International Journal of Scientific and Technical Advancements

ISSN: 2454-1532

Biometrics Security in Mobile Application Development & its Applications

Akanksha Bali[1], Shivangi Goswami[2], Shagun Sharma[3]
[1,2,3]Computer Engineering Department, YCET, Jammu, J&K, India-181205
Email address: [1]akankshabali5@gmail.com , [2]pihugoswami303@gmail.com, 3sshagun386@gmail.com

Abstract: Smart Cell phones are evolving very rapidly making manufacturers introduce various features in small devices and become incredibly important in every aspect of our life nowadays as well as come to be powerful in terms of storage, cpu and installing numerous applications. Biometric technology that differentiate physical or behavioral characteristics like fingerprint sensor to provide identification (who are you?) and authentication (who he/she claims to be), high resolution camera, iris scan provides developers various tools to combine them into one application. Mobile banking is very famous these days because of large development in smartphone industry. To make secure payments through mobile phones Biometrics like FP identification are considered as one of the most effective authentication for everyone. The present security issues surround the loss of personal information through the pilferage of the cell phone. Hence, it is necessary that the biometric identification templates are not surely stored on the phone but will assemble at run time. Various secure algorithms are used to prevent from various to provide enhanced security. Biometrics systems will be present everywhere in the society, such as education, government, smart cities etc. The technological which made smart phones an essential component of our daily lives are GSM, GPRS, 3G, 4G, WiMAX, Blue-tooth and Wi-Fi. However, this rapid growth in technology and enormous utilization of the smartphones make them resistless to malware and other security breaching attacks. In this paper, we review fingerprint recognition technology, a popular biometric security feature, to develop a web login authentication mobile app. In this paper we focus on summaririzing research work carried out in fingerprint matching methods, recognition techniques, and performance analysis. In this paper we also review some of the research issue and tools used under mobile application development.

Keywords: Biometric, Fingerprint, Biometric security, Mobile Banking, Mobile Payment, Android, Threats, Attacks, Malware, Multifactor Authentication. Mobile Devices, User login.

I. INTRODUCTION

Biometric recognition means the user authentication by using different biological features i.e. face, fingerprint, retina, iris (physical attribute), hand geometry and voice, signature, keystrokes (behavioral attribute). These attributes (traits) are known as simply biometrics or biometric identifiers. A biometric system may work either in Identification mode or in Verification mode but before the system can be put into identification or verification mode, a database system composed of templates(biometric) must be generated through the procedure of enrollment. With the world getting more digital and connected, cyber-security possesses supreme importance. Hackers can hack a network, and do massive damage by shutting down digital coordination systems. Hence computer systems are needed to have vigorous and extra ordinary security authentication. A password is always the weakest medium in the entire chain even in organizations that spend millions of dollars for security. This is where biometric systems can play a important role in enhancing the security and privacy of cyber systems. Hence, a fingerprint or iris recognition is used due to less chances of getting hacked. Security identification and authentication machines are the biometric devices available in the market. These biometric devices use automated methods having physiological features like Iris prints, facial images, fingerprints, and voice recognition to identify a person. It improves the convenience of routine transaction and increases efficiency in fraud reduction. Mobile application development companies are exploring various mobile applications for biometric systems with the development of the facial recognition and fingerprint sensor in the latest Android smartphones and iPhones. Mobile phone technology with touch-sensitive screens, front-facing camera and microphones is the central focal point for the execution of these applications, called “multi-modal” biometric systems. Facial Recognition, iris scan, voice recognition, Fingerprint, Hand geometry, signatures scan are the biometric technology used. Universality (every-one should have this attribute), Uniqueness (different values for different persons), Permanence (should be invariant with time), Collectability (can be measured quantitatively), Acceptability (peoples should willing to accept it) and Circumvention (how easy it is to fool the system) are the qualities of ideal biometric trait. [1]

A) Verification and Identification Process

Verification and identification are the two characteristics for biometrics security shown in fig[1]. **Verification** is a one to one (1:1) matching process, where the user states an identity and the system confirm whether the user is authentic or not. If the template of the stated identity and the goals of user’s input are greater than threshold value, then we can say that state is accepted as “authentic” otherwise, the state is rejected and the user is considered as “fraud”.

Identification is a one to many (1:N) matching process in which the goals user's input is compared with the templates of all the persons in the database enrollment and the identity of the person whose template has the highest degree of equivalence with the user's input that is processed by the biometric system. If the highest equivalence between the input and all the templates is not equal to or greater than a predetermined minimum threshold, then system rejects the input, which means that the input presented by the user does not belong to the enrolled users. [1]

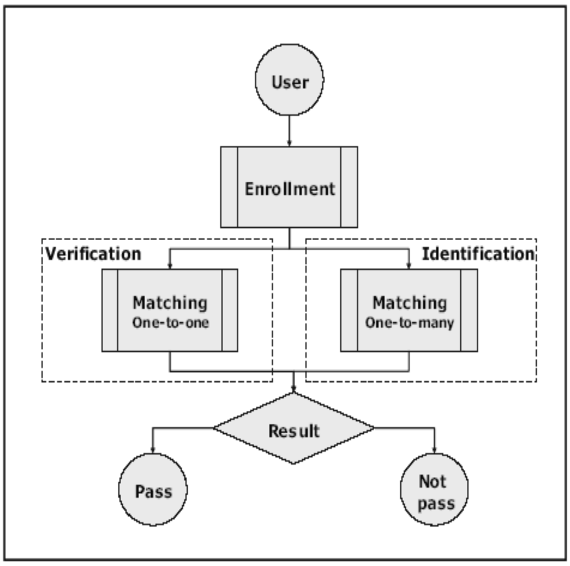

Fig 1: Verification and Identification method [2]

In the enrollment method, user samples are collected, extract their feature and stored in the database and then compare the person's identity with the stored template in database to authenticate it as shown in fig [2]:

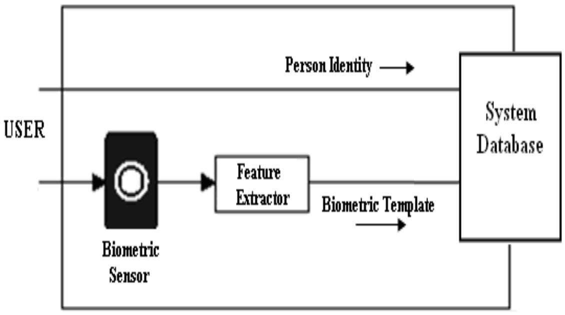

Fig 2: Enrollment Constituting Database [2]

B) Attacks in Biometric Authentication System

In fig[3], numbers like 1,2,3and so on represents attacks and their working is explained in table[1]

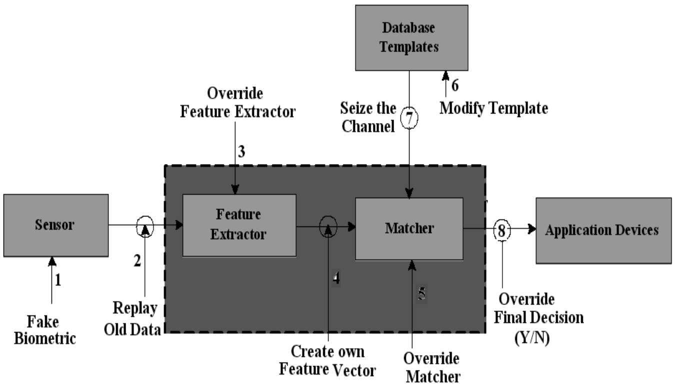

Fig 3: Attack Points in Authentication System [3]

Table 1: Working of Attacks in biometric authentication system. [3]

Attacks	Meaning(Working)
1	It shows a fake biometric (e.g., face, synthetic fingerprint, iris etc.) to the sensor.
2	It can be achieved by submitting a previously intercepted biometric data.
3	It takes place when feature extractor module accepts standards to produce feature values selected by the attacker. It replaces authentic feature values with the ones selected by the attacker.
4	It modified the results of feature extractor modeule because the channel between matcher and feature extractor module is hacked and override by duplicated data.
5	It is attained by imposing an man made high score at matching module
6	It occurs when there is attack on the template database (e.g., modifying an existing template, adding a new template, removing templates, etc.)
7	It results alteration of the transmitted templates due to the hack of the transmission medium between matcher and the template database.
8	Matcher result (accepts or reject) can be overridden by the attacker.

C) Comparison of Various Biometric Attributes

Biometric attributes cannot be forgotten. They are difficult to copy and share. It is necessary for the person to be present at the point of authentication for being authenticated. The Comparison of various attributes like universality, uniquen4ess, permanence, collectability, performance, acceptability, circumvention is given in table [2]. **[1]**

Table [2]: Comparison of biometric attributes **[1]**

Biometrics	Universality	Uniqueness	Permanence	Collect-ability	Performance	Acceptab-Lity	Circumvention	Biometrics
Face	High	Low	Medium	High	Low	High	Low	High
Fingerprint	Medium	High	High	Medium	High	High	Medium	Medium
HandGeometry	Medium	Medium	Medium	High	M	Medium	Medium	Medium
Keystrokes	Low	Low	Low	Medium	Low	Medium	Medium	Low
Hand veins	Medium	Medium	Medium	Medium	Medium	Medium	High	Medium
Iris	High	High	High	Medium	High	Low	High	High
Retinal scan	High	High	Medium	Low	High	Low	High	High
Signature	Low	Low	Low	High	Low	High	Low	Low
Voice	Medium	Low	Low	Medium	Low	High	Low	Medium
Face	High	High	Low	High	Medium	High	High	High
Odor	High	High	High	Low	Low	Medium	Low	High
DNA	High	High	High	Low	High	Low	Low	High
Gait	Medium	Low	Low	High	Low	High	Medium	Medium
Ear Canal	Medium	Medium	High	Medium	Medium	High	Medium	Medium

D) Deformations in Biometric system.

Obtaining high-quality templates of different fingerprint ridges and minutiae is a complex task. People with no or few minutiae points cannot enroll the system. Results can also be rejected by wrong minutiae point due to low-quality enrollment, fingerprint ridge and imaging detail. Cold finger, oily finger, humidity, angle and pressure of placement are some of the examples of deformation in biometric system. Various Deformations are shown in Figure 4. [2]

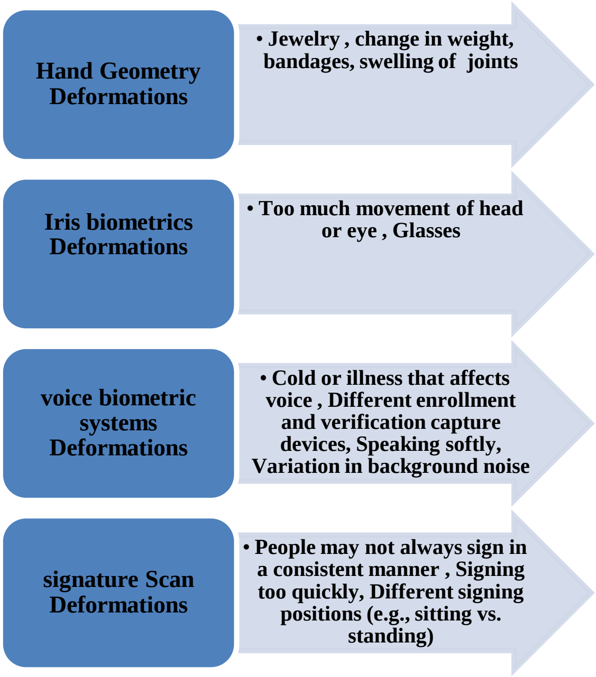
Hand Geometry Deformations
• Jewelry , change in weight, bandages, swelling of joints
Iris biometrics Deformations
• Too much movement of head or eye , Glasses
voice biometric systems Deformations
• Cold or illness that affects voice , Different enrollment and verification capture devices, Speaking softly, Variation in background noise
signature Scan Deformations
• People may not always sign in a consistent manner , Signing too quickly, Different signing positions (e.g., sitting vs. standing)

Fig 4: Various biometric system deformations

II. Multi-Biometric System

A Multibiometric system do data acquisition by using multiple sensors. It captures multiple samples of a single biometric trait or Samples of multiple biometric traits. Sources of multi biometric system is shown in fig 5

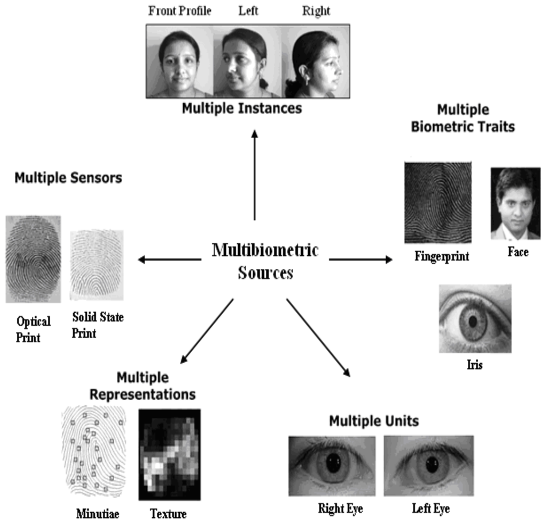

Fig 5: Sources of Multibiometric System [2]

a. Vigorous Multimodal Recognition

Conventional biometric recognition systems depend on a biometric signature for authentication. However they face certain unavoidable problems, which can be controlled by using multimodal biometric systems. Characterization in multi-biometric systems can be done by combining information from different modalities like visual sense, sense of taste, audition, sense of hearing. It can be done at different steps - feature step level, score step level or decision step level fusion. Feature level fusion can be more differential than score or decision level fusion. But, it has been rarely discussed in biometric community. [2]

III. Research issue in Mobile Application Development

The various research issue comes during mobile app development are given below

- Adaptive Web based Systems
- Multi-Modal & Multi Touch interaction
- Virtual reality
- Visualization
- Software Variability
- Flurry of Launches or Smartphone space
- GSMA embarks on LTE interconnection standards
- Mobile Sensor Network
- Environmental Monitoring
- Traffic Accident Detection System
- Security Issues
- Data & Functionality Migration

a. Tools

Some of the tools given below which gives platform for mobile app development are

- Altova-Altova MobileTogether(32 and 64 bit)
- Android-(Eclipse,Android Studio)
- BlackBerry-(Eclipse, BlackBerry JDE)
- Corona SDK-(Xcode)
- Intel XDK-(IntelliJ IDEA)
- IOS SDK-(Embarcadero Delphi)
- Java ME-(Eclipse,NetBeans)
- Flash Lite(Adope Flash)
- Mono for Android-(Visual Studio 2005 and above)
- MonoTouch-(Visual Studio 2005 and above)
- RubyMotion-(RubyMine)

IV. Literature Review

In this paper [4], G.Ogale et.al proposed architecture composed of architecture user, sensor and database. The author explained the method of execution. Firstly install and run the application in the smart-phone device. When the application is installed, the sensor task is given to a user for verification like touching of finger for fingerprint scan, recording of voice by voice detector, capture image of eye for retina or iris scan. When the user accesses some application, the server unit contrasts the template captured with the one which is encrypted and stored in database. After which the device and the user is verified. Now, the user is able to access all its data within the screen. Once the user selects any option from the screen, the application asks for verification to finish the transaction. This two step authorization approaches the demand of establishing stronger authorization to the user. The templates are now matched and the transaction is completed. All these steps prevent fraudulent activities and provide more security with safe transaction.

In this paper [5], R. Subban et. al presented the related works and performance analysis for fingerprint biometric and showed that the performance evaluation is done on surveyed works with different parameters and existing methods. Biometrics gives noticeable advantages over password and token-based security. The author discussed about various issues related to uni-modal biometric systems. The security and privacy covers that biometric authentication raises need to be addressed. It is surveyed by author that automatic fingerprint recognition is the best biometric technology for security from an analysis of the requirements: usability, security, ruggedness, form, size, factor, privacy and operational temperature range.

In this paper [6], M. Belkhede et. al. authors have focused on how biometric mechanism provides the highest security through use of biometric authentication system to the mobile payment due to the misuse of personal information through the loss of the mobile phone. A payment application would be initialized onto a smart android device, for authentication and verification; finger print is taken at run time. The finger print template would be compared against a stored template on a database server and is encrypted by using the RSA algorithms and then sends it to the host server (i.e. Bank). For the mobile-banking application, smart phone will act as a client and the website of bank will act as a host server. Fingerprint is used for the purpose of login and sent it to the host server for matching as request and then waiting for the reply message from host server. Transaction is done by user only if login is successful. In this paper author use the encryption technique and proposed design approach for a biometric mechanism for enhanced security of online transaction on Android system so that no one can hack the fingerprint template. It can be used in M-Commerce and mobile banking. To provide high level security mechanism for mobile payment system, authentication request and reply are put in encrypted form. For mobile transaction, run time fingerprint is taken. To provide more security from third party, it is not stored in the database table.

In this paper [7], M.F.Zanuy et. al presented the criteria which biometric technology depended upon. It assumes that an individual has universal characteristics i.e. identical twins will also differ. The feature must be secure, stable and quantitatively measurable. The hacking of biometric technologies should be negligible also it must be accepted by everyone without experiencing any invasive content. Parameters for biometric security includes face, hand geometry, iris scan and so on. Fingerprint authentication is considered perfect because it not only recognizes the features but also authenticates the characteristics as well as it is preferable because fingerprint remains as it is throughout life and pattern of ridges remains identical an individual.

In this paper [8], S.L.Nita et.al focused only on the machine learning, and data clustering, algorithms with its applicability in the cloud computing environment. Tools used for tests are virtual machine (Virtual Box) with Biometric Analysis and Apache Hadoop tool. The Vulnerabilities and issues found in these algorithms. The purpose of the scheme is to give a big overview on how to use it in real life, and how to use the algorithms. In this paper, author throw some light on the most challenging aspects on how to design, implement an authentication system depend upon biometric features and explained by applying cryptographic mechanisms, machine learning and clustering algorithms over biometric data is not an easy task to complete due to the high complex method of scanning, reading and transferring of biometric data into the system. Every time during the evolution of technology, security and integrity of data becomes the real pain for developers of authentication systems. The paramount characteristics on which author paid attention in this work paper is how the parameters can be represented and adapted in the algorithms and methods used in machine learning and cryptography. Author shown that Blowfish and AES are having the best performance compared with several algorithms, such as SHA-256, RC4, RC5, RC6, MARS, TWOFISH, THREEFISH, RSA (Rivest-Shamir-Adleman), Elliptic Curve, and Diffie Hellman. Various secure algorithms like RSA, AES, SHA-256, RC4, RC5, RC6, BLOWFISH, MARS, TWOFISH, THREEFISH, Diffie Hellman and Elliptic Curve are used to prevent from various attacks like a man in middle and to provide enhanced security.

In this paper [9], S.M.Mahmood et.al presented various techniques as well as methods for security measurements and analysis within the peak of mobile platforms. Author highlighted various security issues and threats faced by smart phones compared to the PCs and explained how hackers are looking for different ways to breach smart phones by making communication more difficult. Therefore, security is one of the challenging activities which need to be taking into consideration during the developing phases and this can be done through manufactures access points or API's (Application Programming interfaces) within different popular platforms such as Android and iOS. Due to rapid increase in number of end users (who are downloading applications), high level security mechanisms are required during sign-in application. Hence, mobile applications simplified the way that applications can be used for: social, business, networking, travel, shopping, education, network utility and banking and its can be used to tackle each and every aspect of life. In this paper, author conclude, further education for user about how to use mobile safely to degrade the number of data lose, attacks as well as threats.

In this paper [10], S.F.A.Zaidi et.al firstly review the vulnerabilities, threats, attacks and their solutions during a period of 2010-2015 with a special attention on smart-phones and secondly, examine findings and judge the market growth of distinct operating systems for the smart-phone in coming years. Author categorizes smart phone security problems into vulnerabilities (defects, lack of user awareness, insufficient management of apps, unsecure wireless networks), authentication (Pin, token, biometric), Data Protection and Privacy and attacks (old (physical attacks, virus, black door, threat, Trojan, malware, worms, spam) and new attacks(relay, USSD, Brute force, counter, DOS,XSS and so on)). Most of the smart-phone attacks occur due to vulnerabilities and it can be saved by minimizing the vulnerabilities. It is very tedious to achieve 100% security in rapidly growing field where development occur at large scale, but the careful design lead to more secure smart-phones. Today is world of internet of things where the devices include electronic devices, machines, vehicles and security based entrances remain online and interconnected so that each routine gadget would be controlled by smart-phone. This will create a lot of problems regarding smart-phones such as performance issue, battery drainage issue and security and privacy issues like illegal access to the personal devices via IoT. So, there is a need of smart-phone that used for IoT, must have best battery consumption, efficient processing, maximum security and be able to achieve maximum benefits from IoT**.** In this paper author discussed the latest authentication problems, data protection, security and privacy problems and investigated the vulnerabilities and attacks occurs in smart-phones. Author also focused on why attacks occur and what are their effects on smart-phones and studied about existing security results to prevent smart-phones from malicious codes, intruder's attacks and infections.

In this paper [11], S.Roy et.al proposed multi-factor authentication which takes a combination of several factors of authentication. Popular email services such as Yahoo mail, Gmail and others have consolidated multifactor authentication by asking users to enter their password, followed by entering a OTP sent to their registered phone numbers via text message. Multi-factor authentication improves the quality of verification, but can still be vulnerable to attacks. For example, if a harmful user theft both the smart card and password of authorized and legal user, the attacker can obtain access to the user's personal account. So, Authentication based on biometric techniques like iris patterns, retinal patterns and fingerprints is also employed due to insufficiency of security provided by both password and OTP. Biometrics improve authentication, but they increase the complexity and are expensive to implement. In this paper, author provided an overview of authentication using biometrics in mobile device and then considered a specific case study of biometric authentication using the Fulcrum fingerprinting scanner and the iPads and outlined the steps required to set up a biometric authentication system. It was implemented using secure internal network of the organization and challenges faced when the same system is to be implemented over an insecure network. In this paper, author did not use any indexing technique to improve the search for a possible fingerprint in the database during authentication. The fingerprints were stored in the database in the bit stream form generated by MINDTCT. AES Algorithm is used to store the bit streams in an encrypted format to provide security and that would have the extra cost of decryption during authentication.

In this paper [12], Nilay Yıldırım et al explored how the fingerprint biometric feature on mobile devices can provide security for web login and initiate a program that make single time passwords for login to a web site on a registered device via fingerprint. This is required that the user saves their fingerprint and logs in to the application with that IMEI number. The importance of the biometric fingerprint features is high in terms of providing the security of applications. The Android-based application has been developed with Pass SDK that is offered to developers by Samsung, and Android application security, available to developers of third party applications, to ensure the protection of mobile applications or for different ideas about fingerprint identifications. They developed an application that gives an idea of how to use the biometric features in a mobile device to authenticate web-based user account so that user login will become more secure for the web sites that are important to authenticate the user. Single use password, the fingerprint biometric security and the IMEI number that identifies user mobile device are the three security features utilized in our application and it meets the belief of a multi-layered security system. The user can open the program with entering his or her user name and password information and fingerprint recognition without saving the IMEI number. Author also explained that the method of recording IMEI number , pass SDK in terms of security measures, use fingerprint records for authentication on web platforms are neither convenient nor practical and we can say that are not possible to use. Only Fast Identity Online (FIDO) perform user authentication with the unique ID of the fingerprint without the need of IMEI number.

V. Future Work

Our future work is to design Fingerprint authentication systems that have unique characteristics, consistency and performance by using multi-modal and multi-biometric system. Multi-biometric systems promise significant improvement over single biometric systems, for example, higher accuracy and increased resistance to spoofing Also it increases universality, uniqueness, acceptability, collectability and permanence by integrating three biometric features namely iris scan, finger print and voice scan so that no mobile threats occur and it will be safe to M-commerce, mobile banking and also prevent mobile app from various frauds. Our main aim is to provide biometric security and internet of things in mobile app development to increases efficiency, scalabilility, trustability, performance of mobile devices or smart phones.

VI. CONCLUSION

In this paper we review how Mobile device producers such as samsung insert biometric identification features to devices to enhance their security features and opened up access to their own FP recognition characteristics via SDK for third party developers. In this paper, we reviewed how the fingerprint security characteristics on mobile devices can provide security for web login. With the quick production of smartphones prepared with many characteristics such as sensors and several connectivity links, the mobile malware attacks are growing. Smartphones have limited resources, including processing units and power. As different types of links, services, sensors and secrecy, these are misused by attackers by increasing the capabilities of the smartphone. In this paper, we reviewed the latest authentication problems, data protection and privacy problems and also findout the the vulnerabilities in smartphones and attacks occur in smartphones and their effects in smartphones. Finally, we have reviewed existing security outcomes to prevent smartphones from malicious attacks, intruder's attacks and infections. Therefore, mobile applications handle each outlook of our life and simplified the way that apps can be used for: business, social networking, shopping, travel, education, banking and network utility. Moreover, security is one of the probable and demanding activities which need to be taking into consideration during the developing phases. In addition, developers must review their application‘s levels of security within different widely used platforms such as iOS and Android. It can be found out that the numbers of mobile end users who are downloading applications are increasing rapidly. Therefore, better security mechanisms should be needed during application login. To conclude, further education for user about how to use mobile safely found to be critical to reduce the number of data lose, attacks as well as threats.

Table 3: Comparison of different biometric techniques

Biometric Technique	**Advantages**	**Disadvantages**	**Applications**	**References**
Fingerprint	• Easy to handle and work on it. • Low power consumption • Inexpensive • Medium catholicity approach • High distinctiveness • Higher execution and	• Susceptible to error • Ink seems to be annoying for users using classical methods • Distortion occurs due to optical illusion of device • Not recommended for mass market production • Get affected during injury	• In getting documents like adhaar card • Forensic department • Mobile phone authentication • Banking authorization • Driver license autrhentication • Organization access	[6][7][13] [14]

	implementation • High durability		control • In issuance of visa	
Face	• High resolution and quality • High catholicity approach • Durable • Easily identify an individual among the crowd • Do not need any direct contact of a person in order to verify identity of a person. • Uers friendly design	• Not effective for less resolution images • Low distinctiveness • Slow implementation and execution • Bad light effect • Not effective work over gain/loss in weight of face	• Mobile phone authenticity • Maintaining records in school and colleges • Official purpose • Criminal identification • surveillance	[4][7][13] [14]
Voice	• Doesnot require any training and faster than other biometric techniques • Easy to operate • Low cost • Readily available • Depend on text • Focus on word/phrase pronunciation • Medium catholicity approach • Helpful for those who are unable to use their hand or suffer a problem during typing	• Low distinctiveness and durability • Get affected during illness • Slow execution and implementation. • Affected through noise and far microphones • Prerecorded voice messages hacking • Affected with similar words like to, two, too and unable to judge it correctly	• To identify criminals • Mobile authentication	[7][13]
Iris/Retina	• Stable throughout life • Due to fine texture, each has independent iris textures • Non intrusive data collection • High recognition, scalability and accuracy even though a user is putting contact lenses. • Easily recognition false irisis • High execution and implementation and high catholicity approach	• Eye position maintenance seems to be difficult for user • Require additional efforts • Increase/decrease in spectacles range • Affected by unsual lighting effects from reflective types of surfaces • Very costly in camparison to additional biometrics • Vulnerable to inadequate image quality • Inadequate to perform well at a distance larger than few metres.	• Forensic department • Mobile authentication • Security (NASA, lands, sea port, air) • Ophthalmological diagonosis • Adhaar card identification • Access Control	[7][13][14]
Hand Geometry	• Needs less storage • Can work in small template size • Low cost processor can be used • Low maintenance cost • Medium catholicity approach • Highly durable • Easily executed and implemented	• Gets affected during injury • Fets afftected during increase in decrease of weight of hand • Affected by increase in height of individual	• Military purpose • Forensic Department • Nuclear power plants	[7][14]
Fingervein/hand vein	• Distinctive to every individual • Less invasive • Hard to steal • Cant be duplicated • Less affected by change in health and	• Loss of finger during accident cause problem • Larger size of CC camera • Government have not proven this technology yet • Not for bulk recognition	• Driver identification. • Security system(door) • Sign in authentication • Bank and financial services • Transport, hospitals, schools and so on.	[13][14]

	weather conditions • Rashes and cracks don't affect it • High accuracy • Also work with low image resolution • Less expensive			
Lip	• Unchangeable • Small template size • Passive biometric means no need of person interaction • It can be hybrid like lip voice and lip face	• Requires lot of attention • Big smile may cause difficulty in recognition of a person	• Financial transaction authentication • Access control • In ATM machines transaction	[13][14]
Palm Print	• Highly distinctive • Suitable than fingerprint • Highly reliable and permanent in nature • Highly recognizable with low resolution cameras	• Expensive and bulkier • Not produce good results for low quality images •	• Personal identification • Atheletes selection • Medical diagnosis • Blood relation identification	[14]
Gait	• Non invasive • Easily obtainable from distance • Useful for obtaining medical disorder.	• Not accurate and reliable • Vary with time • Costly computations	• Medical diagnosis • Forensic department •	[14]
Body odour	• Identification through mixture of odors	• No existing applications • Difficult to sense due to deodorants and perfume • No well for artificial noses	• surveillance • Forensics department	[14]
Ear	• Constant size, appearance • Stable, less complexity, and less processing time • Quick identification	• Affected by hairs, earings, hat and so on • Not distinctive • Poor recognition due to loss of ideality in images.	• Surveillance • Forensic department	[14]
DNA	• High accuracy • Higher distinctiveness than any other biometric trait	• To get desired output, obtaining of sample is time consuming process • Privacy issues • Large storage space is required • Affected by degradation of sample • Expensive and high processing time	• Proving innocence • Network security	[14]

References

[1] H.Srivastava, " A Comparison Based Study on Biometrics for Human Recognition", *IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727, Volume 15, Issue , PP 22-29, sep.-Oct.2013.*

[2] https://studylib.net/doc/5801191/chander-kant

[3] M.Kumar, K.S.Vaisla, "To study of various security attacks against Biometric template in a generic Biometric Recognition System", Proceedings of the Second International Conference on Research in Intelligent and Computing in Engineering (RICE), DOI: 10.15439/2017R57 ACSIS, Vol. 10 ISSN 2300-5963, pp. 235-240, 2017.

[4] G.Ogale, P.Hatte, A.Sutar, P.Chaudhari and A.M. Wade," Survey on Biometric Authentication in Mobile Banking", IJIRCCE, Vol. 5, Issue 5, ISSN(Online): 2320-9801, *pp. 231-233, jan 2017,* DOI: 10.15680/IJIRCCE.2017. 0501033.

[5] R.Subban, D.P. Mankame, "A Study of Biometric Approach Using Fingerprint Recognition", Lecture Notes on Software Engineering, Vol. 1, No. 2, pp. 209-213, May 2013, DOI: 10.7763/LNSE.2013.V1.47 209.

[6] M.Belkhede, V. Gulhane, P. Bajaj," Biometric Mechanism for enhanced Security of Online Transaction on Android system: A Design Approach", ICACT, ISBN 978-89-5519-163-9, pp. 1193-1197, Feb 2012.

[7] M.F. Zanuy, "Biometrics Security Technology", IEEE Aerospace and Electronic Systems Magazine, Vol.21 nº 6, pp.15-26, ISSN: 0885-8985, June 2006.

[8] S.L.Nita, M.I.Mihailiscu, V.C. Pau," Security and Cryptographic Challenges for Authentication Based on Biometrics Data", www.mdpi.com/journal/cryptography, pp. 1-22, 2018, doi: 10.3390/cryptography2040039.

[9] S.M. Mahmood, B.M. Amen, R.M. Nabi," Mobile Application Security Platforms Survey", International Journal of Computer Applications (0975 – 8887), Volume 133 – No.2,pp. 40-46, January 2016.

[10] S.F.A. Zaidi, M.A.shah, M.Kamran, Q. javaid, S.Zhang," A Survey on Security for Smartphone Device", *(IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7, No. 4, pp: 206-219, 2016.*

[11] S. Roy, S. Matloob, A. Seetharam, A.Rameshbabu, W. C. O'Dell, W. I. Davis," Biometrics Data Security Techniques for Portable Mobile Devices", Indian National Academy of Engineering, Springer, DOI 10.1007/s41403-017-0026-8, pp. 123-131, 2017.

[12] N. Yıldırım, A. Varol, "Android Based Mobile Application Development for Web Login Authentication using Fingerprint Recognition Feature", *IJCSMC, Vol. 5, Issue. 10, pp. 61-68, October 2016.*

[13] R.Saini, N.Rana, "Comparison of various Biometric Methods", International Journal of Advances in Science and Technology (IJAST), ISSN 2348-5426, Vol 2 Issue I, pp. 24-30, March 2014.

[14] T.Sabhanayagam , Dr. V. Prasanna Venkatesan and Dr. K. Senthamaraikannan, " A Comprehensive Survey on Various Biometric Systems", International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 5 pp. 2276-2297, 2018.