Survey of Existing Authentication Systems

[1.] S. S. Shinde, [2.] Rituraj Sambherao, [3.] Amit Shahapurkar,
[1.] Professor, Information Technology, Marathwada Mitra Mandal's Institute Of Technology (MMIT) , Pune, India
[2.] Student, Information Technology, Marathwada Mitra Mandal's Institute Of Technology (MMIT) , Pune, India
[3.] Student, Information Technology, Marathwada Mitra Mandal's Institute Of Technology (MMIT) , Pune, India

Abstract— **In last few decades large technology development raised new needs. Financial sector has no exception. People are approaching all over the world to fulfill their dreams. Any sector needs to understand changing need of customer. Recently, with the awareness of businessmen and consumers and the development of mobile technologies, the potential use of mobile devices in financial applications such as banking and stock trading has seen a rapid increase. However, the security challenges being faced are diverse and increasing in number because of huge amount of money flowing across the mobiles. The aim of this work is to provide a secure environment in terms of security for transaction by various ways. But due to many security flaws these schemes are not feasible for real-life implementation. In this project we focus on mobile banking and explore different ways to make authentications more secure as means to improve the security of communication in various channels for any intrusion by the hackers.**

Keywords—Steganography,Cryptanalysis

I. INTRODUCTION

Authentication Systems are used everywhere. They give means to identifying people and ensuring only the authorized user is using the systems. Authentication systems involve various techniques which ensure that only the legitimate user is using the system.

However, these systems are not without their flaws. These systems can eventually be compromised by hackers and can be misused by them. Authentication system should be in a way that it will hide user's fingerprints from attackers and will provide a way by which information can transmit in a secure manner [1]. From old times after every secure systems is created, hackers have found a way to bypass those systems. That is why there is a need of authentication systems which will be easy to operate for a user and will also be robust from attackers.

Mobile users are increasing on a drastic rates and their security is a very important concern when it comes to authentications [3]. The development of the new systems involves techniques which should ensure that the mobile authentications will be secured and protected from attackers

II EARLY SYSTEMS

Many Early systems usually relied on username-password combinations and there unique qualities to identify and differentiate them from each other. After some time more complex systems were practiced which could actually differentiate and identify users on basis of their biological diversity.

i. Username-Password systems.

From early century these techniques are in existence. Password is a certain type of word or a phrase which allow access to a user to gain access to a resource. However these username password had to keep in secrete because anyone could use them if they had possession of passwords. Passwords could be cracked by guessing or some common dictionary words or brute force. This isn't the most secure way to authenticate.

ii. Biometric Authentications.

It is the use of unique biological qualities which distinguish humans from each other. It involves their faces, their eyes, thumb and palm impression and even their DNA's [1]. However, an imposter can actually bypass these systems by providing exact biometric signatures of the user. E.g. an imposter can provide a user's face and gain access. Same goes with the rest of the techniques.

iii. Machine authentication

Instead of authenticating users, devices which they operate on have their unique properties. Only the systems which satisfy these properties are allowed to be used. But property theft is a huge concern in machine specific authentication. Mobile systems are vulnerable to property theft. Therefore, more security measures are needed.

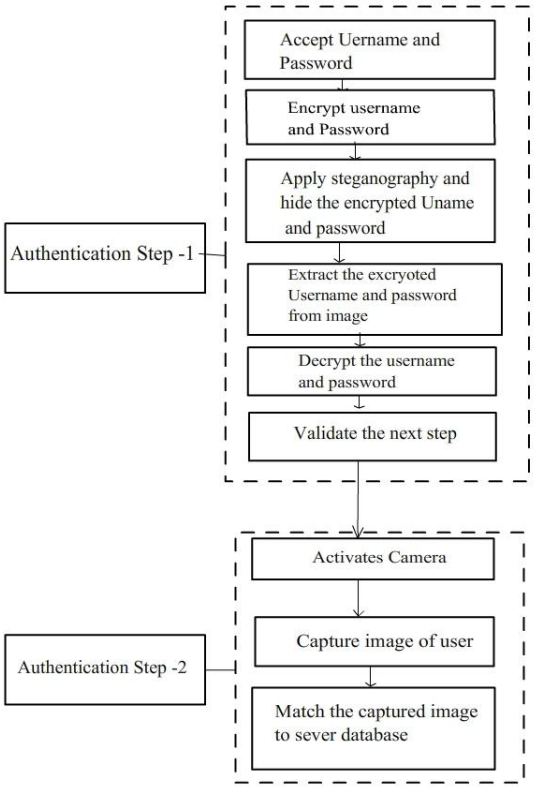
III METHODS FOR AUTHENTICATION

Authentications systems are much more complicated that they seem. A lot of calculations and algorithms are running in background. Many systems apply different techniques. But they all involve extensive use of cryptography [4]. Cryptography algorithms play an important role when information is being transmitted. They convert your plaintext in such a way that they are only readable when they are decrypted. However, a cryptanalyst can crack this encrypted plaintext if he gets enough information about the transmissions.

IJERT

IV PROPOSED SYSTEM

Our Proposed System Steganographic authentication in conjunction with face detection for mobile systems will comprise of two levels of authentications [1].



Product depends on external interfaces like Android Device. The overall architectural components can be depicted by the given diagram. In the above architecture, to steps are included for the authentication. 1st step consist of the username and password acceptance. And 2nd step consist of face detection and authentication if the face is matched to the database

Step-1: A user needs to provide his username and password. Then his Username and Password combination will get encrypted. The encrypted username and password will be hidden in an image i.e., applying cryptography.

Then the image will be transmitted over a network. At the server side the encrypted username and password will get extracted from the image. That extracted username password combination will be matched with the database when password is again decrypted.

Step-2: once the 1st step is successful, the mobile phone camera will get activated. Users face will get captured and then the captured image will be matched with the image data.

Both stages are extremely important as failure in one step would lead to authentication failure.

Flow of the Proposed System

Symbol	Description
C	Client
S	Server
AB - ¿ M	A sends M message to B
K*A*,*KA*−ˆ1	Public Key of A, Private key of A
H(M)	Compute hash value of M using one key hash function
M*KA*	Encrypt M using public key of A
M*KA*−1	Encrypt M using public key of A
Sig*A*(*M*)	A Signs digital signature of M: Sig*A* = *K*(*M*)*KA*−1
SessionID	Session Id
T*i*1, *Ti*2	Time-Stamp used by i message's request response

Communications in the proposed System

C ! *S* : *Request*1*k*, *SigC*(*Request*1), *kKS*, *T*11
S ! *C* : *SessionID*,*Response*1*k*, *SigS*(*Response*1), *T*12
C ! *S* : *SessionID*,*Request*2*k*, *SigC*(*Request*2),*T*21
S ! C: *SessionID*,*Response2k*,*SigS(Response2)*,*T22*

V ADVANTAGES AND LIMITATIONS

a. Advantages

a) Enhanced security with two levels.
Two levels will ensure that user is authenticates only and only when both the steps are levels are successful. Failure in one level would lead to failure in authentication [1].

b) Simple to use
this method is very simple and would have a strong resemblance to the existing authentication interfaces.

c) Image Transmission
Image is transmitted over a network and not the encrypted packet. This will fool an attacker who is listening to the network into believing that image transmission is going on [2].

d) Ease Availability: since the system is designed for mobile systems, due to the popularity of the mobiles. The proposed system would be available to large number of user.

b. Limitations

a) Property Theft: Property theft is a main concern. Mobiles can easily be getting stolen. This will result in the user acquiring a different mobile system and then again using that to authenticate.

b) Bright Environment: To capture an image effectively, user needs to be in a bright surroundings to get a clear image.

IJERT

c. System characteristics

The below table is based on various characteristics of Existing authentication systems. The classification is based on their popularity, simplicity, security and use in mobile systems.

Scales

1- Low
2- Below Average
3- Average
4- Above Average
5- High

System	Popularity	Simplicity	Security	Use in Mobile
Username Password	5	5	3	5
Biometrics	3	3	4	1
Machine Authent-ication	2	4	3	2

Scales 1-5.

VI. CONCLUSION

Authentication is an area of constant research and improvement. We have described a theoretical as well as practical approach to the problem producing a reliable authentication system. Now-a-days need of secure authentication increasingly. Especially on mobile systems as people access information more from mobile phones and PDA's and other small screen devices. In our Proposed system we provide extra measures to make authentication secure by introducing extra measures of security. Our system is most suitable for Authentication on mobile systems where resources are easily available. Our approach protects user from attackers.

IJERT

REFERENCES

[1] Dushyant Goyal and Shiuh-Jeng Wang. Steganographic Authentications in conjunction with Face and Voice Recognition for Mobile Systems, volume 01. 2011.
[2] Yagnik Harsharj A. G.L.Saini Krishan Kantlavania, Kothari Rooshabh H. Steganography Technique Based Mobile Banking System, volume 01. 2011.
[3] Ms. Aaradhana A Deshmukh Mrs. Geeta S. Navale, Mrs. Swati S. Joshi. M-Banking Security - a futuristic improved security approach, volume 8. 2010.
[4] Liu Zhuang. A Web Service Secure Model. South China University of Technology,GuangZhou-510640, P. R. China.
[5] Jessica Codr. Unseen: An Overview of Steganography and Presentation of AssociatedJava.

BIOGRAPHY

Prof. S.S. Shinde Is currently working as an Assistant Professor in Marathwada Mitra Mandal's Institute Of Technology, Pune, Maharashtra, India. Prof. S.S Shinde has completed M.E. (Computer) from University of Pune. His research Interest is Information Security.