Two Way Mobile Authentication System

Raana Syeda, Soniya Khushalani, Khushbu Alwani
Department of Computer Science and Engineering,
Jhulelal Institute of Technology
Nagpur, India

***Abstract* - As the Internet technology is expanding its arms day by day therefore securing a data has become a prime factor to protect mobile data from unauthorised users; this can be useful in confidentiality and data integrity. Hence, authentication is used for protection of data. The usage of authentication techniques has been persistent in the domain of security. Earlier older techniques were not able to secure data as compared to today techniques with the rise of technology. Hence, there is an arising need for the advent of new techniques that make use of authentication at increased complexity so that level of security is enhanced. Two Way Mobile Authentication Systems (2WMAS) provides the higher security and stronger authentication in smart phones. The two approaches being used in two way mobile authentication system are-**
Something you know: Personal Identification Number (PIN)
Something you are: Facial Scan

Keywords- Cryptography, Two Way Mobile Authentication, PIN (Personal Identification Number), Facial Scan, Security and Smart Phone.

I. INTRODUCTON

When it comes to security the most important factor is securing the data from viruses or malwares that increases with the increase of abundant infected data. The security and privacy threats through malware are constantly growing both in quantity and quality. In this context one way mobile authentication using traditional login or password insufficiently secure for many security-critical applications. Two-way authentication scheme promise a higher protection level by extending the single authentication factor, i.e., what the user knows, with other authentication factors such as what the user has (e.g.,smartphone), or what the user is (e.g.,biometrics).

In this globalised world of communications, inexpensive Internet connections, and fast-paced software development, security is becoming more and more of an issue. Hence, security is now a basic requirement for every smart phone.

Traditional cryptography solutions use symmetric and asymmetric keys to perform encoding and decoding of given messages or data.

A brute-force approach uses symmetric or/and asymmetric key cryptographic techniques without considering the limitations of mobile devices and networks. In current wireless networks, such as GSM and GPRS, only private keys (or symmetric keys) are used to implement cryptographic solutions.

Another brute-force approach [Grecas 2003] uses a public key-based cryptographic solution. The major problem using public keys in encryption/decryption is its complex algorithm and higher processing time.

Recently, some published research papers proposed mobile key-based security solutions by modifying existing public-key algorithms. As known, most people still prefer to use asymmetric-key cryptographic techniques on mobile devices over symmetric-key cryptographic techniques. However, they be must be customized and improved for the use on mobile devices. There are innovative approaches using a combination of new cryptographic algorithms based on data distribution, time distribution, and workload distribution.

Authentication is the act of confirming the truth of an attribute of a datum or entity. It involves confirming the identity of a person or software program. By definition authentication means using one or more mechanisms to prove that the persons is who he claims to be.

The main goal of our paper is to investigate and evaluate the security of mobile applications by using two way mobile authentication system which provide a base for stronger authentication that will decrease the probability that the requestor is not who he/she claims to be.(i.e., providing false evidence of his/her identity).

II. LITERATURE SURVEY

Modern cryptography has been diversified in the field of mathematics, computer science, electrical engineering and many others. Cryptography is a technique for implementing the practice for secure communication. More generally, it is about related to various aspects in information security, data integrity, authentication and non-repudiation.

Applications of cryptography include ATM cards, computer passwords, and electronic commerce. Cryptographic algorithms are designed around computational hardness assumptions, i.e. hard to break in practice by any adversary.

The Data Encryption Standard (DES) and the Advanced Encryption Standard (AES) are block cipher designs which have been designated cryptography standards by the US government. Despite its deprecation as an official standard,

DES remains quite popular; it is used across a wide range of applications, from ATM encryption to e-mail privacy and secure remote access. Many other block ciphers have been designed and released, with considerable variation in quality. Many have been thoroughly broken, such as FEAL.

Authentication mechanisms involves the procedural steps require by an authorized user to gain access to some data or grant access to certain resources. In this respect, validation of user's requirements and identity is highly crucial. This can be carried out via different mechanisms such as Username and Password, PIN, tokens, access card and any means of pattern recognition features (such as finger prints, face recognition, biometrics to mention a few). However, the two way factors authentication is a more secure means of authentication than the one factor authentication because it combines both what the user knows (such as password) and the biological identification features (pattern recognition – biometrics features like Fingerprints, retina recognition etc.)

Examples of two way mobile authentication includes withdrawing money from an ATM machine. When someone wants to draw money from the ATM, first he\she has to input his\her ATM card i.e. what you have and again he\she has to enter the pin number i.e. what you know in order to access his\her account.

Two Wsay Authentication is where a user's credentials are made up of two independent factors such as-

A. Something you know- Methods based on something the user knows are often associated with a password, multiple passwords, or a combination of a password and a username. The user has to create his/her username and password by singing up, which can be used in future login session.

B. Something you are- According to Wikipedia, 'Bio' means 'life' and "metrics" means 'measurement'. Biometric authentication has many advantages over the traditional credential-based authentication mechanism. It is widely considered to be more secure, because it is based on "who the user is" and biometric information is difficult to forge or spoof. On the contrary, credential-based authentication relies on 'what the user knows'
This can be lost or stolen and more likely to result in identity theft. The user do not have to remember the list of password as every user has certain different identity Because of the uniqueness exhibited by these attributes of mobile users, it is possible to uniquely identify them and their accesses on the mobile devices. Some of the biometric examples are explained below-

(a)FingerprintTechnology- Fingerprint technology recognition refers to the automated method of verifying a match between two human fingerprints. Fingerprint Technology is one of the forms of biometrics used to identify individuals and verify their identity. The fingerprint technology is the oldest one among all biometric identification. The major features of fingerprint ridges are ridge ending, bifurcation, and short ridge (or dot). The ridge ending is the point at which a ridge terminates.

(b) Voice identification- Voice-based biometric security technology identifies authentic mobile users based on their voice inputs. A voice biometric solution provides a stronger security as compared to other non-biometric security solutions.

(c) Facial scan- Face recognition can be divided into two categories: verification and identification [2]. Face verification is a one to one match that compares a face to a template, whose identity is being claimed. Face identification, in-stead, is a one to *N* problem that compares a face to all the templates in a face database to determine the identity of the face being queried.

Existing security tools-

A. Google Authenticator is an application that implements TOTP security tokens from RFC6238 in mobile apps made by Google, sometimes branded "two-step authentication". Authenticator provides a five to six digit one-time password users must provide in addition to their username and password to log into Google services or other sites. The Authenticator can also generate codes for third party applications, such as password managers or file hosting services.

B. AppLock can lock SMS, Contacts, Gmail, Facebook, Gallery, Whatsapp, Settings, Calls and any app you choose, with abundant options, protecting the user's privacy. AppLock can hide pictures and videos, AppLock empowers user to control photo and video access.

III. PROPOSED SYSTEM

Two Way Mobile Authentication is designed to provide security to android applications, which requires users to authenticate themselves with two unique criterions - a username and password at the time of login, and facial scan during verification before they are permitted to access an application.

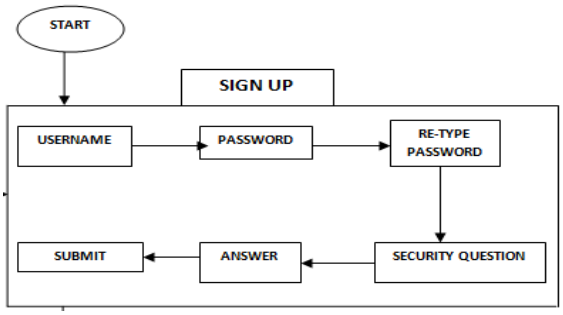
At home page the user is expected to log-in on the logging-in panel with their username and password based on the criteria supplied during registration phase of login section where user has to sign up and create his own username and password, User is redirected to the second authentication phase that begins with facial scan in which image is captured and saved.

After the combination of these two phases the two way mobile authentication app grants an access to secure your mobile application for future security.

Database can be maintained by defining a set of proactive tasks that a DBA (Database Administrator) needs to perform on a periodic basis to help ensure that their databases perform optimally and maintain high availability.

IMPLEMENTATION:

The functionality of the software is as follows –



1. Sign up:

This allows the user to register him for the first time.

A. Username: a user name should be provided by the user.

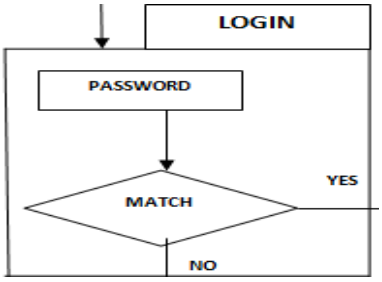
B.Password: this allows the user to set up a password.

C.Retype password: here the user is supposed to re- enter the password to avoid any errors.

D.Security question: this allows saving a security question which can be used in case the user forgets the password.

E.Answer: here the user is supposed to enter the answer to the security question which will help him to recover the password in future.

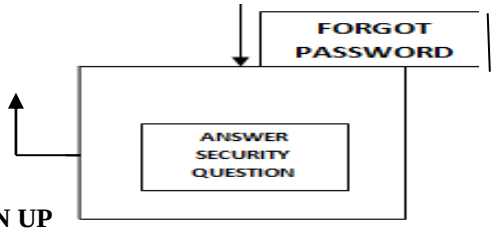
SIGN UP



2. Login:

The user needs to enter the password here which should match with the password provided by the user at the time of registering.

LOGIN

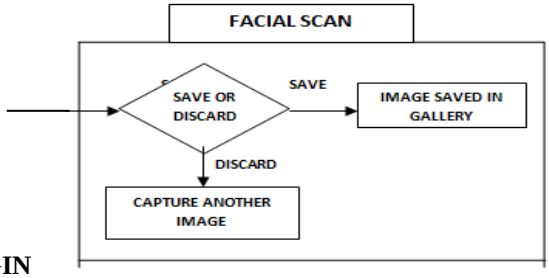


SIGN UP

3. Forgot password:

This helps the user to recover or change the password, in case he forgets it. here the user will be required to answer the question saved as the security question at the time of registry.

If the answer matches to the answer saved at the time of registering then the user will be able to see or change the password.

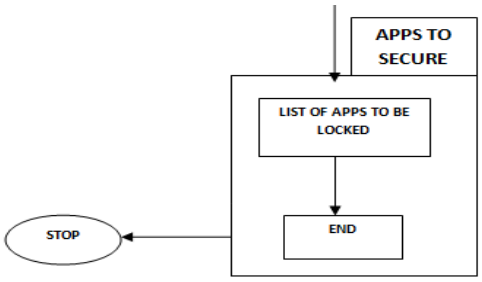


LOGIN

4. Facial Scan:

In this section the user caputures his/her own image for face detection and accordingly the image is being saved or discarded.If the image is detected properly,it is saved in gallery else the user needs to capture another image.

FACIAL SCAN



5. Apps to be locked:

This provides the user the list of applications installed on his phone. He can select from this list the applications he wants to lock using the two way mobile security system.

IV. APPLICATIONS

Two way mobile authentication systems can be used in institutes for attendance. It can also be used in sensitive areas like military and banks and further we can implement it for tablets.

V. CONCLUSION

This research aims to study and implement the two way mobile authentication for android system and analyzing its advantages over the one way mobile authentication system. This research was initially examined and analyzed the traditional way of authentication which involves the use of username and Password/Pin to gain access to applications. The analysis was concluded and states the urgent need to introduce the two way mobile authentication system as a more secure and reliable mode of authentication for an android system.

VI. REFERENCES

[1] Aloul F, Zahidi S, El-Hajj W. (2006): Two Factor Authentication Using Mobile Phones, IEEE/ACS International Conference on Computer Systems and Applications.
[2] IAshchenko (2002). "*Cryptography: an introduction*". AMS Bookstore. P.6. ISBN 0-8218-2986-6.
[3] (2014) The Wikipedia website. [Online] Available: http://www.en.wikipedia.org/
[4] Do Van Thanh Jorstad , Do Van Thuan and I. Jonvik (2009): Strong Authentication with Mobile Phone as Security Token, Mobile Adhoc and Sensor Systems, IEEE 6th International Conference
[5] The Google Scholar website. [Online] Available: http://www.googlescholar.com/
[6] Aloul F. etal, (2006): Authentication means using one or more mechanisms to prove that the person is who he claims to be.