Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 5, May 2015, pg.444 – 449

RESEARCH ARTICLE

Secured Information Retrieval from Cloud Database using OTP and Voice Authentication

Deepak

Department of Computer Science & Engineering, M.Tech, Punjab Technical University, India
deepak_dhiman43@hotmail.com

Abstract— 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.

We wish to develop an application that enables the users to exchange classified multimedia content, securely from any geographical coordinate. We aspire to implement security at all levels, in order to shield the data, right from the point of its creation to delivery. Our intention is to be different from the existent applications under this domain, in the form of latest technology, ease-of-use and scalability. We propose to provide convenience to the user through simple, understandable yet secure communication interfaces. Our goal is to shield date at all checkpoints through which it travels i.e. Sender Device à Network à Cloud à Recipient Device.

Keywords— android, cloud security, otp, voice authentication, information retrieval

INTRODUCTION

In this world of advanced communication, people prefer mechanisms through which data can be saved or retrieved quickly, easily and securely from any geographical coordinate. To facilitate this objective, smart phones and mobile cloud computing play an integral role. They fortify the user to use techniques for smart storage and retrieval of data using infrastructure, platform and software as a service being provided by 3rdparty. In our implementation also, we shall make use of the newest technologies, i.e. Android and Cloud Computing. Android is a software stack for mobile devices that includes an operating system, middleware and key applications. By providing an open development platform, Android offers developers the ability to build extremely rich and innovative applications. The Android SDK provides the tools and APIs necessary to begin developing applications on the Android platform using the Java programming language.

Whereas, the term Cloud computing refers to the many different types of services and applications being delivered in the internet cloud, and the fact that, in many cases, the

devices used to access these services and applications do not require any special applications. Once a cloud is established, how its cloud computing services are deployed in terms of business models can differ depending on requirements. The primary service models being deployed are commonly known as:

Software as a Service (SaaS) — Consumers purchase the ability to access and use an application or service that is hosted in the cloud.

Platform as a Service (PaaS) — Consumers purchase access to the platforms, enabling them to deploy their own software and applications in the cloud.

Infrastructure as a Service (IaaS) — Consumers control and manage the systems in terms of the operating systems, applications, storage, and network connectivity, but do not themselves control the cloud infrastructure.

PROPOSED IMPLEMENTATION

In our proposed implementation:

- There would be 2 tiers of the project namely Android and Cloud.
- Both the tiers would be connected wirelessly using HTTP, independent of their geographical location. The application's database shall be on cloud.
- Using the Android tier, the user would be able to do Registration or Sign – up and Login tasks
- During the sign up, he/she would input basic details like: Name, DOB, Gender, Mobile, E – Mail etc.
- 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 (One Time Password) 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

Before working on this idea, we consulted the below research:

One of the solutions 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 [1].

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 enrols 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. 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[2].

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. The security level of cloud provider in terms of secure authentication is much improved by using face recognition system [3].

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. 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 [4].

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 [5].

According to the studies that we have considered, the pros and cons of different biometrics methods could be listed as:

1. Finger Prints: 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.

2. Hand Scans: Hand scans requires low data storage but may not be unique to every user.
3. 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.
4. 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.
5. 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 users 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.

After studying the prevalent researches, we discovered that:

Most of the studies were based on the facial biometrics and we wanted to design a solution that depends on multiple techniques rather than one. All the studies focused on one idea only and they did not concentrate on eliminating its disadvantages whereas we attempt to balance the demerits of one with the merits of another technique. The studies mostly depend on the complicated calculations in order to secure the retrieval of data whereas we shall focus on simplistic calculations that not only use minimum resources but also produce efficient output in the minimum possible turnaround time. The studies reveal that they do not combine effective output of hybrid techniques in order to protect the data on cloud thereby leaving the end user vulnerable to thefts and security attacks whereas we address this issue through utilizing the common services that the user use like reliable mail services so that once they are put to use, the user is extra satisfied about the integrity of sensitive data. The techniques do not discuss about the efficient resource utilization of the user's resources be it hardware or software whereas in our study we plug and bridge this gap through minimizing the consumption using simple yet efficient verifications checks that put minimum possible load. The studies showed a large gap in harnessing the power of latest technologies available in the market to its full potential whereas in our study we shall make an attempt to use the latest tools, techniques and technologies that only are output – oriented but also possess a vast future scope of expansion possibilities.

PROBLEM FORMULATION

There is large need of an application that protects user's data from geographically any coordinate and allows them to conveniently store and retrieve data from the cloud. The users face problem to manage the security and integrity of their data because of authentication issues in a way there are less or just one check which can be easily compromised through several attempts and once that is done, the user data is left to be on open exploitation. There is a large need of an application that implements hybrid or crossbreed checks that strengthens the users through maintaining the integrity of their data. There is a large need of a simple system that does not involve much user interaction and is able to verify the authenticity of a user through utilization of common services that are being used by everyone like Gmail, for ex:, for the purpose of sending a dynamic one time password for every login session so that the user become extra satisfied that since Gmail is a highly secure and reliable service and since our application utilizes its services it becomes automatically secure and reliable thereby ensuring 100% security to the data. Furthermore, large number of systems involves very complex mathematical calculations and procedures during facial recognition for ex: that occupy huge memory resources, calculation overheads due to processor loads and thereby slow turnaround times eventually leading to downtimes. There is a large need of a system that simplifies all that, that enables the user to access a simple application while on-the-go and facilitates him/her to save as well securely retrieve data using simplified yet very robust authentication mechanisms.

Conclusion & Future Scope

Since data nowadays, is being stored and retrieved digitally through electronic means from any geographical coordinate, our objective is to implement a robust mechanism that assures both its security and integrity comprehensively. We propose to provide convenience to the user through simple, understandable yet secure communication interfaces that are not just easily navigable but also interact intelligently with the user. Our goal is to shield the retrieval of user data using multi-layer virtual security barricades that check the entry of every access and prevent unauthorized attempts, minimizing them to the negligible levels.

Although we have attempted to make an idea that successfully simulates the concept of data security on cloud using implementation of multi – layered authentication techniques, it still consists of a vast scope of future enhancements and improvisations some of which are:

- In addition to securing personal textual data on cloud, this application has a future scope of securing user data files of all the formats on cloud.
- We can include robust cryptographic algorithms to further encode the user data on cloud in addition to already existing secure access mechanisms like OTP and voice biometrics.
- This application could be made dynamic so that it works on any client and not just Android client.
- We can implement a feature of mirror-cloud that not just fortifies the user to secure his/her data but also create a secure backup on cloud.
- Depending upon the level of data confidentiality, we can implement additional authentication mechanisms like IVR passwords, IRIS / Palm / Facial / Fingerprint recognition and offer users to select mechanism(s) of their choice to secure their data.
- The application can further be enhanced to offer comfort to the users to use it even in the rare absence of internet connectivity wherein we can secure the data using alternate offline modes and protocols like Bluetooth, GSM, Wi-Fi, FTP, etc. to local

servers using LAN and then upload them to cloud when the internet / mobile data is available.

- Further continued improvisations to this application in terms of data security could be done through implementation of custom – made encryption algorithms combined with a strong hybrid implementation of robust existing encryption techniques which make our data nearly impossible to break.

REFERENCES

[1] Vrushali Joshi, Payal Sanghvai & Yogita Bhargude "Three Tier Data Storage Security in Cloud Using Face Fuzzy Vault" International Journal of computing ISSN No. 2231 – 6965, Vol – 1, ISS – 3 (2012)

[2] Himabindu Vallabhu, R V Satyanarayana "Biometric Authentication as a Service on Cloud: Novel Solution". International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-4, September (2012)

[3] Akshay A. Pawle, Vrushsen P. Pawar "Face Recognition System on Cloud Computing for User Authentication". International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-4, September (2013)

[4] Praveen Tiwari, Ashish Saklani "Role of Biometric Cryptography in Cloud Computing". International Journal of Computer Applications (0975 – 8887) Volume 70– No.9, May (2013)

[5] Peter Peer and Jernej Bule "Building Cloud-based Biometric Services. Informatica" 37 (2013)

[6] Cong Wang, Sherman S.-M. Chow, Qian Wang, Kui Ren & Wenjing Lou (Members IEEE) "Privacy-Preserving Public Auditing for Secure Cloud Storage" . IEEE Journals, Volume 62 , Issue 2 (2013)

[7] Sagar Shankarrao Dake, Hemanta kumar Mohanta & Yechuri Durga Prasad "Secure User Authentication by using Biometric and Keystroke in Cloud". International Journal of Computer Applications (0975 – 8887) Volume 104 – No 10, October (2014)

[8] Cong Wang, Student Member, IEEE, Qian Wang, Student Member, IEEE, Kui Ren, Member, IEEE, Ning Cao, Student Member, IEEE, and Wenjing Lou, Senior Member, IEEE "Towards Secure and Dependable Storage Services in Cloud Computing". IEEE Journals (2013)

