Integration of Biometric based Authentication Mechanisms to Prevent 'Shoulder Surfing'

Hardik Garg
Ajeenkya D Y Patil University
Pune

Shibu Dubey
Ajeenkya D Y Patil University
Pune

Shabnam Sharma
iNurture Education Solutions
Bangalore

ABSTRACT

Nowadays the world has migrated to a social media platform where a social platform is prerequisite for data sharing which is done through texts, multimedia and electronic data over Whatsapp, Instagram, Messenger and many more common platforms where one may be talking about business plans, while some may be talking about their personal lives or they might be sharing any type of confidential information. But what if there are possibilities that someone else can access your confidential data or one can crack your passwords through performing social engineering attacks or many more patches if found and misuse your data or modify it, thus your data is at risk.

In today's era security is one of the major concerns and the deciding factor for the growth and advancement of the services through a vendor or to an individual, this security can be enforced through different medium either physical or biological security depends which is more preferable according to the scenario. The technology is working to develop a strong and authenticated security system which will not only authorize the user but will provide authentication parameters for the access of his/her data or data sharing platforms, thus trying to build and implement the advancement of biometrics which requires the measurement of biological characteristics such as fingerprint, retina image, iris pattern, retina image or palm geometry or the unique behavior characteristics using cryptography, technology traits and various secure algorithms and advancement in biometrics which will help to overcome the patches in confidentiality, integrity and availability of data.

Keywords

Authentication, Biometrics, Cryptography, Social engineering

1. INTRODUCTION

The traditional user verification technique does not provide proper security. But the advancement in biometrics will make it possible to authenticate an individual's identity rather than just providing authorization based on one's unique personal characteristics. So, implementing biometric in computer

Networks or in any organization or on to an individual level is a challenging technique. In this paper, there is a brief introduction to how advancements can be done in biometrics, their working and their role in computer networks and applications. Traditionally, access to these networks involves the use of a network login ID associated with a password or personal identification number (PIN). Biometrics will change all of these current trends. Biometric login process offers a significant improvement over the security of simple passwords and actually makes the user's life easier, rather than imposing a new burden. Instead of manually typing user names and passwords, all users need to do is click a button and lay their thumb or finger over the scan window on the keyboard or mouse. The software uses one or more databases to compare the fingerprints or other biological characteristics. Since the fingerprint of everyone in this world is unique these can be used for strong authentication.

Authentication and security has been the major issues from the beginning of computer as well as digital age earlier these security patches were tried to tackle through imposing some sort of physical security but as the technology got advanced modern parameters of security have been introduced but they also carry some bugs as well as loopholes which can be used to gain access over the protected system or resources, tough biometrics make it possible to tackle the existing challenges but the advancement in biometrics can be proved a boon in technology which would later known to be a blessings in the field of security.

1.1 Authentication is Generally based on One or More of Three Factors

- ✓ What you know
- ✓ What you have
- ✓ What you are

In general, traditional passwords or one factor authentication is the obvious example of 'what you know' talking about the biological geometry or biometrics are the example of 'what you are'.

1.2 Loopholes of traditional systems

Here, traditional system refers to password-based authentication. The problems associated with this type of systems are mentioned below:

a) The passwords can be guessed, stolen, or cracked.

b) In some environments, users deliberately share passwords for their own convenience. So, passwords may not be secured in such cases.

c) A system that uses only passwords to control access cannot authenticate whether the user identified with a password is really the authorized user.

d) Passwords are also costly to administer. Password hassles account for a significant portion of help-desk costs.

2. LITERATURE REVIEW

This chapter reviews the literature on biometrics enhancement [1]. The review of [2] focuses on studies which provide insight into the following questions: What factors adds up enhancement in biometrics security? What is the role of technology in the formation of two factor authentication, as mentioned in [4]? This idea and technique vitalize the enhancement of the security to the next level and helps u to rely on your personal device and ensure security features for you [5], as a multitasking device compromising security in the process is not upheld, from the study of past few research paper and ideas of biometrics security [6]. It helps in improved confidentiality trends, maintains integrity of data as well as authenticates and makes it available to the authorized person helping in improved efficiency and economical factors to flourish,[7] the thing which makes it ultra secure is that biometrics cannot be forged[8].The accuracy of a Biometrics system is measured by two different parameters FMR (False match or acceptance rate) the lower the biometric identification system's FMR, the better the security FNMR(False non-match or rejection rate), the lower the biometric identification system's FNMR, the easier the system is to use.[9]. Mainly in a digital world where the information is vital and confidential one need’s a secure platform to rely upon[10]

3. PROBLEM STATEMENT

There is serious problem of password cracking or password stealing through implementing various attacks and gaining unauthorized access to ones’ data and making it vulnerable where confidentiality of data may get weak and user’s data is compromised which makes its insecure and no privacy is left. Also, looking at the previous messaging applications like messenger and Instagram where it require password to open user account and if someone get to know or have cracked the password then he/she may be able to use and send messages through his account where the person on other side of chat to whom he/she is chatting is unaware whether the correct person is chatting with him/her so there should be an secure application which passes the CIA triad. There are features in some messaging apps which can be used for performing malicious activity like WhatsApp is having ‘whatscan’ feature which is designed to ease the data duplication if required over a different physical machine but if somehow unauthorized person came to knew the password he can perform and use this feature for doing illegal things and use this data further for malicious activity thus data is at risk. A person’s live biometric data is being matched against a bio print in the database, such as on a smart card. If it matches, it means that the person is who or she claims to be and access is granted. This process is called verification. Whereas in identification using Passwords the system only cares if the password is valid one and not care about whether the user using the password is authorized to use it.

4. PROPOSED SYSTEM

Well living in 21st century and taking a step towards future world, where the technology is getting advanced and nowadays in every mobile there is an inbuilt finger print scanner and as there is advancement in biotechnology and is contributing in IT industry, which is implementing the features of biometrics i.e. iris scanner, retina pattern, palm geometry and many more biological traits, using this features and technological features, technology can create an android application or implement the proposed security system in existing application which uses two factor authentication, where the first factor is finger print scanner in which the user has to pass through it and confirm that he is the authorized user of the resources but still there is no confirmation that is the authenticated user sending and receiving messages or not, so here comes the use of advancement in biometrics security system where after passing the first factor of authentication the user can open the application but still he will not be able to see the previous chats ,contacts ,status, the upcoming messages etc

To get access to these features and resources he has to pass through second factor of authentication i.e. iris scan or palm geometry every mobile will have biometrics for the owner which is unique so when the owner of the mobile will use the app the app will perform the iris scan and if the iris scan matches the user will be able to utilize all the features like chatting etc ,at a time only one biometrics will be scanned and only one user can get access to the resources at one time and if the other user tries to see the content or chats he will get to see the encrypted format of the texts and every content in the app making it the secure app developed ever.

5. SYSTEM ARCHITECTURE

This technology can build application which will prove to be one of the most secured messaging applications where two-factor authentication is done using biometrics i.e. finger print scanning and iris scanner. Every time user has to pass the first layer of security i.e. finger print scanner, as the user passes the first layer then also he will not be able to see the contacts and messages because it is in decrypted form, so if the user want to see the messages then he/she have to pass the iris scanner test and the test will pass only and only by the desired user which means no other can see the messages or send the messages and if anyone from behind is also looking at the chat then there will be two iris detected which again decrypt’s the message. The system architecture of proposed work is depicted in figure 1.

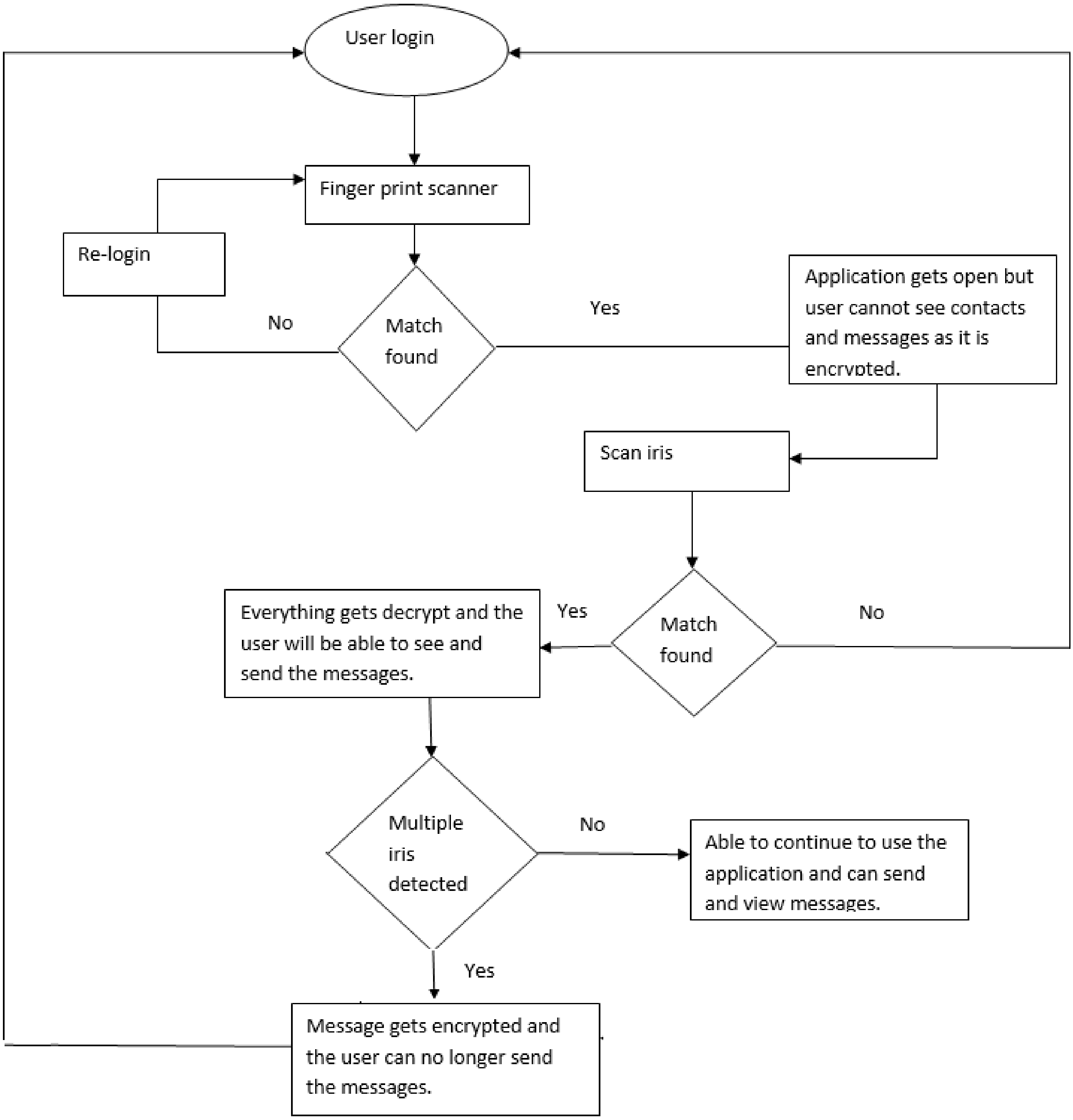
User login
Finger print scanner
Re-login
No
Match found
Yes
Application gets open but user cannot see contacts and messages as it is encrypted.
Scan iris
Everything gets decrypt and the user will be able to see and send the messages.
Yes
Match found
No
Multiple iris detected
No
Able to continue to use the application and can send and view messages.
Yes
Message gets encrypted and the user can no longer send the messages.

Figure 1: System Architecture of Proposed System

6. ADVANTAGES

1. New layer of security is added using biometrics which compose of two factor Authentication.

2. Passes the three triads i.e. confidentiality, integrity and availability.

3. No other user than the desired user will be able to see and send the messages which makes it one of the most powerful application till now.

4. The user on the other end of chatting is sure that the person to whom he/she is chatting is the intended person, no other person is chatting or misusing the app in his/her absence.

5. No other person can see the messages or with whom he had chat previously even if he passes the first factor of authentication or the application is left open.

7. PSEUDO CODE

Algorithm 1: Biometric identifier

```
DATA: Input fingerprint

RESULT: Authorized/Non-authorized

BEGIN:
    compare input fingerprint(fg) with database
        if (fg == fingerprint stored in database)
            Authorized user;
            Algorithm 2;
        else
            Not authorized;
            rejected;
            Application will not open;
END
```

Algorithm 2: Iris Scanner

```
DATA: Input iris scanner

RESULT: Able to decrypt contacts and messages/ encrypted
message and contacts

BEGIN:
    Compare scanned iris(ir) with database
        if (ir == iris image stored in database)
            Authenticate user;
            Algorithm 3;
        else
            Not an authorized user and no authentication;
            rejected;
            contacts and messages will be encrypted;
END
```

Algorithm 3: Encryption and Decryption Process

```
DATA: Authenticate user iris

RESULT: Able to view and send messages

BEGIN:
        1. authenticate user(au) is using app
        if (au == using an app)
            Able to view contacts and send messages;
        else
            Not be able to view the messages and contacts;
        2. More than authenticated user iris detected
        if (ma == app)
            messages and contacts will again get encrypt,
END
```

8. CONCLUSION

In this research work, integration of biometrics along with two-factor authentication is done. The motive of the research is to propose a technique in order to avoid shoulder surfing. Iris scanning is used as biometric-based authentication, in this work. In future, implementation of proposed technique will be carried out, using appropriate technology.

9. REFERENCES

[1] Zhang, D., Lu, G., & Zhang, L. (2018). Advanced Biometrics. Springer International Publishing.

[2] Zhang, D. D. (2013). Automated biometrics: Technologies and systems (Vol. 7). Springer Science & Business Media.

[3] Chao, L., Yang, Y. X., & Niu, X. X. (2006). Biometric-based personal identity-authentication system and security analysis. The Journal of China Universities of Posts and Telecommunications, 13(4), 43-47.

[4] Duta, N. (2009). A survey of biometric technology based on hand shape. Pattern Recognition, 42(11), 2797-2806.

[5] .Monrose, F., & Rubin, A. D. (2000). Keystroke dynamics as a biometric for authentication. Future GenerKhitrov, M. (2013). Talking passwords: voice biometrics for data access and security. Biometric Technology Today, 2013(2), 9-11.ation computer systems, 16(4), 351-359.

[6] Khitrov, M. (2013). Talking passwords: voice biometrics for data access and security. Biometric Technology Today, 2013(2), 9-11.

[7] Schneier, B. (1999). The uses and abuses of biometrics. Communications of the ACM, 42(8), 136-136.

[8] Fenu, G., Marras, M., & Boratto, L. (2018). A multi-biometric system for continuous student authentication in e-learning platforms. Pattern Recognition Letters, 113, 83-92.

[9] Fierrez, J., Morales, A., Vera-Rodriguez, R., & Camacho, D. (2018). Multiple classifiers in biometrics. Part 2: Trends and challenges. Information Fusion, 44, 103-112.

[10] Elhoseny, M., Elkhateb, A., Sahlol, A., & Hassanien, A. E. (2018). Multimodal biometric personal identification and verification. In Advances in Soft Computing and Machine Learning in Image Processing (pp. 249-276). Springer, Cham.