of public key cryptography. The user initially enrolls with the biometric system which is

provided by a cloud, once the identity is registered his/her biometric authentication details are stored in cloud service provider database. The authorization details are also entered at the registration time which is also encrypted[34].

Whenever the user wants to use any cloud service user first uses the biometric authentication service rather than a traditional password mechanism. Once authenticated, the user is redirected to the actual cloud service for which he is authorized to use. The Biometrics allow for increased security, convenience we can say that fused biometric authentication system will be novel solution for authenticating users on cloud computing ,which can be provided as service on cloud and can be used as a single sign on.

Akshay A. Pawle et al. suggests that the services of cloud computing is based on the sharing. Cloud computing provides variety of services like Iaas, SaaS, and PaaS. These services are paid services, so security is a major concern to identify authorized user in cloud computing. To provide cloud services only to the authorized user, secure authentication is necessary in cloud computing. There are so many authentication techniques like password, OTP, Voice recognition, finger recognition, palm recognition etc. but still it has some drawbacks like at times password techniques are not feasible, password can be easily stolen by hacker or if user uses complex password, user may forget that password etc.So it is a better option to use face recognition system rather than traditional or other biometric authentication techniques[3]. The security level of cloud provider in terms of secure authentication is much improved by using face recognition system.

Praveen Tiwari et al. concludes that the biometric key formed from the sender's and the receiver's fingerprints has many advantages over current authentication methods because it can neither be forgotten nor shared and is convenient for users to generate[35].

The technique provides a new way to authenticate in different approaches. It provides availability of data by overcoming many existing problem like denial of services, data leakage. As additional it also provides more flexibility and capability to meet the new demand of today's complex and diverse network. Peter Peer et al. says that Cloud based biometric services have an enormous potential market value and as such attract the interest of research and development groups from all around the world. In this paper some directions on how to move existing biometric technology to a cloud plat presented. Issues that need to be considered when designing cloud-based biometric services have been presented and a case study, where a cloud fingerprint service was developed and integrated with the e-learning framework Moodle was describe part of our future work we plan to migrate more biometric modalities to the cloud and, if possible, devise a multi-modal cloud-based biometric solution [36].

Summary of Literature Review

According to the literature survey that we have done, we have found some pros that we leverages in our research work and overcomes the cons that was found.

In Finger printing techniques, It's impossible to lose your finger prints, no chance of forgetting them. However in practice, uniqueness is the thing that makes using biometric data an inherently flawed choice for a primary method of authentication. Once you have your fingerprint scanned it will give a unique data sequence which if compromised is not exactly something you can change. Imagine having an option of only one password 'ever'. One loss and you are screwed. The above problem can be solved by using biometric and password together for authentication. Whereas, Hand scans requires low data storage but may not be unique to every user.

Retina Scans and iris scans: Retina scans are highly accurate and require low storage space but they need expensive hardware and user identification frequency is less. Iris scans are low intrusive and they are more accurate and needs less storage space.

Voice authentication: Voice authentication is unique and non intrusive method and also the hardware requirements required for this type of authentication are cheap and are available readily. Microphones can be used for this purpose. However the back ground noise must be controlled, high storage is required for this kind of authentication. This type of authentication can also be extraneously influenced by once sore throat and cold.

Facial scans: One major advantage is that facial-scan technology is the only biometric capable of identification at a distance without subject complicity or awareness. Another advantage of facial-scan technology is the fact that static images can be used to enrol a subject.
Disadvantages include acquisition environment and facial characteristic changes that effect matching accuracy and the potential for privacy abuse. Images are most accurate when taken facing the acquisition camera and not sharp angles. The user's face must be lit evenly, preferably from the front.
Therefore, keeping the above studies into perspective, we intend to develop an application that uses multiple, multi – layer authentications checks on the user trying to access the data on cloud.
The advantage of multiple authentications is, it balances the disadvantages of other methods in a way that if one authentication fails, the data will still remain protected in the form that the another authentication cannot be compromised using which we can be assured that only the genuine users will be allowed to access the data and therefore, we can conclude that with a 4 or 5 layer retrieval verifications, the data will remain shielded.

III. Proposed Work

In this section, we will give brief details about our proposed word and its implementation details.
In our proposed implementation:

1) There would be 2 tiers of the project namely Android and Cloud.
2) Both the tiers would be connected wirelessly using HTTP, independent of their geographical location. The application's database shall be on cloud.
3) Using the Android tier, the user would be able to do Registration or Sign – up and Login tasks
4) During the sign up, he/she would input basic details as mentioned below:

i) Name
ii) DOB
iii) Gender
iv) Mobile
v) E – Mail

After the successful sign up, a unique user id will be automatically generated by the application.

The user will thereafter input his voice password. The voice password would eventually be converted into text and stored on the cloud database.

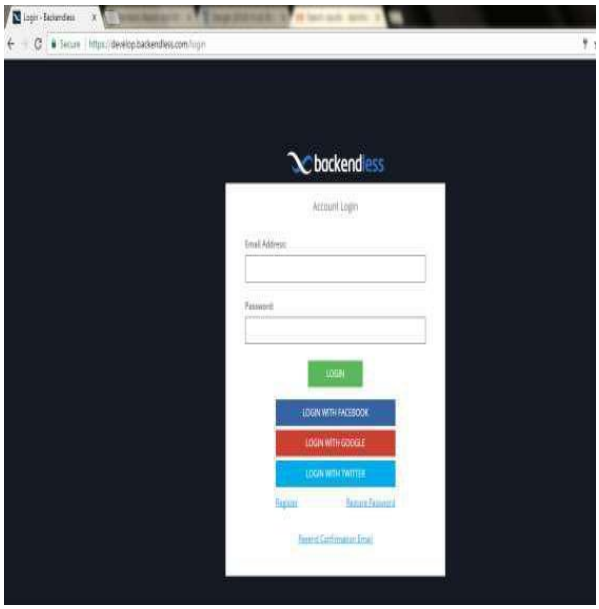
During login, the user would first input his ID

Upon successful match, a unique, random OTP would be generated and delivered to the user's e – mail ID

Only after inputting that OTP correctly, the user would input his/her voice password Upon successful match of the voice password, the user shall be able to login successfully and view his details inputted during the sign – up phase

3.2 Backenedless platform

Welcome to Backendless, a powerful API services platform. The platform can be used to build and run mobile and web applications. Backendless consists of built-in, general purpose API services and also supports deployment of custom, developer-defined services and functions. The built-in API services support common backend tasks and operations such as user login and logout, password recovery, data persistence, file upload, etc. Developer-defined services and functions can be used for custom server-side business logic. This is how our login page looks



Proposed procedure

1) User registers on http://www.backendless.com cloud service for obtaining the *Application ID* and *Client Key* to be integrated with Android tier.
2) Using the Android tier, user does the registration or sign up through inputting basic details like Name, DOB, Gender, etc. A unique user ID is automatically generated henceforth.
3) During registration user inputs the account password in human voice. After successful registration, the registration details are submitted on the parse cloud database through the integrated keys using HTTP
4) During Login process, the user first inputs the user ID which is crosschecked with the Backendless database.
5) After successful first-level authentication, a unique, random one-time-password(OTP) is automatically generated and sent to the registered e-mail address of the user.
6) After successful first-level authentication, a unique, random one-time-password (OTP) is automatically generated and sent to the registered e-mail address of the user.
7) After inputting the voice password correctly, the third level of authentication clears after which the user is successfully able to view his details which are stored on Parse cloud database.

IV. RESULTS

In this section, we will perform evaluation of our proposed work.

Voice Recognition-An Application

Alternatively referred to as **speech recognition**, **voice recognition** is a computer software program or hardware device with the ability to decode the human voice. Voice recognition is commonly used to operate a device, perform commands, or write without having to use a keyboard, mouse, or press any buttons. Today, this is done on a computer with **automatic speech recognition** (**ASR**) software programs. Many ASR programs require the user to "train" the ASR program to recognize their voice so that it can more accurately convert the speech to text. For example, you could say "open Internet" and the computer would open the Internet browser.

1) After opening this application you have to put a unique id for login ,if you don't have to make a unique user id by sign up process.
2) Now for the sign up process you have to put some general information about the user's like name , date of birth, email id (where otp is to mailed), mobile no.,and gender.
3) After saving the signup form , aunique id is generated like for eg,vr8826 , after that you have to speak a voice password two times and then submit. This information is stored in the cloud database.
4) Now by using user's unique user id login should be done .for login process enter your unique user id(generated at the time of signup) and then login.OTP is generated on your email id that user is enterd at the time of signup .after entering the correct OTP user have to speak their voice password and then submit This all information is validating after this user can access their information on cloud database.

V. CONCLUSION

Therefore, keeping the above studies into perspective, we intend to develop an application that uses multiple, multi – layer authentications checks on the user trying to access the data on cloud.

The advantage of multiple authentications is, it balances the disadvantages of other methods in a way that if one authentication fails, the data will still remain protected in the form that the another authentication cannot be compromised using which we can be assured that only the genuine users will be allowed to access the data.And therefore, we can conclude that with a 4 or 5 layer retrieval verifications, the data will remain shielded.

VI. REFERENCES

[1]. Gosling, James, A brief history of the Green project. Java.net, no date ca. Q1/1998]. Retrieved April 29, 2007.

[2]. Gosling, James; Joy, Bill; Steele, Guy L., Jr.; Bracha, Gilad (2005). The Java Language Specification (3rd ed.). Addison-Wesley. ISBN 0-321-24678-0.
[3]. Lindholm, Tim; Yellin, Frank (1999). The Java Virtual Machine Specification (2nd ed.). Addison-Wesley. ISBN 0-201-43294-3.
[4]. java.com - Java for end-users
[5]. Oracle's Developer Resources for Java Technology.
[6]. Java SE 7 API Javadocs
[7]. Oracle's Beginner's tutorial for Java SE Programming
[8]. A Brief History of the Green Project
[9]. Michael O'Connell: Java: The Inside Story, SunWord, July 1995.
[10]. Patrick Naughton: Java Was Strongly Influenced by Objective-C (no date).
[11]. David Bank: The Java Saga, Wired Issue 3.12 (December 1995).
[12]. Shahrooz Feizabadi: A history of Java in: Marc Abrams, ed., World Wide Web – Beyond the Basics, Prentice Hall, 1998.
[13]. Patrick Naughton: The Long Strange Trip to Java, March 18, 1996.
[14]. Open University (UK): M254 Java Everywhere (free open content documents).is-
[15]. research GmbH: List of programming languages for a Java Virtual Machine.
[16]. How Java's Floating-Point Hurts Everyone Everywhere, by W. Kahan and Joseph D. Darcy, University of California, Berkeley.http://www.coderanch.com/forums - A good community for discussing java concerns.
[17]. Android Developer Guide: http://developer.android.com/guide/index.html.
[18]. Android API: http://developer.android.com/reference/packages.html
[19]. Java 6 API: http://download-llnw.oracle.com/javase/6/docs/api/
[20]. GoogleAPI: http://code.google.com/android/addons/googleapis/reference/com/google/an droid/maps/package-summary.html
[21]. Android Fundamentals: http://developer.android.com/guide/topics/fundamentals.html
[22]. The Java Tutorials: http://download-llnw.oracle.com/javase/tutorial/index.html
[23]. Android Native Development Kit: http://developer.android.com/sdk/ndk/index.html
[24]. Android User Interfaces: http://developer.android.com/guide/topics/ui/index.html
[25]. Declaring Layout: http://developer.android.com/guide/topics/ui/declaring-layout.html
[26]. CommonTasks: http://developer.android.com/guide/appendix/faq/commontasks.html
[27]. List of Sample Apps: http://developer.android.com/resources/samples/index.html.