Group 12 - An Analysis of Various Authentication Mechanisms in Mobile Systems

Sagar Parekh [Leader]
sjparekh@asu.edu

Arvinthan Sundaram Govindaraju [Deputy Leader]
asunda25@asu.edu

Mugdha Kolhe
mkolhe@asu.edu

Achyutha Bharadwaj
asbhara2@asu.edu

Sai Pragna Etikyala
setikyal@asu.edu

Venkatesan Murali
vmural17@asu.edu

Prajwal Kodi
pkodi@asu.edu

Harish Ravichandran
hravich4@asu.edu

Dhrumil Shah
dpshah8@asu.edu

The School of Computing, Informatics and Decision Systems Engineering

Arizona State University, Tempe, AZ 85281

Submitted to: Professor Dr. Stephen S. Yau

Summary:

In the last few years, Mobile devices have become integral part of our everyday lives. They enable us to access a large variety of ubiquitous services such as Emails, Messages, Banking, Investing, etc., many of which contain sensitive information about the user. Therefore, mobile devices have become ideal target for malicious attacks. Once the information on these devices is compromised, it is difficult to recover and the process is too expensive. The most effective way to prevent such attacks and secure user's privacy is by building strong user authentication mechanisms. With this project, we have analyzed various kind of traditional authentication mechanisms like PIN, Password, Pattern based, fingerprint, voice and many more and also novel authentication systems like behavioral profiling, touch dynamics, keystroke based, token based, periodic, gait based, multimodal, location based, gesture based, continuous authentication mechanisms. As the number of vulnerabilities and, hence, of attacks increase, the authentication techniques have improved greatly as well and research are still taking place for further enhancements. In this project we also present an in-depth analysis of vulnerabilities of authentication mechanisms and methods to overcome those vulnerabilities in context to mobile devices.

Table of Contents:

1. Introduction:

1.1. Background and Motivation:

Mobile security can be defined as protection of portable computing devices (laptops, smart phones, tablets) from the threats and vulnerabilities. Usage of portable devices which are connected to internet has been increasing exponentially every day. Almost two-thirds of the world are connected by mobile phones on which sensitive personal information is being stored. With exponential increase in organizations moving towards expanding their mobility in order to engage more customers on different platforms, mobile security has become one of the biggest challenges. There is a greater need more than ever to focus on mobile security because a lot of personal information is stored now a days on these devices and an unauthorized access would cause significant consequences. With significant increase in development and usage of wireless communication, there is a need to focus on addressing the threats and vulnerabilities that the portable computing devices are posed with. Single factor authentication has been found vulnerable to malware attacks, replay attacks, offline brute force attacks, key logger Trojans, dictionary attacks and shoulder surfing. So, organizations are moving towards multi factor authentication for better security. Strength of multi factor authentication can be found by taking into consideration how many forms of authentication it depends on. We are now looking at adaptive authentication, risk based authentication systems emerging, which use different forms of authentication methods like password, pin, Yubikey, tokens, biometrics. We have advanced into a world where we have access to biometric devices, sophisticated methods to recognize spoofing attacks and with big data solutions to authentication, we have come a long way. But this doesn't guarantee 100% secured applications, everyday several applications are being hacked into and the user's sensitive data is being comprised. We definitely have more scope to better our authentication methods. There is a greater need to understand the existing solutions and innovate.

Usability is another important aspect that needs to be considered on the path to making applications more secure. If the authentication method is not usable or if the authentication process is tedious, it is going to affect the usability of the application. We cannot have an application with too many steps for authentication process because it poses a risk of frustrating the user. We need to maintain the balance between usability and security without compromising the security needs. That is why there is a need to choose the right form of authentication methods based on user profile and the application sensitivity. We need to study existing solutions to build and compare the user profile and calculate the risk and adapt. Due to high-speed internet availability and increase in mobile storage, accessibility to sensitive data as increased. Thus, it is necessary to have a good authentication mechanism to prevent potential security breaches. That is why there is a great need to study and improve present day authentication processes and methods.

1.2. Goals and Scope of the Project:

Smartphone devices nowadays contain sensitive data and access external sites through Apps and APIs. Our smartphones are linked to all of our online accounts such as personal bank accounts, email accounts and social media accounts. If a potential hacker/intruder gets hold of an individual's phone, he gains access to all of this critical information. When compared to authentication in a computer or any device other than smartphones, the stakes are high in this case. Thus, it is of utmost importance to protect sensitive data in our smartphones against unauthorized access. One way to do that is to use a foolproof authentication which identifies users who have the privilege to access this data. Our goal is to understand how these authentication systems function and how they protect vulnerable data. We aim to explore and analyze modern authentication mechanisms for mobile devices and analyze their vulnerabilities and security concerns in order to ensure maximum security of user data. Our objective is to understand the advantages and disadvantages of each authentication technique and conclude which technique will work best for specific scenarios.

The scope of this project is to understand and compare different authentication techniques in order to meet our goals mentioned above. Exploring vulnerabilities and security concerns in authentication mechanisms and developing a fool proof approach to combat them accordingly will enable users to trust mobile devices with vulnerable data. Challenges associated with each authentication technique must be understood in detail to equip developers with the correct knowledge to reduce threats to the system as much as possible. Case studies for each technique will be referred to in order to understand their working in depth. Latest developments in technology will also be considered while devising solutions to vulnerabilities in order to create a scalable and long time solution. The pros and sons of various authentication technique should be compared to understand which method will work best for a given use case.

2. Overview (Contributions):

Sagar Parekh is the group leader of this group. He was responsible for pulling the group together. He handled the logistics of conducting group meetings every week, reserving rooms for the same, taking the minutes of every group meeting and planning out the time-table so as to complete the final report within the available duration of time. He also planned tasks to be finished by every member each week and took updates from every member on the allocated work and gave recommendations to improve it. Aside from carrying out the responsibilities as the leader of the group, he was also responsible for researching about the Traditional Authentication mechanisms on mobile phones, and provided a concise summary of one paper every week. He learned how these techniques were implemented, what are the attacks they are succeptible and how they set a path for modern authentication techniques.

Arvinthan Sundaram Govindaraju as the deputy leader for this group, worked along with the group leader in supporting the meetings. He was responsible for studying mechanisms in Continuous Authentication and Periodic Authentication of mobile devices. He read a range of papers on this topic which gave him in depth detail about how to design a good continuous authentication system and explain the ways in which it could fail. For periodic authentication, he read a few papers [73] and summarized the basic working and implementation of them along with the shortcomings of periodic authentication and the need to go for some other advanced techniques.

Mugdha Kolhe was responsible for analyzing different ways of authentication in a mobile system based on “Something user has” as well as “Somewhere user is”. She studied papers based on token based authentication including a OTP system called TrustOTP and OAuth 2.0 framework. She also researched a location based authentication system for smartphones. She learnt the various ways attackers can exploit vulnerabilities in a mobile system and how to make authentication secure accordingly.

Achyutha Sreenivasa Bharadwaj was responsible for the detailed study of Biometric authentication techniques for mobile systems. He narrowed his focus area and provided in-depth insights into the topics of Physiological biometric authentication techniques such as Fingerprint, Face recognition and Iris recognition. He started with an extensive analysis of the survey of Biometric authentication systems [60]. After which he investigated the evolution of Physiological biometrics as a viable approach toward User authentication and wrote about the system design and implementation [49] [60]. He further studied the various security threats and provided a detailed description about the various attacks associated with every sub system [33],[37],[61].

Sai Pragna Etikyala was responsible for studying and understanding Adaptive authentication methods along with risk based authentication methods. She studied the design concepts of distributive adaptive authentication systems, adaptive authentication based on analysis of user behavior. To understand risk based authentication in depth she researched about designing risk based authentication systems and building a risk based authentication system using machine learning techniques.

Venkatesan Murali was responsible for studying mechanisms in Unimodal and Multimodal Biometric Authentication, Gesture based authentication of mobile devices. He went through a list of papers which explains the drawbacks of unimodal authentication and the security vulnerabilities that could exist in these systems. He explained the architecture of a multimodal systems [38] and explained each component involved in it. He read papers which spoke about threat models, security vulnerabilities and counter-measures [2] to tackle these problems and explained each of these in detail in the report. He also worked on gesture based biometric authentication [76], was able to understand one case study which used the same and finally note down pros and cons of the same.

Harish Ravichandran was responsible for transparent authentication and one-shot authentication. . A basic introduction and overview of the different techniques used were discussed followed by different implementations. One of them is using multimodal biometrics by assigning varying Security levels to different applications, followed by a system where gait and location are used to authenticate a user. He learnt preserving privacy while collecting data related to human traits and has summarized the recent challenges in transparent authentication. He has reviewed the basic process of one shot authentication, the different attacks and how pattern locks can be cracked using smudges.

Prajwal Suresh Kodi was responsible for studying the papers related to authentication in mobile device using single sign-on and multi-factor authentication system. He went through the different methods for single sign-on and the threats they incur while these methods are used in mobile sign in and methods to overcome them. Went through the different techniques of the multi-factor authentication and discussed in details about a dynamic multi-factor method and also gave an overall system architecture and system requirement. As well as the procedures used in that method.

Dhrumil Shah was responsible for the detailed study of behavioral biometric authentication techniques for mobile phones. During his study, he has surveyed behavioral biometric authentication techniques like voice, fingerprint, signature, as well as novel behavioral biometric approaches like keystroke dynamic, gait, behavior profiling and touch gestures. He has thoroughly studied each method with the aspects of reliability, authentication accuracy, speed, potential ways the attackers can attack on various biometric authentication system and also studied the countermeasures which would effectively protect the system.

3. Results:

3.1. Threat Models

Mobile phones nowadays are powerful devices, as they can perform a wide variety of tasks such as, play music, look for directions, mobile banking, send/receive emails, SMS, MMS, play videos, scan barcodes, etc. Due to its wide variety of uses and compact/portable size, the threat model for mobile systems differs compared with others such as client/server architectures. The goals of Attackers can be divided into three major categories,

i) Collecting User's Private Data.

ii) Exploiting Computation Power of the Device.

iii) Perform Harmful Actions.

Among these, the first two goals are Covert, while the last one is Harmful. Since mobile devices nowadays have essentially become storage units of personal data such as SMS, MMS, Email, Photos, Videos, etc., a single successful attack can land all of the user's private data in the hands of the attacker compromising the confidentiality and integrity of the stored information. Furthermore, the attacker can make use of the mobile devices' basic hardware such as inbuilt mic or camera to collect additional data from the user's surroundings. For example, the attacker can turn the mobile phone into a listening device by turning on the voice recording system. In recent years, the mobile devices have come into focus for malicious exploits, such as the deployment of botnets, with aim of covertly exploiting the raw computing power in combination with broadband network access. We have analyzed threat models for each technique in their respective subsections.

3.2. Security Models

3.2.1. Android Security Models:

Android is built on top of the Linux kernel which is responsible for the execution of application by interacting with the operating system, development frameworks, and core libraries. As Android applications are sharing the same resources, drivers; it becomes necessary to prevent one application not to influence the execution of other application and as well as not to steal the private data. Android has already implemented a security model called Sandbox. Sandboxing is performed at the Linux Kernel Level. In order to achieve isolation, Android utilizes standard Linux access control mechanisms. Each Android application package (.apk) is on installation assigned a unique Linux user ID. This functionality is useful for providing a secure environment for application execution but it reduces the overall application functionality. To enhance the user experience by not compromising the security, there are two mechanism implemented in android. 1. Shared User ID: It allows applications to share data and application components. The developers can bypass the isolation model restrictions by signing applications with the same private key. 2. Permissions: Each Android application can request and define a set of permissions.

3.2.2. IOS Security Models:

iOS security model provides different philosophy for achieving mobile device security and user‟s protection. Each application submitted by a third party developer is sent to the revision process. which makes sure that the application is safe before it is released the application store. The iOS security APIs are located in the Core Services layer of the operating system and are based on services in the Core OS (kernel) layer of the operating system. Keychain Services API: It is used to store passwords, keys, certificates, and other secret data. CFNetwork is a high-level API: It is used to create and maintain secure data streams and to add authentication information to a message. The Certificate, Key, and Trust Services API: It is used to create, manage, and read certificates, keychain, encryption keys. Randomization Services: It is used to get cryptographically secure pseudorandom numbers. The Linux kernel is responsible for executing core system services such as memory access, process management, access to physical devices through drivers, network management and security. This approach allows the IOS to enforce standard Linux file access rights. Since each file is associated with its owner‟s user ID, applications cannot access files that belong to other applications without being granted appropriate permissions. This way an application cannot compromise system security by running native code in privileged mode.

3.3. Authentication Techniques:

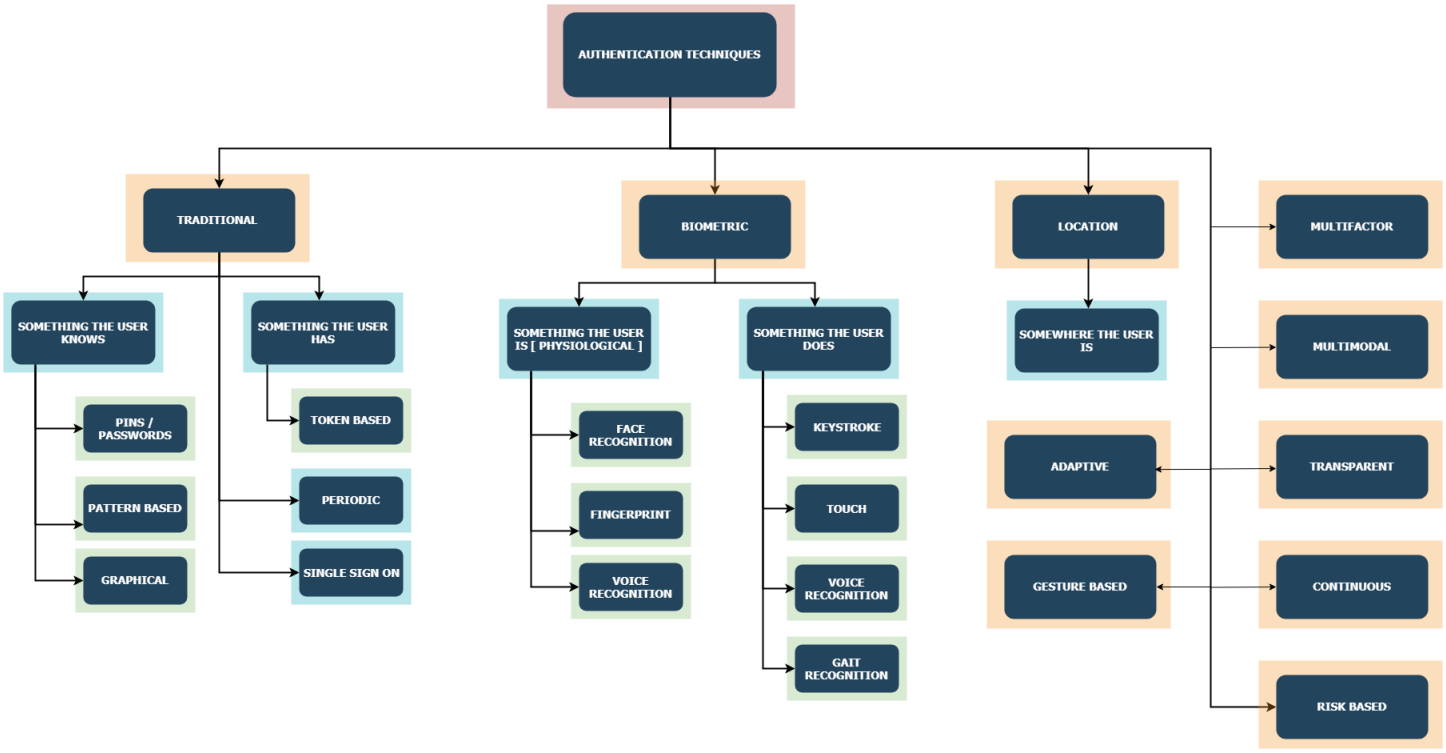

Figure 1: Authentication Techniques Classification

3.3.1. Classification of Authentication Techniques

3.3.1.1. Something that user knows:

A knowledge-based authentication (KBA) is a security measure that identifies the users by asking them to answer specific security questions [40]. Knowledge-based authentication has become prevalent where users are asked to answer these questions in order to gain access to personal, password protected areas. These authentication techniques are based on the knowledge of the user. Something that user knows is often associated with a password, multiple passwords, or a combination of a password and a username. User usually choose password before he/she starts using the service. This same static password has to be provided by user for every future use of service. The information must be remembered by the user and presented for accessing the smartphone resources. Even though this technique is effective but still it gets difficult for people to learn the pins and passwords. The security of all the methods can be evaluated based on password space. Password Space is the possible combinations of options available to any user to choose the password.

3.3.1.2. Something the user has:

User authentication in this case is based on something that user has, a physical object. An object could be a mobile device or a token. Its use is to basically check the user's validity. The token is generated by using the username and password of the users. The user can then use that token at other places which will grant them access to those places without having them put their usernames and passwords. This token will however let them access until a specific time period. In short, a token is provided to the users based on their login credentials. This token lets them access their protected resources till a limited time, without using their credentials repeatedly. This approach for user authentication is especially suitable for authentication of the user for mobile applications and services. The biggest reason for this is that mobile device is usually considered as private device that belong just to one person, and because of that is ideal example of "something that user has". On that manner mobile device is in the same time terminal that provide service and user authentication token. Using this approach, a user is not required to reveal any private information about him/her (like in biometrics) nor is it required remembering some secret information (password).

3.3.1.3. Something the user is:

This authentication is based on the unique features or characteristics a user possesses. These unique features various kinds of physiological and biological features which are voice, iris, fingerprint, face and many more [26]. Authentication systems which work on any of these features have challenge of during data collection, processing and classification based on the complexity of the task. Novel methods use various other biological features like touch, palm, and many more. Novel research in authentication systems which try to leverage the uniqueness of the biological or physiological features implement more than one biometrics to increase the confidence in the decision making ability of the system [22],[29],[30].

3.3.1.4. Something the user does:

User can be authenticated from the actions being made by the user. These actions contain the actions made with the usage of keyboards [22], touch, gestures, mobile phone usage pattern [65] and walking pattern [26]. Advantages to use these patterns are mostly these methods are user friendly and don't much rely on the memory of the user. Due to which, these methods create a hassle free and user friendly authentication. Challenges about implementing these methods are to decide the importance of each recorded feature to detect anomalies in user authentication system.

3.3.1.5. Somewhere the user is:

Smartphones are equipped with an inbuilt global positioning systems (GPS) chips that can accurately detect the location of the user. Hence, smartphones can be used to detect and send the location of a particular user to back-end servers, which shall verify the location as a factor for authentication and authorization purpose [50]. The advantages of location based authentication is that it us transparent to user, and the location record cannot be stolen by attackers. There is also no need for establishing a separate infrastructure since the mobile infrastructure is already established. However, accuracy of authentication will depend on the efficiency of GPS is critical. For example, the GPS might not work in basements, inside bigger buildings.

3.3.2. Traditional Authentication Techniques:

3.3.2.1. Pins/Passwords:

The dominant method for achieving security on smartphones is by using a 4 to 8-digit Personal Identification Numbers (PINs) and at-least a 4-letter password [40]. 4-digit based password scheme provides much security when compared with the slide lock but still it has weak security because less password key space brute force attack is possible 0 to 9999 are password space [7]. This is the simplest method and is easy to break by brute force attack. Here if the user selects a simple code it will be easy to remember and easy to enter, but it will be difficult to break.

According to a survey [56], 56% people enter wrong password because their length is limited. This is a secret-knowledge 12 authentication approach, and thus relies upon some knowledge that the authorized user has. Unfortunately, secret-knowledge techniques have long-established drawbacks, with weaknesses often being introduced as a result of the authorized users themselves. Bad practices include selection of weak (guessable) strings, as well as sharing passwords and PINs with other people, writing them down and never changing them.

PINs are open to accept surfing and systematic trial and error attacks. This technique is user friendly and easy, less time

consuming and has large address space. Nevertheless, it can be affected by Brute Force Attack, stored passwords can be accessed in some way, password gets revealed while logging in a public place and there is always a chance of conflict with other passwords [40]. This system may also go through impersonation in which an unauthorized person can steal confidential data using password and ID. Once an intruder acquires the user ID and the password, the intruder has total access to the user's resources. In addition, there is no way to positively link the usage of the system or service to the actual user, that is, there is no protection against repudiation by the user ID owner.

3.3.2.2. Pattern Based Passwords:

Pattern passwords typically are done using a 3x3 grid that a user draws a pattern on. The pattern password system follows certain rules: the pattern has to have a minimum of 4 swipes as this prevents the pattern from being a straight line, the pattern is not able to cross itself without activating the center node and a node cannot be activated twice [3]. The problems that arise from this system is the linear behavior of the scheme and the device used for authentication. Pattern passwords are susceptible to smudge attacks and Video tracking algorithms [3].

Cell phone clients commonly utilize their fingers to enter in their example secret phrase, their fingers leave buildup on the screen. That buildup makes it simple for assailants to distinguish your secret word [3]. A study was done to see if general use of a phone would cause enough distortion in the smudge to make it impossible to discern the password [3]. That review had clients put the telephone in their pockets and move around to check whether the apparel contact would expel the buildup; the outcomes demonstrated that the secret pattern was as yet perceptible from the smear [3]. Users can wipe down their phone every time their password is entered, however that is not convenient.

Another issue with the pattern password scheme is its linear behavior, this can lead to attack via video tracking. There was an ongoing strategy made that can follow client's fingers directions and from the direction reproduce the secret pattern. What is intriguing about the referenced technique is it doesn't require the video to have a perspective on the screen it just needs to see the client's finger and the video can be taken from up to 2 meters away.

3.3.2.3. Graphical Based Password:

Picture-based passwords include Graphical Password. This method is based on the fact that people are easily remember images than strings. Graphical Password (GP) was originally introduced by Greg Blonder in 1996. A graphical secret key is an authentication framework that works by having the client select from pictures, in a particular request, displayed in a graphical UI (GUI) [40]. Hence, the graphical-secret word approach is once in a while called graphical client verification (GUA). Graphical passwords (GP) use pictures rather than textual passwords and are somewhat persuaded by the reality [40].

This technique is further classified into two types: i) Recall based technique and ii) Recognition based technique [7]. In a recall based technique, a user is required to draw image which he has created in registration phase. In a recognition based technique, users are required to identify image and recognized image which he has selected in registration phase. Although the system is resistant against shoulder surfing, it takes time from user to login or differentiate the degraded pictures. A hybrid technique which combines recognition (select specific symbols) and recall (try to redraw selected symbol on screen) [40].

Along these lines, graphical passwords give a way to making easier to understand passwords while expanding the dimension of security. Graphical passwords may offer preferred security over content based passwords in light of the fact that numerous individuals, trying to retain content based passwords, utilize plain words.

3.3.2.4. Token Based Authentication:

The "Something you have" authentication mechanism is based on token based authentication. Token based authentication is a security technique that authenticates the users who attempt to log in to a server, a network, or some other secure system, in our case a mobile phone, using a security token provided by the server. The general concept behind a token-based authentication system is simple. Allow users to enter their username and password in order to obtain a token which allows them to fetch a specific resource - without using their username and password. Once their token has been obtained, the user can offer the token - which provides access to a specific resource for a time period - to the remote site. Token based authentication for smartphones is being utilized for authentication purposes in several sensitive operations by the means of OTP via SMS, offline OTP using App, etc. One Time Password (OTP) - A password that is valid for only one login session or transaction. It is widely used for Two-factor Authentication. The two types of OTP are HOTP (HMAC-based OTP) and TOTP (Time-based OTP).

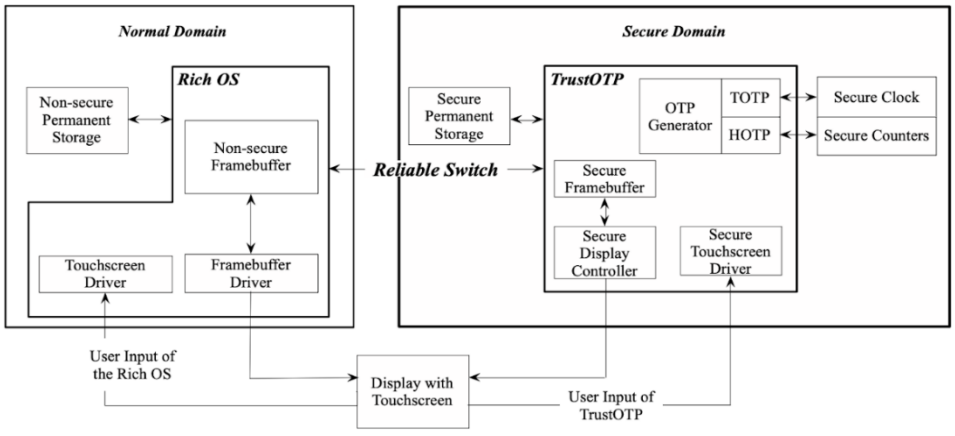

Figure 2: The Trust OTP System

3.3.2.4.1. TrustOTP System [36]:

TrustOTP is a new proposed system with hardware-assisted OTP Token on smartphones. It increases security (confidentiality, integrity, availability) and flexibility (various and multiple OTPs) as compared to traditional OTP systems. It has the goal to achieve both the security of the hardware tokens and the flexibility of the software tokens. This design can prevent all types of attacks from the malicious mobile OS and continue to display the OTP even if the mobile OS crashes.

It is flexible to support various OTP algorithms and multiple OTP instances on one smartphone. It requires no changes of the mobile OS and has small impacts on the mobile OS's performance and works efficiently with tiny extra power consumption. TrustOTP is installed in the secure domain and consists of the following major components:

i) The OTP generator: Responsible for continuously generating one-time passwords even if the Rich OS is malicious or crashes. It supports various OTP algorithms to compute OTPs. It supports the two most popular categories of OTP: the time-based OTP (TOTP) and the event-based OTP (HOTP).

ii) Secure Display Controller: Securely copies the image from a secure framebuffer to the display device, where the framebuffer stores the image of the OTP to be displayed. To prevent potential OTP leakage, the secure framebuffer is different from the framebuffer used by the Rich OS and reserved in the secure domain.

iii) Secure Touchscreen Driver: A self-contained secure touchscreen driver in the secure domain for the user to input into the secure domain.

3.3.2.4.2. Token Based Authentication Advantages:

i) Stateless: There is no need to keep a session store, the token is a self-contained entity that conveys all the user information.

ii) Mobile ready: when you start working on a native platform (iOS, Android, Windows 8, etc.) cookies are not ideal when consuming a token-based approach simplifies this a lot.

iii) Decoupling: you are not tied to any particular authentication scheme. The token might be generated anywhere, hence your API can be called from anywhere to authenticate calls.

iv) Cross-domain / CORS: They don't play well across different domains. A token-based approach allows you to make AJAX calls to any server.

3.3.2.4.3. Threats [74]:

i) Man-in-the-Middle attacks: With this attack the attacker gets between two parties, where each party thinks they are interacting over a private connection, but it is actually being controlled by the third-party attacker.

Prevention: It is important to use strong encryption and authentication between the application and the server. Using encryption, the server authenticates the application's request by presenting a digital certificate, and only then can the connection be established.

ii) Replay attacks: Replay attacks allow attackers to gain access to a network and information which would not have been easily accessible and complete a duplicate transaction. These are attacks on the security protocol using replays of data transmission from a different sender into the intended receiving system.

Prevention: Replay attacks can be avoided by using session tokens. However, if these credentials are stolen from local storage (like during an XSS attack), there are ways to prevent someone from holding on to a valid token forever such as setting a short expiration time for tokens and using OTP.

iii) Cross-site Request Forgery: A Cross-site Request Forgery (CSRF or XSRF) attack occurs when a malicious program causes a user's web browser to perform an unwanted action on a trusted site on which the user is currently authenticated. This type of attack specifically targets state-changing requests to initiate a type of action instead of getting user data because the attacker has no way to see the response of the forged request.

Prevention: One way to verify the requests that are being sent is to utilize the OAuth 2.0 protocol state parameter to authenticate the response

3.3.2.5. Periodic Authentication:

Periodic authentication is simply the variant of “one-shot authentication” in which idle timeout duration is set, for closing the session, automatically [115,52]. If a user remains inactive for more than the idle timeout duration, the device locks itself. Bertino et al. [73] defined periodic authorization with a mathematical expression “{[begin, end], P, auth}” holding of 3 prime attributes, where “begin” is authorization start date, “end” is either the constant ∞, or a deauthorization date after the start date, “P” is the duration of a session, and “auth” is an authorization function. Feng et al. [52] determined that periodic authentication or automatic logouts are more detrimental while one-shot authentication solutions are prone to a wide variety of attacks. Typing an error-free username and/or password on smartphone’s keyboard is really a tedious

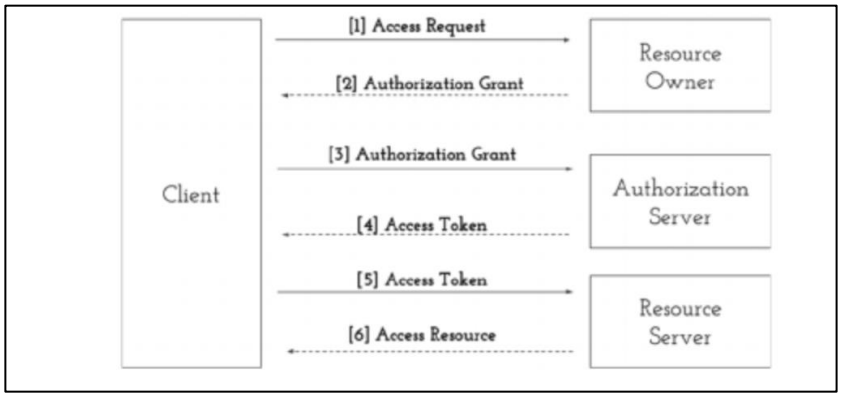

Figure 3: OpenAuth 2.0 Schema

task, especially when an average user initiates 76 phone sessions a day. Single sign-on (SSO) has been seen as the solution to the problem.

3.3.2.6. Single Sign On:

OpenAuth 2.0[14] is a Single Sign On (SSO) framework with a unified single account to authenticate user's identity throughout the different services. Websites that use OAuth: Google, Facebook, Renren, Amazon, PayPal. There are several vulnerabilities. Based on HTTP Protocol, credential storage, Invocation of Supported Services and brute force attack.

Working as shown in Figure 3:

The client requests access for data belonging to the resource owner. The resource owner replies by sending the authentication grant. The reply contains the chosen grant type, the preferable authentication server to be used and which is server holds the resources. The client forwards the authentication grant to the authentication server, requesting access token. The authentication server validates it and then sends back an access token, which represents the resource owner and states that the authorization has been approved. The client asks the permission to access the protected resources from the server that contains the data by providing the access token. The resource server receives the token and validates it, returning the requested data. The types of threats and their prevention are :

i) Impersonation Attack [55] : When an illegal user tries to fool the server in believing his/her identity.

Prevention: IP address is used for detection.Adversary login as the legal user IP address, writes correct service provider IP address and request the file that is needed. Here, the filename that is uploaded at the IP is checked with the IP address of the legal user.

ii) Credential Privacy [55]: Credential privacy is that the dishonest service provider should not be able to recover user credential.

Prevention: Here, authenticated party is used in between the client and the server, server do not know who the legitimate user is. So he will not be able to give wrong service to the receiver. User is also not allowed to modify any file; he has the permission to read the file. If the user is modifying the file he is the attacker. When the user tries to modify the file, he feels like he is modifying the file, because the original file is seen. It visualizes that the attacker is writing on the file but actually the file is not modified. This trial of modifying the file is updated at the AP.

iii) Replay attack [55]: This is an attack in which an adversary intercepts the data and retransmits it at valid time window.

Prevention: Trick is to use random no/code that is nonce in the transmitted data every time the message is being transmitted. Every time the message is transmitted a different random code is added to the message. This random number can be said as the secret key. The random number generated is of 32 bit and is added to the message at the end. Initiator intractability Prevention from linking the message send in communication. This is covered by using the Random number.

3.3.3. Biometric Authentication Techniques:

The term Biometrics refers to the metrics related to human characteristics. I.e., they are the distinctive, measurable characteristics used to identify or label individuals. They are mainly used as a form of authentication and authorization.

Biometrics technology is based on the principle of measuring and examining the biological traits of individuals, extracting the unique features from this acquired data and then comparing it with the template set stored in the biometric templates database [8]. Biometric authentication systems can be broadly classified into two categories, Physiological and Behavioral biometrics. Physiological biometrics refers to measuring the physical characteristics of the body. Examples include, but are not limited to Fingerprint, Face, Iris, etc. Behavioral biometrics identify individuals based on their pattern of behavior, including but not limited to Keystroke, Gait, Voice, etc. Biometric characteristics are unique to individuals. Therefore, they are more reliable in verifying identity than the traditional ways of authentication; however, the collection of biometric characteristics raises privacy concerns about the ultimate use of this information.

3.3.3.1. Physiological Biometrics:

Physiological Biometrics are automated methods of recognizing a person based on physical characteristics. Some of the biometrics measured are the face, fingerprints, handwriting, iris, retinal, vein, voice, etc. The easiest way to identify and authenticate a user is by using the unique physical attributes of the human body, such as fingerprints or iris. Because we are born with these traits, Physical Biometrics are an inherence factor or "something you are," making them impossible to guess and difficult to alter or fake. Although biometric technology has been around for many years, modern advances technology, coupled with big reductions in cost, has now made biometrics readily available and affordable to all consumers. The Different types of Physical Biometric Authentication in Mobile Systems:

3.3.3.1.1. Facial Recognition:

Face Recognition is an emerging technology capable of identifying or authenticating a user from a digital image or a video feed. There are multiple algorithms based on which the facial recognition systems work. These algorithms can be broadly classified into two categories, holistic and feature-based. The former attempts to recognize a person by comparing the entire face image. But most commonly used ones work by extracting facial features from a given digital image and comparing it with the extracted features from saved images of the user. Some of the features used to identify users are the relative position, size, and/or shape of the eyes, nose, cheekbones, jaw, etc. Some of the popular facial recognition algorithms include but not limited to principal component analysis, linear discriminant analysis, hidden Markov model, dynamic link matching, etc.

3.3.3.1.2. Fingerprint:

With Fingerprint recognition systems, users can conveniently and securely unlock their mobile devices or authenticate themselves on an application by means of a quick touch. These algorithm solutions are based on close to 20 years of cutting-edge research and have been implemented by hundreds of millions of users worldwide. Any fingerprint

recognition system has two major jobs, scan the image of the finger, and determine whether the pattern of ridges and valleys in this image matches the pattern of ridges and valleys in pre- scanned images. Only specific unique characteristics are filtered and saved as an encrypted biometric key or mathematical representation. No image of a fingerprint is ever saved, only the biometric key, which is used for verification is saved. The algorithm cannot be reconverted to an image, so duplication of fingerprints is not possible.

The performance of the fingerprint authentication system depends directly on the quality of fingerprint images scanned by the fingerprint sensor. If the quality is lower, image enhancing steps such as Gray scale converting, noise filtering and edge detection processes, etc., can be used to enhance the quality of the scanned images.Among the wide range of authentication methods available, when fingerprint authentication is combined with a second form of authentication, such as a PIN, it provides maximum security and unparalleled user convenience.

3.3.3.1.3. Iris Recognition:

Iris recognition is an automated method of biometric identification that uses video images of one or both of the irises of an individual's eyes to identify and authenticate users. There are complex patterns present in the images of irises that are unique, stable, and can be seen from some distance, that can be used to precisely identify users. This method of authentication is different from Retinal scanning where unique patterns on a person's retina blood vessels are compared, whereas Iris recognition systems apply mathematical pattern-recognition techniques to images of the irises of an individual's eyes.

However, it is a challenging task to match iris images since iris pattern deforms significantly under diffe rent illumination conditions. A person’s pupil contracts in the bright and dilates in the dark. The change of pupil size leads to nonlinear deformation of iris and becomes extremely hard to identify. It is reported iris deformation is the main source of fa lse reject errors in iris recognition. To solve this issue, two major approaches are used. The first is Image normalization and the other is robust feature representation and matching. With these two approaches we can reliably use Iris recognition for auth entication with lower failure rates.

3.3.3.1.4. Process Model [60]:

i) Sensor module: In this module, raw biometric data is captured by the sensor and converts the biometric trait into digital form. After converting it to digital form, transmits the data for preprocessing.

ii) Preprocessing module: This module transforms the loaded samples to prepare them for feature extraction. For example, it can do image histogram equalization, geometric normalization, operations to ensure the system becomes shift, rotation, and size invariant. It is also possible to retrieve new information about the image, such as determining the position of eyes (in case of images with faces) and add it to the sample in an explicit way.

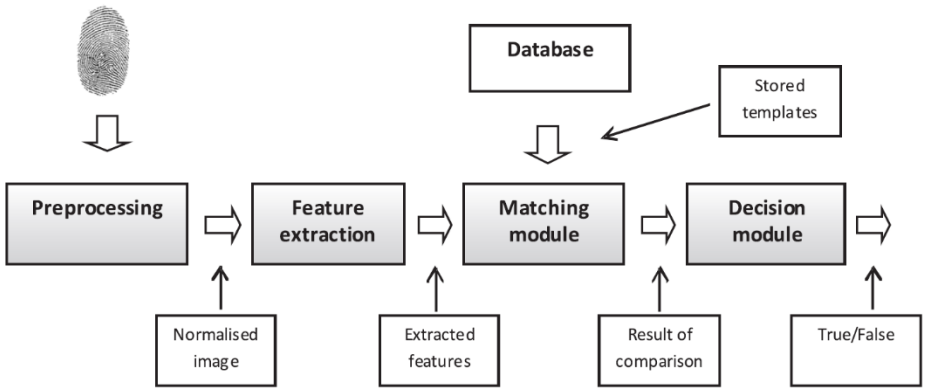

Figure 4: Biometric Recognition Process Model

iii) Feature extraction module: The most important step in the majority of biometric methods is feature extraction and this step is provided by feature extraction module. The result from this module is a set of features (in the form of matrices) associated with each sample.

iv) Post processing module: This module is optional. It works similar to the preprocessing module, it is designed to transform result from the feature extraction stage (but not limited to) if such a transformation is needed.

v) Matcher Module: This module compares the input sample with the templates being stored in the database using the matching algorithm and produces a match score. The resulting match score is transmitted to the decision module, which decides whether to accept the individual or not.

vi) Decision Module: After accepting the match score from the matcher module, it compares the matching score against the predefined security threshold. This module accepts or rejects the individual on the basis of predefined security threshold. If the match score is greater than the predefined security threshold it will accept the individual otherwise reject it.

3.3.3.1.5. Threats:

The main advantage of Physical biometric systems is that; while users may forget passwords or pins, they will always have their fingerprints and other physical biometric measures with them and in many ways, it's a vast improvement over the alphanumeric passwords we use today. While it may seem that biometric systems are foolproof, unfortunately, it is not so. The main advantage of biometric systems is also its greatest disadvantage. For example, if a user's password is compromised, there is always the option to reset their password and protect their systems. But it is not so for biometric systems as there is no way for anyone to reset them. Even with this disadvantage, Physical biometrics is one of the most widely used authentication systems in the world today. Biometric systems offer great advantages over traditional systems, but they are vulnerable to attacks. The attacks on Biometric Authentication Systems can be divided into two categories, Direct attacks, and Indirect Attacks.

Direct Attacks or Attacks on Sensor module [37]:

It refers to the attacks that do not require any specific knowledge about the system operation such as matching algorithm used, feature vector format, etc. In this attack, a fake biometric trait such as an artificial finger or facial image is presented to the sensor by an imposter to bypass recognition systems. An imposter can also physically damage the recognition system and flood the system with bogus access requests. It is very easy to attack at the sensor because no specific knowledge about the system operation is needed and there are no digital protection mechanisms such as watermarking, cryptography, etc., are used at the sensor level. Sensors are unable to distinguish between fake and real characteristics of an individual and can be fooled easily by using synthetic fingerprints or facial image of a person. Following are some examples of the direct attacks :

Smudge Attack: Smudge attack is possible when latent smudges of fingerprints are visible after a user uses the smartphone to unlock it.

Spoofing [61]: This attack is aimed at biometric authentication systems. In this attack, the attacker tries to imitate the user by making use of fake biometric samples or some type of synthetically produced artifact. Alteration Attack [33]: Alteration is one of the critical attacks against biometric systems. The impostor alters the image of the real user and he presents it as a request in order to gain unlawful access to the system. Analysis shows that both systems are vulnerable to the proposed attack and the alteration level has a serious impact on the security of biometric systems.

Indirect attacks [37]:

Unlike direct attacks, these attacks require working knowledge of the authentication system to make a successful attack. These attacks are aimed at specific modules of the authentication system to make them unable to distinguish between real and fake samples. Following are some of the indirect attacks,

Replay attack: When the sensor sends the raw data to feature extractor module for pre-processing through a communication channel, it is intercepted to steal the biometric trait and stored somewhere. The previously stored biometric trait is replayed to the feature extractor to bypass the sensor.

Attack on Feature Extractor module: The attacker pressurizes the feature extractor module to produce the feature values chosen by him instead of producing the feature values generated from the original data obtained from the sensor.

Attack on Decision Module: The attacker overrides the result declared by the matcher module. In this attack, the attacker tampers the match score which is transmitted through the communication channel between the matcher module and application device. It tampers the match score to change the original decision (accept or reject) of the matcher module.

3.3.3.1.6. Techniques to Resist attacks:

3.3.3.1.6.1. Liveness detection:

Liveness detection is a mechanism that is used to detect that the input sample feature is provided by a live human being or not. It is used to prevent attacks at the sensor. Liveness detection can be applied using software or hardware means. Use of extra hardware to implement liveness detection means to measure various life signs like pulse detection, blood pressure, the temperature for fingerprints and movements of the face, eyes for face recognition. The limitation of using extra hardware makes the system too much expensive. Using software means to use the information already captured to detect life signs. For example, we can use Image Quality Analysis [39] after receiving the sample from the sensor to determine if the sample is from a live human or not.

3.3.3.1.6.2. Biometric cryptosystems [37]:

Biometric cryptosystems combine biometrics and cryptography to take advantages from the strengths of both the fields. Cryptography provides a higher degree of security and biometrics eliminates the need to remember any passwords or to carry any tokens. Biometric cryptosystems are subdivided into key generation and key binding. Key generation: In this helper data is only obtained from the biometric traits and the cryptographic key is directly generated from the helper data. Key release: In this helper data is obtained by binding a key with biometric template.

3.3.3.1.6.3. Steganography and Watermarking:

Steganography means covered writing. It refers to the process in which cover image is used to hide the original data. Watermarking technology is the embodiment of steganography. Steganography and watermarking is used to prevent indirect attacks that aim the transmission channel between different modules of the Biometric authentication systems. Watermarking is used in the authentication of ownership claims. Steganography can be used for transferring critical biometric information from a client to a server.

3.3.3.2. Behavioral Biometrics:

Biometric Authentication method focuses on the behavioral matrices like touch dynamics, keystroke patterns, gait features and many more. Biometric features could also be evaluated by means of the following seven characteristics [26]:

Universality: every person should have the biometrics

Uniqueness: no two persons are expected to have such identical biometrics.

Permanence: the biometrics should not vary with time.

Collectability: the biometrics should be easily collected and measurable.

Performance: the accuracy of the biometrics should be stable under varied environmental circumstances.

Acceptability: common users should widely accept the sample collection of the biometrics.

Circumvention: the biometrics should be difficult to deceive and fool.

Behavioral biometric features include traits that monitor performance or a specific activity over time. These features are not left behind and are almost impossible to deceive.[30] As the users of mobile phones is increasing exponentially in recent times, the data collection, it becomes necessary to improve user authentic systems. As user is constantly in the vicinity of the mobile, it becomes easier to behavior matrices of the user. Behavioral biometrics are based on a behavioral trait of an individual such as voice, signing a signature, gait, behavior profiling and typing rhythm (also called keystroke dynamics). With the advent of touchscreen mobile phones, touch dynamics has quickly become a hot topic for both academia and industry [26].

3.3.3.2.1. Keystroke dynamics:

Keystroke dynamics verification is based on how a user types at a terminal equipped with a keyboard, which may belong to a personal computer, or be a generic interface equipped with keys which can be pressed [64]. While verifying the user with keystroke dynamics different approaches could use various features like key hold time, latency, horizontal digraph, vertical digraph, error rate, non-adjacent horizontal digraph and non-adjacent vertical digraph. [26]

Keystroke authentication can be classified as either static or continuous. The first refers to keystroke analysis performed only at specific times, for example during the login process, while the analysis of the typing rhythm is performed continuously during the whole session when the latter is applied, thus providing a tool to also detect user substitution after a successful login. [64]

According to generalized biometric authentication system presented in fig. [x], data collection here would be the timing of key press - release events, data processing would be creating a statistical model with the captured event, data classification would be calculating similarity between captured event model and authentic user model. [64]

3.3.3.2.1.1. Static Keystroke authentication:

There have been approaches for keystroke dynamics to use different size and shape of keys, neural network based approach, statistical analysis approach and many more. There have been many approaches proposed which would do the calculation based on the input and match with the profile and profile of the user is generated using initial input. In some approaches, instead of using profile building, all authenticate data points are stored and they are compared with the input point to detect anomaly.

3.3.3.2.1.2. Continuous Keystroke authentication:

Systems which implement continuous keystroke authentication systems use features like typing speed, error rate, gait movement while typing, etc. These approaches are difficult to implement since these approaches do not have static data to authenticate the user.

3.3.3.2.2. Touch Dynamics:

With the rapid development of mobile platforms, touchscreens have recently become a leading input method, which is an electronic visual display that users can control through simple or multi-touch gestures by touching the screen [26]. Authentication system based upon touch dynamics use various features of human gestures.

Pressure: Pressure during the touch varies a lot on the user basis. There are two types of pressure which are being considered: 1) Instantaneous pressure: It uses the current pressure and find the probability of the authenticated user based on the input. 2) Sessional pressure: It refers to many statistical features like pressure range, pressure min, pressure max, etc. for one particular session. It is generally used in continuous authentication system.

Size of the finger: Size of the fingers is considered as one of the unique biological features of human beings. Whenever the user touches the phone, size of the all the fingers are measured and by doing statistical analysis of finger sizes, authenticity of the user is decided.

Posture angle: This feature focuses on the way the user holds the phone. This angle refers to x and z coordinates of the angle of the held mobile.

Touch movement: This feature focuses on the way user moves the finger on the screen. It includes the features like finger movement speed, duration of touch, etc.

In [22], the author proposes a method to authenticate user using the touch dynamics features like posture angle, pressure, finger movement combined with the signature. In [22], the author collects data using TouchLogger, GyroLogger and input data points from the user. Logs collected from these sensors are calculated and statistical pattern is found within the logs. If any new input from the user comes than it would be checked with the authenticate pattern of the users. There have been approaches proposed also based on touch dynamics which combines the signature of the user to increase the confidence in the system [22]. Since these methods rely on continuous input from the user to find the pattern, these methods are generally useful in continuous authentication systems. These systems require less effort from the user so they are user friendly as well as highly secure.[30]

3.3.3.2.3. Voice Recognition

This biometric attempts to identify a person who is speaking by characterizing his/her voice. The key point is that each human has different voice signatures, and identical words may have different meanings if spoken with different inflections or in different contexts [26]. The voice biometric authentication systems usually fall into two categories [26]:

Text-dependent: the text must be the same for enrollment and verification.

Text-independent: no text constraints during enrollment and verification.

The voice authentication is easy to use, widely accepted by users and allows remote authentication. In addition, the cost of implementation is relatively low and the storage size is small. But a major weakness is the high false non-match rates

since the human voice may change under special conditions (i.e., when people get sick). This biometric technique has been implemented in current touch-enabled mobile phones like iPhones.[26]

In [26], different kinds of systems based upon voice recognition were also been surveyed. These systems have implemented voice recognition in various ways like A* algorithm, Baidu algorithm, Compressed Feature Dynamics (CFD), and many more. Different implementation of the systems yet to solve the problem of high false non-match rate. High false non-match mostly occurs when human voice is changed under certain circumstances like falling sick.

3.3.3.2.4. Gait Recognition

This type of recognition techniques is an emerging biometric technology which involves people being identified purely through the analysis of the way they walk.[26] Currently, this kind of biometrics is still under development while it is feasible to be deployed on mobile phones as mos phones like iPhones now can provide accelerometers with three primary axes. There are three main types of gait recognition:

Machine vision based: The walk behavior would be captured by videos and video-processing techniques are used for analysis. For example, gait data can be captured by using various digital/analog cameras from certain distances. Later, different signal processing, image processing, and machine learning techniques are used for extracting gait related information and identifying individuals [154].

Floor sensor based: The sensors would be placed in the floor to measure force or pressure when an individual walks on them, and utilizing this information for identifying individuals.

Wearable sensor based: The user wears a device aiming to measure the way of walking and recognize the patterns.

In [31], novel approach on gait recognition has been discussed. In [31], firstly, author proposes a novel gait authentication system on mobile devices in which the security and privacy are preserved by employing a fuzzy commitment scheme. Secondly, the discriminability of sensor-based gait templates is investigated to determine appropriate parameter values to construct an effective gait-based biometric cryptosystem.

3.3.3.2.5. Mobile Phone Usage profiling:

Current research [65] found that usage pattern of mobile phones remains similar over the period of time. Using this property, user can be authenticated. Since this relies on the usage pattern, usage profiling method is more useful for continuous authentication system.

3.3.3.2.5.1. Phone level usage profiling:

By default, several common applications are pre-installed in the mobile devices. In this approach, usage of applications like phone book, messaging service, clock are analyzed with the help of logs. For the experiment, total 104 users have

participated and total of approx. 7.2 lac logs have been taken for the analysis. Based on the logs, data analysis is performed, and user profile is created. Based on the user profile and threshold, anomaly can be detected.

3.3.3.2.5.2. Application level usage profiling:

This method focuses on the application-based behavior. In this approach, usage of applications like phone book, messaging service, clock is analyzed with the help of logs but profile is built for each application separately. For the experiment, total 104 users have participated and a total of approx. 7.2 lac logs have been taken for the analysis.Based on the logs, data analysis is performed, and user profile is created. Based on the user profile and threshold, anomaly is detected.

3.3.3.2.6. Attacks and Countermeasures:

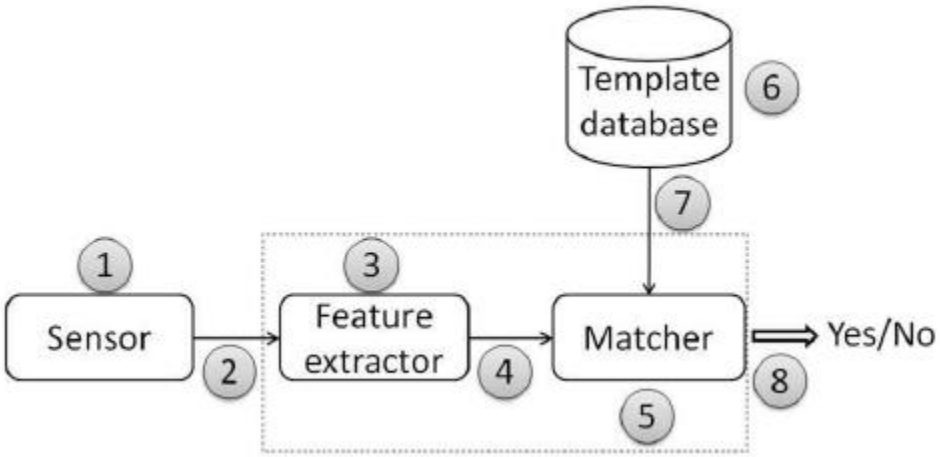

Figure 5: Potential attack points on behavioral biometric system

The above figure explains the various parts of the authentication system and also explains where the system could be attacked. Eight potential attack points for a generic behavioral biometric authentication system:

1) Faking the sensor.
2) Resubmitting biometric signals.
3) Overriding the feature extractor.
4) Tampering the biometric features.
5) Compromising the matcher.
6) Tampering the stored templates.
7) Attacking the channel between the stored templates and the matcher.
8) Overriding the final decision.

Since these attack points are generic, each specific system should focus on the attack point on which that system is most vulnerable. For example, voice recognition system is most vulnerable to spoofing attack [26] so these systems should focus more on the input processing before submitting to feature extractor. This attack is said to have an attack on phase 1. Finger print based systems can be attacked using submitting the fingerprint samples using previously collected

authenticated fingerprint. This attack is said to have an attack on phase 6.

3.3.4. Multifactor Authentication:

Multi-factor authentication is a technique of using extra level of authentication on top of an existing one. This gives an extra layer of security on top of a given method. While doing multi-factor authentication user authentication is usually done on mobile devices. Ordinary passwords and one-time passwords both of them have security and usability drawbacks. An alternative, public key certificates, provides strong security but is difficult to deploy. Instead [56] proposes novel one-, two- and three-factor authentication methods based on public key cryptography without certificates. These new methods provide strong security and are easy to deploy and use. Experiments in [56] show that multifactor authentication on a mobile device is feasible and is able to provide a higher level of security compared to single-factor authentication. Having a multiple layer of authentication will ensure that the authenticator is the intended user. They can be further classified as:

3.3.4.1. Compartmentalized Multi-Factor Authentication [4]:

This method includes obtaining data representing a printable authentication pattern, where the printable authentication pattern encodes access information. at the mobile telephone , a user request to access the feature for a software and this is done by capturing the image using a camera of the mobile device, an image of an input pattern printed on to a substrate , decoding the input pattern to obtain captured information and determining the access information , and if the captured information matches the access information provide access to the feature on the mobile device.

A mobile device may be configured by software to require a user to pass a multi factor authentication process in order to access specific applications or data on a mobile device . The multi – factor authentication may utilize a barcode , such as a Quick Response (QR) code for image capture using digital camera componentry built into the mobile device , and another authentication factor , such as a password . The mobile device , and / or a remote server , analyzes the digital image of the barcode to decode the barcode into its encoded character data . If the character data and password are determined to be valid , then access to specified data and / or applications may be granted .

3.3.4.2. Dynamic multi-factor authentication [17]:

A multi-factor authentication mechanism is designed which will dynamically adjust its complexity based on the assessed security risk of the smartphone's environment. By detecting signals from the user's environment, our proposed mechanism is able to calculate a trust value that will be used to tighten or ease the security require ments. This authentication is combined into the authentication mechanism to continuously observes the current user to ensure that he is still the authenticated user.

3.3.4.3. System Architecture:

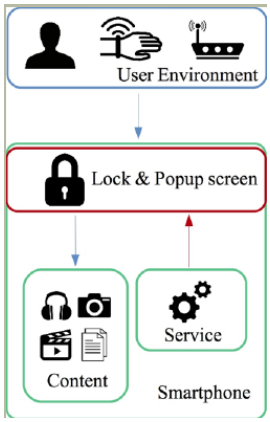

Figure 6: Multifactor System Architecture

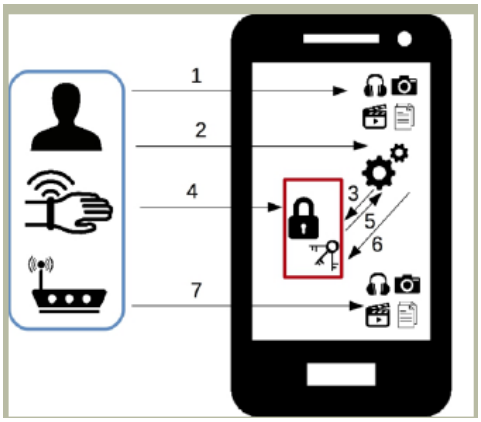

Figure 7: Multifactor Authentication

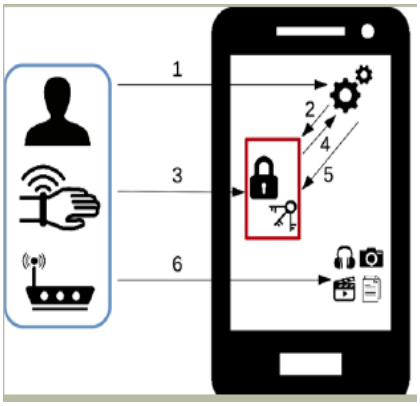

Figure 8: Implicit Multifactor Authentication

The system operates by running a background service which will authenticate by monitoring the presence of trusted Bluetooth and Wi-Fi signals. These data are then processed to generate a trust value, which indicates how likely it is that the person who is going to use the phone is the authorized user. When the phone is used from a standby condition, the user is presented with a lock screen. In order to use the phone, the user will have to pass the multi-factor authentication on the lock screen. The amount of authentication that the user needs to successfully pass depends on the trust value that the system continuously calculates in the background.

First phase of Authentication: When the user is trying to use the smartphone from locked state, the authentication service will call a handler to display a lock screen to the user. After the authentication service issues a handler to display the lock screen, the user is required to input the demanded authentication factors displayed on the lock screen. This serves as explicit authentication, whereby the user is granted access if he can bypass the authentication requirements. The user enters his authentication factors as requested, with this being a combination of three factors: knowledge, possession, and inherence factor. The amount of authentication that the user needs to pass is determined by the trust value which is obtained from monitoring the user's surroundings. The service checks the user's entered credentials. If the user is able to provide all the correct credentials, then he has passed the authentication. When the user passes the authentication phase, the service closes the lock screen. With the lock screen closed, the user can now use any features on his smartphone, because he is already authenticated.

Implicit Multi-factor Authentication: [Fig. 7] After the user passes the lock screen, he can access the mobile device's contents. While the user is using the mobile device, the system continues to monitor the user's environment to update

the trust value in the background. If the service determines that the current user's authenticity is questionable (through calculation of a low trust value), then the service will temporarily revoke the user's access by creating security pop-up requesting the user to re-authenticate. Re-authentication is done by asking the user to prove his authenticity with one authentication factor chosen randomly from the three available factors. If the user is able to provide a correct factor, then he/she has passed the authentication. If the user is able to provide the correct credential, then the user has passed the authentication. When the user passes the authentication, the service closes the security pop-up. After passing the re-authentication phase, the user can continue to use the phone as usual.

3.3.5. Unimodal vs Multimodal:

Biometric identification systems which use a single biometric trait of the individual for identification and verification are called unimodal systems. Biometric identification systems which use or can use a combination of two or more biometric modalities to identify an individual are called multimodal biometric systems [38]. The most important reason behind using multimodal biometric systems is to improve the recognition rate.

3.3.5.1. Advantages of Multimodal technique:

The accuracy of a multimodal biometric system is measured by the errors in image acquisition and matching of the biometric traits. Image acquisition errors include failure-to-acquire (FTA) rate and failure-to-enroll (FTE) rate. Matching errors consist of false non-match rates (FNMR) in which a legitimate subject is rejected and a false match rate (FMR) where an intruder is granted access. Multimodal systems have almost zero FTA, FTE, FNMR and FMR rates [38]. In a scenario where millions of people need to be enrolled in a system and some people might be facing problems with a biometric trait, multimodal systems can overcome this limitation by using a different biometric for that segment of the population. This will ensure almost zero failure-to-enroll (FTE) rate.

3.3.5.2. Drawbacks of Unimodal technique:

Susceptibility of the biometric sensor to noisy or bad data: The captured biometric trait might be distorted due to imperfect acquisition conditions. This limitation can be seen in applications which use facial recognition. The quality of the captured facial images might get affected by illumination conditions and facial expressions. Another example could be in fingerprint recognition where a scanner is unable to read dirty fingerprints clearly and leads to false database matches. An enrolled user might be incorrectly rejected whereas an impostor might be falsely accepted. It might not be compatible with certain groups of population. Fingerprint images might not be properly captured for the elderly and young children because of faded fingerprints or underdeveloped fingerprint ridges [8]. Unimodal biometric systems are quite vulnerable to spoof attacks where the data can be imitated or forged. For example, fingerprint recognition systems can be easily spoofed using rubber fingerprints.

3.3.5.3. Implementation of Unimodal Authentication:

A technique called TAP (Typing authentication and Protection) is proposed. The proposed system called TAP is a virtual key typing based authentication system for mobile devices. It has a 2 stage security which is unique about this particular system- 1) Login stage, 2) Post Login stage. During the Login stage, TAP leverages biometric information embedded in the typing habit and hand morphology to accomplish user identity management using a simple password. During the Post Login stage, TAP monitors the user's virtual key dynamics behavior to continuously authenticate the user [44].

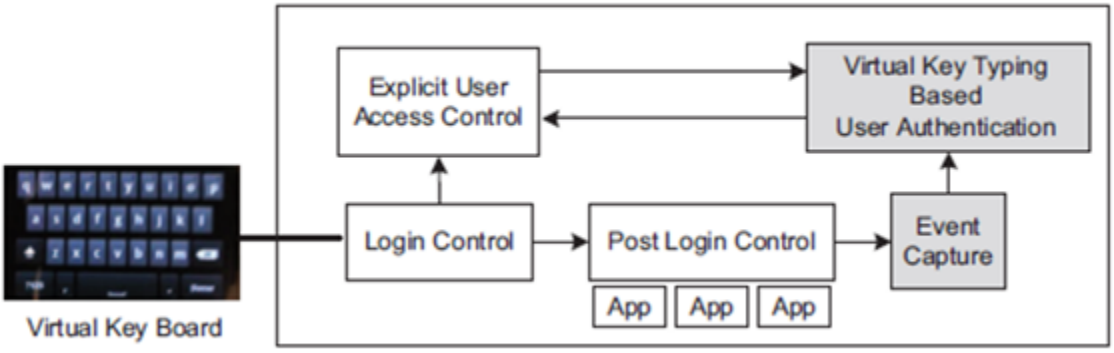

Figure 9: Typing authentication and protection flow of events[44]

At first, the window shows a sentence and the user types the sentence using the displayed virtual keyword. Then the users are also asked to enter a password of 4 characters. The post login stage involves data collection of sentences between 14 words to 53 words. When users behave differently i.e. their typing patterns vary or their pressure input to keys vary, they are logged out.

3.3.5.4. Implementation of Multimodal authentication system:

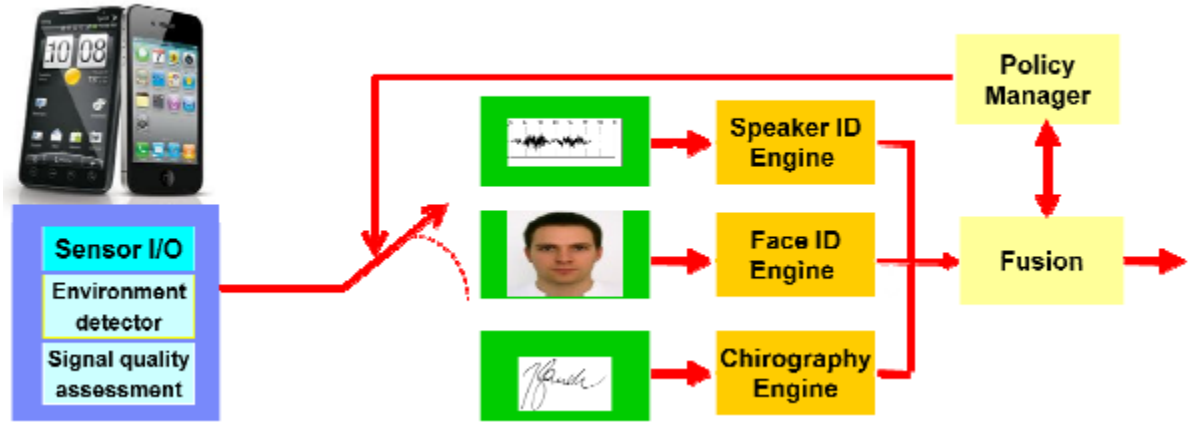

Figure 10: Architecture of multimodal biometric authentication system [38]

Three biometric engines are integrated in the system – 1) Voice, 2) Face, 3) Chirography. Enrollment is done by gathering input from the users. Verification is done by a policy manager who gets the following inputs – signal quality of voice and face modalities [38]. The three Engines process the data and gives a score as output. A confidence score is produced by the fusion engine taking into account the signal quality.

The chirography engine receives handwritten inputs written on a touch sensitive screen (user uses a finger here to sign). Scores are calculated using an algorithm which measures the stroke and the speed of the signature. (Given two sequences, how similar are they with respect to speed and time). Rotation, translation and normalization are done to both space and time for verification. Enrollment consists of user doing 6-10 iterations of signature. Verification consists of verifying current sign with the ten iterations and matching it with any [38].

It consists of five components - Face Detection (localize face area as an input image), Face Alignment (aligns the eye and the chin), Quality Evaluation (measures quality index – illumination, blur, asymmetry etc are considered), Feature Extraction (PCA is used to extract features from the input matrix), Similarity Measurement.

This consists of voice recording. Three authentication conditions are used here – 1) Global (common text is used for enrollment and verification), 2) Speaker (a user dependent password is used for enrollment and verification), 3) Prompted (a user is asked to speak a prompted text). Score fusion combines all three scores highly independent [38].

3.3.5.5. Threat Models:

i) Administrative frauds: Certain frauds like collusion, coercion, negligence, false enrollment and exception abuse can happen. These types of frauds happen before input is specified. For instance, before recording the fingerprint into the sensor, input can be modified by any of these frauds [2].

ii) Adversary attacks: Some of the adversary attacks include spoofing, altered finger, obfuscation, fake digital biometric and latent print reactivation.

iii) Unauthorized access through external compromised system: Templates or fingerprints are stored in the external database in the server. Unauthorized access to this database would result in stealing, deleting, modifying, substituting, reconstructing templates. Either of these would compromise the existing biometric system.

3.3.5.6. Counter-measures:

i) Viable cryptographic design: Viable cryptographic design must address power analysis attacks. Masking is a commonly used technique to defend against attacks. A robust secure cryptographic fingerprint matching technique would be immune to the general attacks [2].

ii) Time out/lock out policies: Hardening or increasing the security of the server where data is stored is an important aspect. One of the policies would be to have a time out or lock out system which activates if an intrusion is detected. Lock out helps to preserve data and it would prevent unauthorized access through external systems.

3.3.6. Transparent Authentication

Mobile phones usually authenticate once in the beginning and after that, the user can do anything using the phone including accessing secure apps. Hence there is a necessity for the user to be monitored and checked in a continuous (periodically in the background) and transparent (non-intrusive) manner even while the phone is being used.

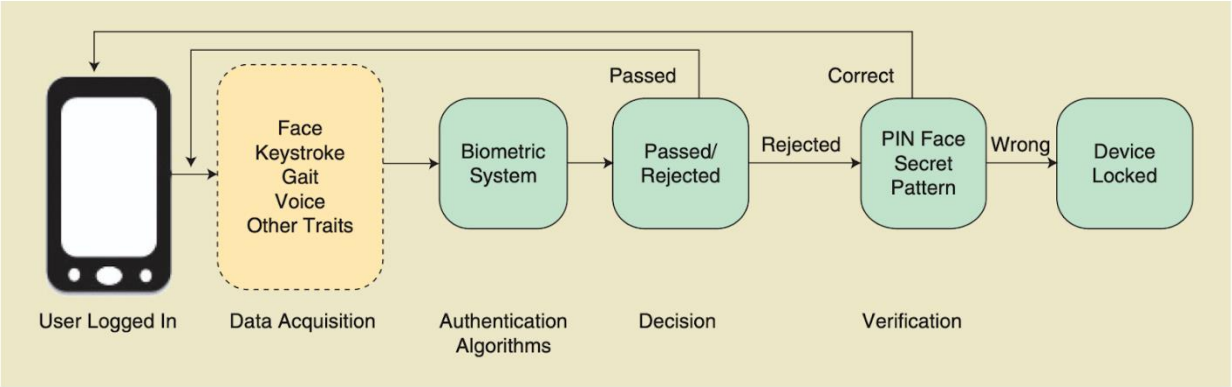

Figure 11:The steps involved in a generic process of transparent authentication [21]

A typical transparent authentication in mobile is shown in the figure above. The data for classifying the user is chosen and acquired by using the sensors in the mobile device. One (unimodal) or multiple (multimodal) sources of data can be used. Some kind of machine learning algorithm is applied over the data and a model is built. By comparing the current sensor values of the current user, the user is classified as a legitimate user or a fake user.

3.3.6.1. Metrics:

Physiological biometrics require more time and resources as compared to behavioral biometrics. The different metrics used to compare them are :

False Acceptance Rate (FAR): The rate at which fake users are authenticated by the system as legitimate users due to errors in the authentication system.

False Rejection Rate (FRR): The rate at which legitimate users are denied access by the system as fake users due to errors in the authentication system.

Equal Error Rate (EER): The rate at which FAR becomes equal to FRR are used in measuring the effectiveness of a biometric-based authentication system.

3.3.6.2. Typical methods

Saud Alotaibi et al. [34] provide a review of the 5 most widely employed types of transparent authorization systems (TAS). TAS is done using biometrics available on the can be widely employed using physiological biometrics such as fingerprint and behavioral such as touch.

i) Keystroke based authentication: is done by analyzing the key hold time, latency etc., when the user is typing. A behavioral feature vector is extracted from the recorded screen touch data, and a discriminative classifier is trained on these extracted features for authentication image-based feature called graphic touch gesture feature (GTGF) proposed in [43] for modeling touch dynamics. From the collected touch data, the system can identify the intruder from the owner.

ii) Gait: Wearable sensors or floor sensors or machine vision-based techniques can be employed for gait-based authentication. Once the raw data are measured, discriminative features are extracted, which are then fed into a classifier to distinguish users. Sensor orientation invariant gait representation called gait dynamic images. Also, pace independent gait recognition approaches have been proposed [70][99][53][62][47].

iii) Touch sensors based authentication: can be done by measuring the pressure, acceleration, time etc. that can be obtained from the touch screen. Other methods using touch employs analyzing gestures, analyzing touch in the context of different applications.

iv) Using devices sensors: such as the gyroscope, accelerometer etc. can also be used to perform authentication. Some papers argue that using multiple sensors for authentication can improve efficiency. Increased power consumption while reading the data from the sensors can be an issue while using device sensors.

v) Behavioral profiling: Based on the applications and services the user uses (Behavior). A behavior profiling method based on application usage, Bluetooth sightings, and Wi-Fi access point sightings was recently presented in [27]. The authors reported average identification rates of 80%, 77%, 93%, and 85% when using applications, Bluetooth, Wi-Fi, and the combination of these three types of behavioral features respectively.

vi) Face recognition: In [68], the feasibility of face and eye detection on cell phones was evaluated using the Adaboost cascade classifiers with Haar-like and local binary pattern (LBP) features [71], [72] as well as a skin color-based detector.

vii) Other approaches: Mobile-device movement and the ambient noise measured by smartphone microphones were used in [58] to implicitly authenticate mobile-device users. They also showed that a mobile user's identity could be verified by his or her voice with an EER of 7.77%. Linguistic profiling was used to authenticate users based on their writing vocabulary and style of short-message-service message.

3.3.6.3. Implementations

Mohammad Tanviruzzaman and Sheikh Iqbal Ahamed [41] demonstrate a framework that can be used to identify a user using gait and location using an android application. A set of sensors, with each sensor having a particular sampling rate, is used to compute the traits of the user. The authentication criterion is derived from a subset of traits using which the user is authenticated. A subset of templates (set of values representing a trait) is generated for a known set of n random users in the local DB. In the training phase, a subset of templates that represent the current user is generated which are sorted based on discriminatory power first and then using the required cost and used to check the authenticity of the

user. The application changes the confidence level depending on the familiarity of the location. Hataichanok Saevanee et al. [23] provide an implementation of a framework that performs authentication using biometric features of the user while

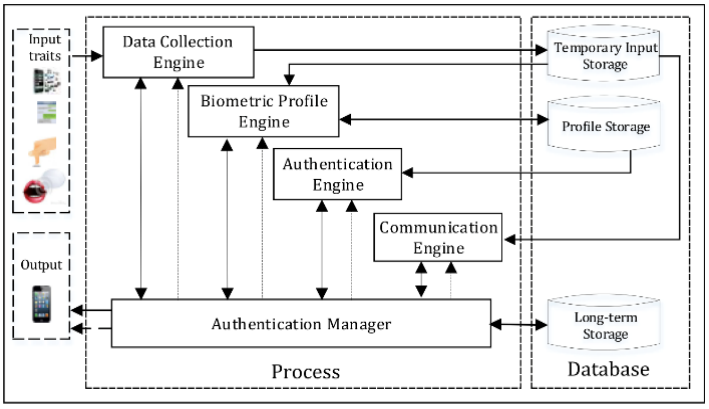

Figure 12: Text-based multimodal framework [3]

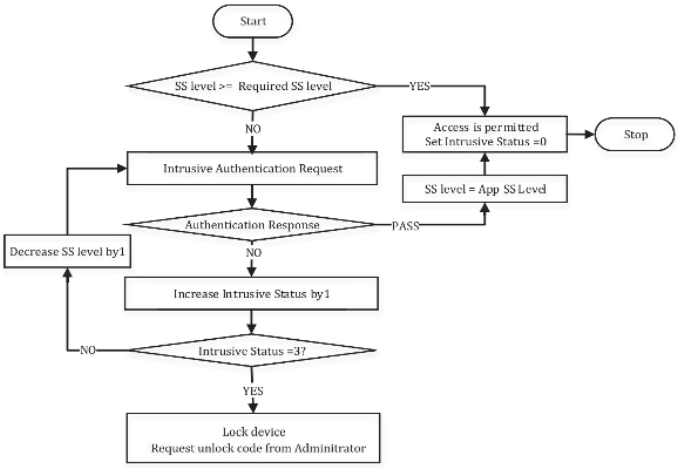

Figure 13: Process by which application requests permission from the framework [23].

also considering the security importance of an application using a numeric value called SS.

Data Collection Engine captures a user's typing patterns when user utilizes a text-based application. The Biometric Profile Engine generates the various biometric profile templates based on user's combination of the historical data and a number of template generation algorithms. The Authentication Engine authenticates the user by comparing the current input samples with the biometric templates while also considering the SS value. Authentication Manager is to monitor the security level updating them when necessary. One of the problems in transparent authentication is the privacy of the user data. Julien Hatin et al [11] present the idea of preserving the privacy of biometric data by usage of Biohashing algorithms, converting the raw sensor data into a hash, and comparing the hash with user biometrics to authenticate. The transformation function combines the user secret key K with the biometric features. Random vectors are generated using K, which are orthonormalized to generate the feature vectors. A code called BioCode is obtained from the feature vectors and this is stored instead of raw data. A new Biocode can be generated using secret key in case it gets lost. In the experiment, the phone number and location of the callee are used for authentication, which is done in the server. Every time a phone call is made the biocodes are sent to the server, where the server generates a bio template. When there is sufficient enrollment data stored for a particular user, the server changes to verification mode where the subsequent samples are classified as genuine or not by a classifier.

3.3.7. Continuous Authentication

Continuous authentication is a new technology that uses a person's behavior to continuously verify their identity throughout a session and not just at the entry login point. While two-factor authentication provides an extra layer of security over traditional authentication issues, by letting the user confirm their identity through multiple devices but the system is still open to vulnerability, since the password doesn't need to be confirmed again once a session is opened. Through analysis of a user's behaviors and interactions with a device, continuous authentication can spot vulnerabilities at any point in a session. Continuous authentication systems essentially make use of physiological and behavioral biometrics, using built-in sensors and accessories such as the gyroscope, touch screen, accelerometer, orientation sensor, and pressure sensor, to continuously monitor user identity. For example, front camera of a phone can capture images of the user and continuously authenticate the user. This ensures that the person using the device is actually the owner and not any impostor.

3.3.7.1. General Continuous Authentication Architecture and Workflow:

A general architecture of continuous authentication consists of two stages, i) Enrollment phase, ii) Authentication phase. In Enrollment phase, the system monitors and obtains data from the chosen sensor/ hardware such as camera, microphone, accelerometer etc., Features are extracted from the data and are fed to train a classifier. In Continuous Authentication Phase, the system continuously tracks data from the chosen sensor/hardware and the trained classifier estimates if it is a legitimate user or not.

In the figure 11, biometric system will determine whether these biometric traits correspond to a legitimate user or not. If the features do correspond to a legitimate user, the biometric system will continue processing the new incoming data. However, if the biometric system produces a negative response, the system will ask the user to verify his or her identity by using the traditional explicit authentication methods based on PIN, face, or secret pattern. [21] also talks about some of the continuous authentication implementation approaches as explained above in transparent authentication.

3.3.7.2. Implementation:

Sensor Based Smartphone Continuous Authentication

The paper by Y. Li et al. [6] proposed a novel sensor based Continuous Authentication System, **SensorCA.** The system uses three sensors namely: **Accelerometer, gyroscope, magnetometer** to continuously authenticate user's behavioral biometric pattern. This system is among the first to exploit the data augmentation approach of the rotation, which creates additional data by applying it on the collected raw data and improves the robustness of SensorCA. Here, the accelerometer records larger motion pattern such as how the user moves his arms or how he walks, gyroscope records fine grained motions, such as how to hold the smartphone, magnetometer records the ambient geomagnetic field. In the data

collection phase, data is captured from the above mentioned sensors when the screen is on. After preprocessing, data is stored in a protected buffer for data rotation. Users may prefer their own way of holding smartphones and sensors may generate non-diverse data. So, Data is rotated, augmented and stored in the form of a matrix. Then, 135 sensor-based features are extracted in both time and frequency domains within a time window on the augmented data. From these features, the most discriminable ones are selected and with the selected features, using the kernel ridge regression with truncated Gaussian radial basis function kernel (KRR-TRBF) to train the classifier in the enrollment phase. During the authentication phase, with the trained classifier and testing features available, SensorCA classifies the current user as a legitimate user or an impostor in the continuous authentication phase.

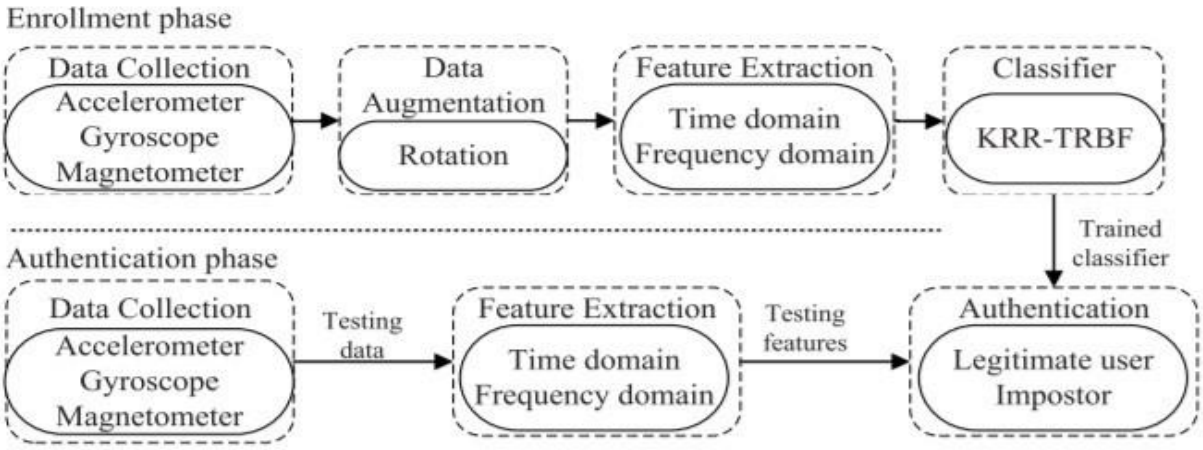

Figure 14: Architecture of SensorCA

3.3.7.2.1. Touch-Screen Based Smartphone Continuous Authentication

In this paper, Frank et al. [46] lays foundational work for continuous authentication schemes that rely on touchscreen input as a data source and without any dedicated and explicit security action that requires attention from the user. Frank et al. [46] main hypothesis is that continuously recorded touch data from a touchscreen is distinctive enough to serve as a behavioral biometric. A continuous authentication application could run in the background and extract multiple features from all available raw input. This raw input is readily available through the phone's API. The system defines two particular user actions called "Trigger-actions". - frequent and primitive actions. When user performs trigger-actions, system logs the fingertip data. Actions used are: (i)Sliding Horizontally and (ii)Sliding vertically .

During the enrollment phase, the system monitors the touch biometrics and extracts particular features from the touch data. This process continues until the distribution of touch-features converges to an equilibrium. This is the point in time when one can assume that i) the user got used to her device and her device-specific 'touch-skills' can no longer improve and ii) the system has observed sufficiently many strokes to have a stable estimate of the true underlying feature

distribution of that user. At that point, the system can train the classifiers and switch to the classification mode for authentication. During the continuous authentication phase, the system continuously tracks all strokes and the trained classifier estimates if they were made by the legitimate user. Here, t consecutive negative classification results the system resorts back to the initial entry-point based authentication method and challenges the user. The classifier strength affects the time it takes to make a decision.

3.3.7.2.2. Progress and Challenges with Continuous and Transparent Authentication:

Vishal M. Patel et al.[21] provides information about the recent progress and remaining challenges in transparent authentication.

3.3.7.2.2.1. Problems with Unimodal Authentication

i) Noisy data: Poor lighting on a user's face or occlusion are examples of noisy data.

ii) Non-Universality: The continuous authentication system based on a single source of evidence may not be able to capture meaningful data from some users. For instance, gait-based systems may extract incorrect patterns for certain users due to leg injuries.

iii) Intraclass variations: These often occur when a user incorrectly interacts with the sensor.

iv) Spoof attack: Using a photograph to gain access to a user's mobile device is an example of this type of attack. legitimate user.

Fusion using information from different modalities can solve some of the issues mentioned above. Information fusion can be done at different levels, which can be broadly divided into :

a. Feature-level,
b. Score-level, and
c. Rank/decision-level fusion.

Feature-level fusion method based on multitask multivariate low-rank representations was recently proposed in [28] for fusing touch gestures and faces for continuous authentication. Decision-level fusion method was proposed in [32] for fusing four modalities based on stylometry (text analysis), application usage patterns, web browsing behavior, and physical location of the device for continuous authentication. A set of behavioral features called hand movement, orientation, and grasp (HMOG) [18] . HMOG features are combined with tap and keystroke features using a score-level fusion framework.

3.3.7.2.2.2. Usability and security issues

i) In the continuous authentication context, a false rejection is less costly than false acceptance. This is due to the fact that higher false acceptance rates will lower the security level of the continuous authentication system, while a higher false rejection rate will frustrate a legitimate user.

ii) Human factors should be incorporated into the design of continuous authentication systems, where usability is central

during the whole development process.

3.3.7.2.2.3. Other Issues to be addressed:

i) Some of the physiological, as well as behavioral biometrics-based continuous authentication methods, are vulnerable to spoofing, mimic, statistic, or digital replay attacks.

ii) There is no clear standard for evaluating the performance of different methods in the literature. Guidelines on an acceptable benchmark are needed.

iii) Most continuous authentication methods ignore usability and acceptability issues.

iv) The biometric data at enrollment time may have different characteristics than those presented during authentication.

v) As private firms begin implementing the transparent authentication on their devices, the collection of data increases privacy issues such as data being disclosed to third party companies.

vi) Preventing the theft of the biometric patterns of mobile-device users, biometric template protection schemes such as cancelable biometrics should be incorporated

vii) Most of the approaches are tested only on small or midsize data sets. The authentication mechanisms need to be evaluated on large-scale datasets containing thousands and millions of samples.

3.3.8. Location Based Authentication

Fig. 14 shows the architecture of a location based authentication system. It has the following components:

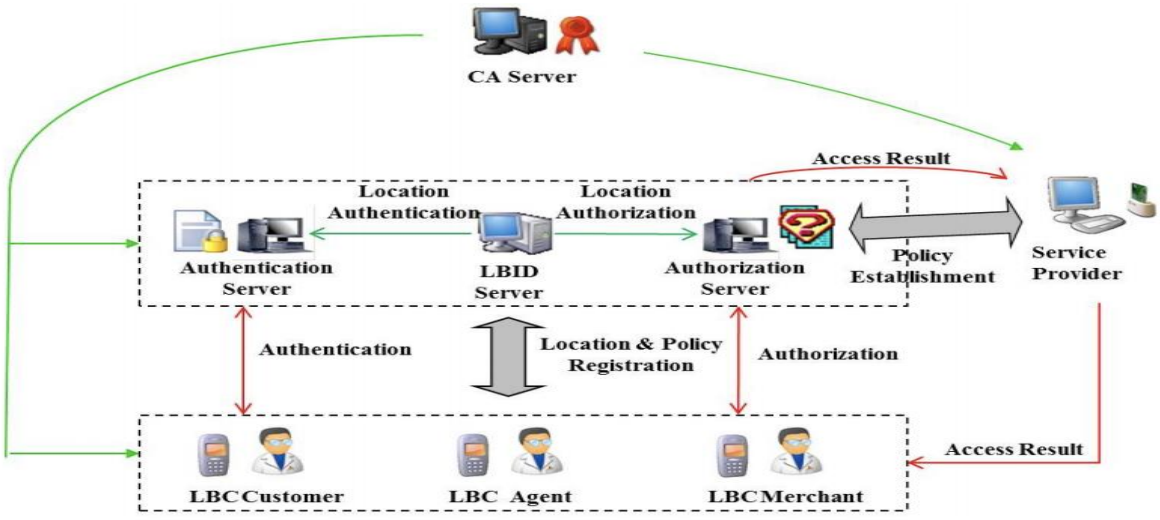

Figure 15: Location Based Authentication and Architecture

i) Location-based ID (LBID) server: core component of architecture, which stores users' location information and authorization policies. It provides location registration, authentication and authorization services. (Users' location information contains latitude, longitude, range of location accuracy, technology used to determine location.)

ii) Certificate Authority (CA) server: provides certification of all system participants, issuing, managing and distributing

their certificates

iii) Authentication server: provides authentication service for all participants. It can be any existing authentication service, such as username-password authentication.

iv) Authorization server: provides authorization services for all participants. It can be any existing authorization service, such as role-based authorization.

v) Service Provider (SP) server: provides various mobile services.

vi) Location-based Client (LBC) Application: an application running on the user's mobile device, capable to collect location information from trusted Location Providers (LP) and providing user interfaces to register, store and manage location data. The biggest vulnerability here is to secure the user's location. The system used cryptographic techniques, based on Public Key Infrastructure (PKI) and certificate mechanisms.

3.3.8.1. Protocols:

3.3.8.1.1. Registration:

It is done only once, after joining the system. Download LBC on phone. Link to LBID server using pin. After entering PIN/random number, the LBC sends data together with user's location data, determined in that moment to the LBID server. The message is signed by LBC and encrypted with LBID server's public key. Once receiving the message, LBID server decrypt it with its private key and verifies the user's signature with user's certificate and stores the information in the form of a new rule in the authorization policy.

3.3.8.1.2. Authentication and Authorization:

The process begins when the user tries to access the protected resource (e.g. login into his/her account). The process is initiated by user sending a service request to the Location registration SP server. SP server directs service request to the Authentication server to authenticate the user. The Authentication server sends an authentication challenge to the user. The user then responds to the challenge by providing his/her security credentials back to the Authentication server for authentication purposes, which can be any existing mechanism depending on the implementation of the particular

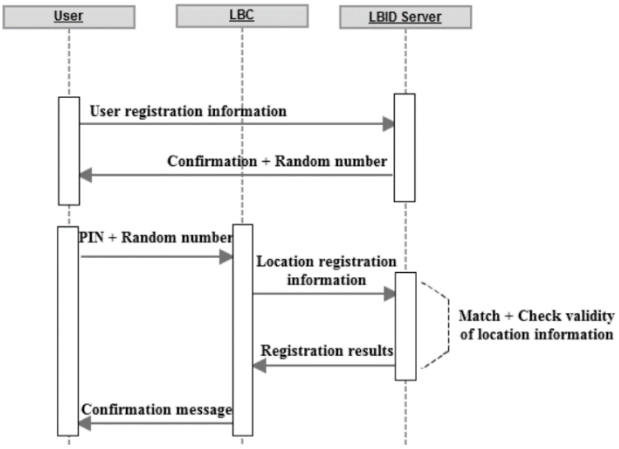

Figure 16: Location Registration

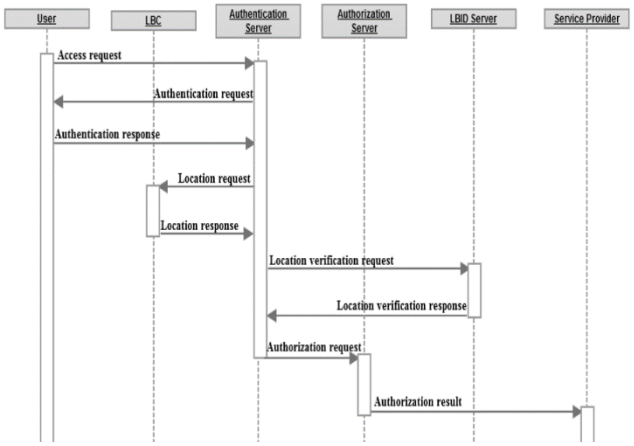

Figure 17: Location Based Authentication and Authorization.

system.

Upon successful verification of user credentials, the Authentication server sends a location verification request to the LBC running on user's smartphone. The LBC prompts the user to enter PIN. User responds by entering the PIN in order to authorize a location response.

LBC then determines the user's location and sends it back to the authentication server within location response message. The location information is signed by LBC's private key and encrypted by LBID server's public key. After that, the authentication server delivers user's location information to the LBID server. LBID server decrypt the message using its private key and verifies the user's digital signature.

If the verification is OK, it compares user's location information with the location data stored in its database during registration phase, namely compare static location with dynamic location, and sends authentication result with user's location information to the authentication server. On authentication, the authentication server sends authorization request, comprising user's access request and user's location information, to the authorization server.

3.3.8.2. Threats:

i) Spoofing on hardware level: Done via the location (GPS) module. An attacker can directly hack into the GPS hardware or module or simulate it in software and modify it to provide fake location signals to the smartphone operating system and consequently to the location-based client. In this way, the signals are intercepted at the lowest possible level before they reach the client and as a result it ends up deducing an incorrect location.

ii) Spoofing on the OS level: This is done by intercepting and modifying the location APIs in the smartphone operating system so that they report a fake location to the client application. This kind of an attack is possible in open source type of smartphone OSs where the source code is accessible and can be modified.

iii) Spoofing on the application level: This kind of spoofing happens directly on the location client application by modifying its source code or by intercepting and modifying the final location result that is sent to the location-based server. A fake or modified copy of the location client application can be installed in the smartphone and report spoofed locations to the server.

3.3.9. Risk Based Authentication

Risk based authentication is a type of multi factor authentication which customizes the authentication for each user login. There is a huge increase in cyber threats because of conventional methods of authentication like username/password. The systems are prone to cyber-attacks like phishing, DNS attack and risk based authentication adapts and customizes the login using the login parameters/context and makes applications more secure.

For the Risk Based Authentication System using Machine Learning [12] the design of risk engine which is coupled with the

application follows the following steps: i) Examine user's past login records. ii) Generate suitable pattern using Machine learning algorithms. iii) Calculate risk level of user. iv) Decide Authentication method based on risk level.

Risk based authentication system consists of 3 following blocks:

i) Profile Analysis Block: The authentication severs taken into consideration users' parameters which are needed to model the user's behaviors. The parameters that are taken into consideration are IP address, Geo location, Time zone, Login time, OS version, Browser version, Device type. All the user's past login records are stored into the authentication server. Profile analysis block sends the record of history of the user's parameters and current user's parameters to risk engine. Profile analysis block also keeps track of the number of failed authentication attempts.

ii) **Risk Engine:** Risk Engine is one of the core components of this system and this component helps to predict the risk level of a user. The risk engine is built using following machine learning algorithms like Support vector machines, one-class support vector machines, Naive Bayesian. Main objective of risk engine is to find out anomalies in the given data. One-class SVM is applied and the output of one-class SVM is either true or false. True indicated that the user is genuine and false indicates that the user may be fraudulent. If the output of one-class SVM is false then we need to then calculate risk score of the user:

Risk score = sum of(user_parameter_value X user_parameter_weight)

user_parameter_value = 0 (behaviors exists in the past login records)

user_parameter_value = 1 (otherwise)

Naive Bayesian classifier is based on following baseman formula:

P(h|d) = (P(d\h) * P(h))/ P(d)

Where h refers to user being genuine or gradient and d refers to each user parameter stored in server database.

iii) **Adaptive Authentication Block:** The risk score which is calculated by the risk engine is fed into policy manager which then considers the risk score and calculated risk level.

3.3.9.1. Risk Based Authentication management model:

3.3.9.1.1. Description of user authentication :

Any user who wants to use the authentication management system must first register where they have to answer information about their behavior. Otherwise the system can also automatically collect this information with user's consent. The system begins in learning mode and once the system decides that it has enough information to work then it switches to working mode. Once the system has enough information to calculate level of security and level of risk, the system goes ahead and chooses authentication mechanisms which meet security requirements. The system changes authentication mechanism after 3 failed attempts to login.

3.3.9.1.2. Risk parameters

Level of risk is calculated according to the following formula:

$$R_i = L * I * (1 + \alpha) * \beta$$

Where L is the likelihood of a success of an attack, I is the impact of an attack, α is the factor of fluctuation of contextual data in a given category and β is data correlation factor and data correlation factor can be calculated using data correlation checking algorithm [5].

$$\alpha = |V_w - V_\alpha|$$

Where Vw is the fluctuation factor for the model event, Va is the fluctuation factor for the current event.

β = 1 if no correlation exists and β = 2 if correlation exists.

3.3.10. Adaptive Authentication

Adaptive authentication helps us secure the authentication process by identifying any anomalies in the attribute factors from the context information. Adaptive authentication is helpful in avoiding high risk and suspicious login attempts. Login Attributes like IP address, geo location, time zone, login time, OS version, browser version, device type is taken into the consideration. Adaptive authentication enables customization of authentication process for a user, based on login context and tries to spot high risky login attempts and immediately customizes the user's login requirements. Nowadays services are adopting authentication which is less intrusive like key strokes dynamics, gait recognition, user voice etc. There is no one-size-fits-all type of authentication and where adaptive authentication plays an important role. We need to sense the environment and customize our authorization for more usable, secured systems. Users tend to carry same habitual behavior for authentication. We can define a user's normal behavior by taking the login time, geolocation etc. into consideration and apply data analytics to build rich and comprehensive information about users. User authentication can be defined as user identification based on what user knows, what user has and what user does.

3.3.10.1. Adaptive system Model [11]

Adaptive system comprises set of managed resources and adaptation logic which

i) Monitors the environment (M)

ii) Analyses the data for changes (A)

iii) Plans adaption (P)

iv) Executes adaptation (E)

v) Contains shares Knowledge repository (K).

The above activities together are called MAPE-K cycle. To decide what has to be done in MAPE-K cycle, we need to answer the following 5 basic questions:

1. Why to adapt? (Reason)

We need to adapt to make applications more secure, improve usability of authentication process for the user and we can take users authentication preferences into consideration

2. When to adapt? (Time)

Adaptation can be triggered in 2 ways

Reactive: Here the adaptation is triggered after the occurrence of the event

Proactive: Here the adaptation is triggered if the adaptation logic predicts an event top happen. This is suitable to avoid interrupting the users flow but it utilizes CPU cycles and resources in order to constantly monitor and predict users' movements.

3. What to adapt? (Level)

Adaptation techniques must be identified on different levels. There are 2 types of techniques

Parametric: Parametric system modify system behavior by modifying the system parameters

Structural: Change of components or new composition of components or addition/removal of components

4. Where to adapt? (Technique)

Authentication can be adapted on following levels: Application level, System level, Communication level. System architecture which has application level authentication is better because it provides space for granular security whereas at system level adaptation, we must put tightest authenticators in place because we are giving access to entire system and we must be most careful.

5. How to adapt? (Control)

To answer this question, we take 3 aspects into consideration, approach, criteria, degree of centralization. **Approach:** The logic follows an internal approach which combines the system resources with adaptation logic. Or we can follow an external approach which splits the system into adaptation logic and resources.

Criteria: One can consider Rules, Goals, Models, Utility function, Combination of the above as a criterion. **Degree of centralization**: One can develop a Centralized, Decentralized or a Hybrid system.

3.3.10.2. Adaptive Unified Authentication Platform (UAP) [34]

This platform provides a method to decide if a user can be considered as an authenticated entity. An additional trust engine component is added to unified authentication platform to create a new generation of UAP. This trust engine takes attribute factors into consideration from the behavior of user profiles. Pattern generation and trust evaluator are the 2 processes of adaptive UAP.

Pattern generation: It analyses context information from the past logins of the user.

Trust Evaluator: Analyses, decides and acts on login request from users. Trust evaluator takes decisions on user authentication based on Authentication method score, Attribute score, Application required trust level.

For a user to be considered as an authenticated entity by the service it has to satisfy the following formula

$$attributeScore = ((time * weight_{time}) + (geolocation * weight_{location}) + (browserOS * weight_{browser}) + (application * weight_{application})) * (maxuserscore)$$

A is Authentication method strength, B is User attribute score, C is application security requirement.

User attribute score: User attribute score is the uncertainty level of current login attempt compared to the user behavior profile which is established.

3.3.11. Gesture Based:

Biometric authentication is one of the popular methods of authentication systems due to its security. Adding gesture as another metric in biometrics makes it much more harder to hack because it is difficult to imitate gestures. This research aims to use three-dimensional (3D) depth information of gesture movement to perform authentication with less user effort. We propose an approach based on depth cameras, which satisfies three requirements: Can authenticate from a single, customized gesture; achieves high accuracy without an excessive number of gestures for training; and continues learning the gesture during use of the system [76].

3.3.11.1. Process:

Different users have different muscle memories and hence their gestures would be different and unique. This is hence a dynamic behavior feature. When the user wants to unlock their computer or mobile, they need to perform their own gesture “password” which is captured in the camera and then the device is unlocked. The entire process is natural and smooth.

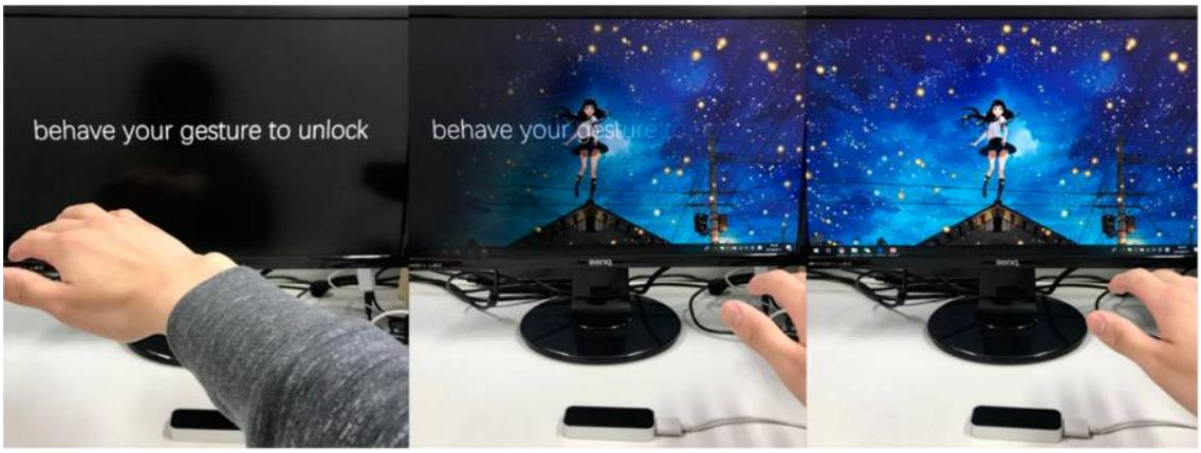

Figure 18: Unlocking a computer by gesture

The idea of this system is to: 1)Authenticate from a single and customized gesture, 2)Achieve high accuracy without an excessive number of gestures for training, 3)Continues learning the user’s gesture during the use of the system. The system has some drawbacks though - it cannot be used by all mobile devices since it needs a depth camera to record 3D gesture movement [76].

Some of the steps for this method is described below in the diagram. It involves preprocessing which uses Gaussian filters to clean the data, then 3D data is mapped to three 2D images in XY, XZ, YZ planes. 3 sparse autoencoders will classify these input data as a legal or non-legal gesture.

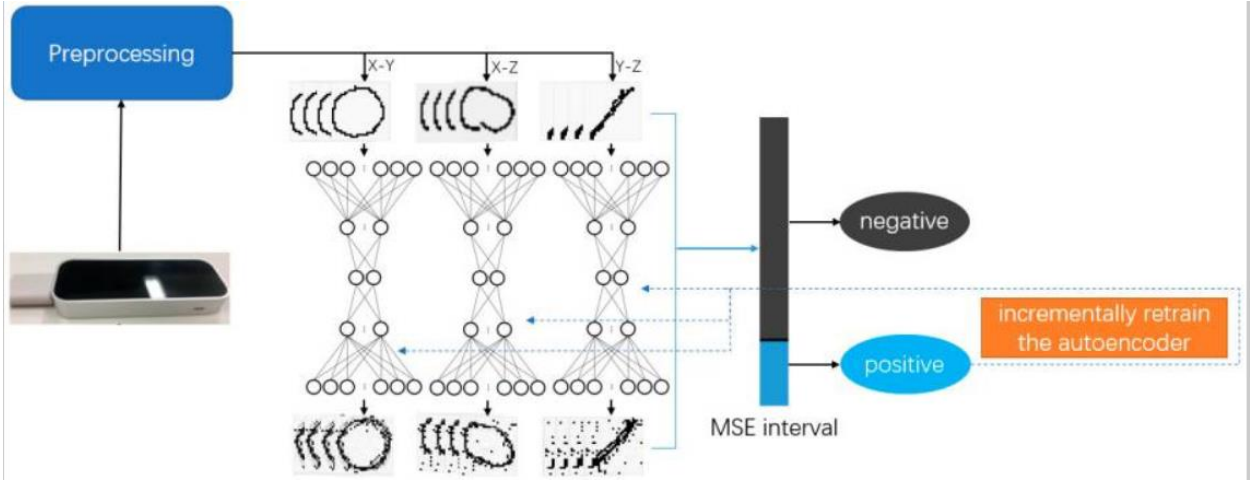

Figure 19: Algorithm Flow Chart

One important aspect of this system is the incremental learning. This system has the ability to gradually learn new knowledge from new batch of data. While the system is been used, the system would simultaneously learn from new batch of data. There are two main reasons for using incremental learning. One reason is our user-friendly consideration that it is not practical for a user to perform several gestures during the training stage. Using incremental learning will solve this problem, because it prevents the need for several gestures. Another reason is that incremental learning will increase the accuracy during use, because the autoencoder gradually learns the user habits, and from the unique data of others that will largely reduce the false rejection rate of the system.

3.3.11.2. Threats:

i) Lego-driven robotic attack [77]: This attack uses input derived from swiping samples stolen from the victim. This is basically based on the Lego robot which runs an algorithm that attacks the user's input.

ii) User-tailored robotic attack [77]: This attack uses inputs gleaned from the general population and uses this data to attack user's gesture. If only a single point of gesture is used for authentication, then simulation of this gesture can be done with substantial time.

3.3.11.3. Counter-Measures:

i) Fusion of metrics: Instead of just single point of entry, having multiple metrics for authentication would help - combining multimodal biometrics with gesture based would fortify the system.

ii)Pattern Recognition/Liveness detection: Such techniques would identify patterns of user's vs robot's. The principal idea is that robotic movements rotate around a small set of canonical movements. For ex: a given motor can rotate left or right only through a finite set of possible angles. Humans on the other hand are able to execute much more complex movements.

4. Conclusion:

The increasing popularity of mobile phones and ever improving possibilities makes mobile devices such as phones and tablets an inevitable part of human life. People use mobile phones more and more, and they have started storing and transmitting important data from mobile phones. Understanding the importance of the data and the privacy of the user, in this paper, we have researched about the authentication of users in mobile phones. We discuss about the typical methods employed currently for mobile authentication. Then we move on and start discussing about more advanced techniques such as biometric authentication and multimodal authentication. Those are followed by recently developing techniques like continuous and transparent authentication where the users are continuously being verified throughout the phone usage session. While providing the background and concepts about various authentication techniques we have also researched and presented the various real-world implementations of the above-mentioned concepts, resulting in more understanding of these concepts and how they can be improved further.

In Table 1 we have performed a comparative analysis of the security level of each technique. We took the 5 most common attacks on all authentication techniques and classified whether each authentication technique discussed above is sussceptible to that attack or not.

One-shot authentication is one of the earliest and simplest forms of authentication on mobile devices. Though they are easy to implement and use, they come with their own drawbacks. Once the user is authenticated, the user will have full access to the device (except for protected areas) resulting in potential security issues. Even after the drawbacks and security issues, one-shot authentication tends to be the most commonly used form for authentication for mobile devices because of their convenience and ease of implementation.

Token based authentication allows users to fetch specific resources with the help of a token as a means ofauthentication. Tokens are stateless, scalable and simplify authentication, which is just a click away with tokens.However, using tokens for authentication also makes the system susceptible to man in the middel and replayattacks.

Single sign-on method serves use to those who wish to login into multiple applications using the same account of one application. While it improves convenience for the users, it also comes with a risk of privacy breach because we will provide one application control over other applications.

Table 1: LEVEL OF SECURITY FOR DIFFERENT SMARTPHONE AUTHENTICATION TECHNIQUES

Technique Name	Brute Force	Shoulder Surfing	Smudge Attack	Dictionary Attack	Spyware
Pins/Passwords [40],[7],[56]	Yes	Yes	Yes	Yes	Yes
Pattern based Passwords [3]	Yes	Yes	Yes	Yes	Not Defined
Graphical based Passwords [40], [7]	Yes	Yes	Yes	Yes	Not Defined
Software Token Based [75],[63],[45],[40],[7]	Yes	Yes	Yes	Yes	Yes
Hardware Token Based [75],[63]	Yes	Yes	Yes	Yes	Yes
TrustOTP System [36]	Yes	Yes	Yes	Yes	Yes
OAuth 2.0 (Single Sign On) [14]	Yes	Yes	Yes	Yes	Yes
Location Based [50]	No	No	No	No	Yes
Fingerprint [37], [39], [40], [60], [70]	Yes	No	Yes	Yes	Not Defined
Face recognition [37], [39], [40], [60], [70]	Yes	No	No	Yes	Not Defined
Iris [37], [39], [40], [60], [70]	Yes	No	No	Yes	Not Defined
Voice [40], [7]	No	No	No	No	Not Defined
Keystroke-dynamics based [64]	No	No	No	No	Yes
Accelerometer Biometrics [26]	No	No	No	No	Yes
Power Consumption [30]	No	No	No	No	No
Touch Gestures [22]	No	No	Yes	No	Yes
Single Sign-On [55],[24]	Yes	Yes	Not Defined	Yes	Yes
Multi-Factor [56],[17],[4]	No	No	Yes	No	No
Continuous [6],[21],[46]	No	No	Not Defined	No	Not Defined
Transparent [41],[21],[11], [23], [34]	No	No	Not Defined	No	Not Defined
Behavioural Profiling [65]	No	No	No	No	No
Gait Recognition [26]	No	No	No	No	Yes
Gesture Based Biometric [76]	No	No	Not Defined	No	Not Defined

We finally discuss the advantages, disadvantages of the concepts, the types of attacks that can be performed and the risks they possess.

Table 2: COMPARATIVE ANALYSIS OF DIFFERENT AUTHENTICATION TECHNIQUES FOR SMARTPHONES

Technique Name	User friendly	Computational cost	Security	Reliable	Fast Authentication	Resource requirement	Merits	Demerits
Pins/Passwords [40],[7],[56]	Yes	Low	Low	No	Yes	String Comparison only	Easy, less time taking, User friendly	Breakable, Conflict in passwords
Pattern based Passwords [3]	Yes	Low	Low	No	Yes	Pattern comparison only	Easy to remember, user friendly,fast.	Breakable, trackable.
Graphical based Passwords [40], [7]	Yes	Medium	Medium	Medium	Medium	Database requirement	Better to memorize graphical passwords, reliable and accurate. More difficult to break than Text based passwords.	Not widely used, requires more memory so higher storage requirement
Software Token Based [75],[63],[45],[40],[7]	Yes	Low	Low	Yes	Yes	Authentication device such as a smartphone.	Flexible, cost effective, easy to implement	Vulnerable to viruses, software attacks.
Hardware Token Based [75],[63]	Yes	Medium	High	Yes	Not always	Hardware device with built-in LCD display.	Highly secure, time based passcode	Devices might break, easy to forget, expensive
TrustOTP System [36]	Yes	Medium	High	Yes	Yes	Smartphone, touchscreen driver	Flexible, low power consumption, secure	Depends on battery of phone, phone might get lost
OAuth 2.0 (Single Sign On) [14]	Yes	Low	High	Yes	Yes	Credential storage	Ease of use, privacy promoting, secure	Vulnerable to data misuse, phishing, lack of anonymity
Location Based [50]	Yes	High	Medium	No	Not always	Smartphone with GPS	Transparent to user, Easy to integrate into existing system, No need to set up separate infrastructure	Accuracy of GPS is critical, might not work in basements, inside big buildings
Fingerprint	Yes	low	High	Yes	Yes	Mobile	Highly secure, faster	Can be hacked if

[37], [39], [40], [60], [70]						device with fingerprint sensor	and easier to authenticate. Currently used in most of the modern devices.	fingerprints can be obtained. Doesn't change with time
Face recognition [37], [39], [40], [60], [70]	Yes	low	High	Yes	Yes	Mobile device with camera	Secure, faster and easier. Currently used in most of the modern devices.	Is vulnerable to spoofing.
Voice [40], [7]	Yes	High	High	No	Not always	Smartphone	User friendly and ease of use is high	Difficult to reduce noise from data.
Iris [37], [39], [40], [60], [70]	Yes	Medium	High	Yes	Yes	Mobile device with high resolution camera	Highly reliable and quick authentication	One of the best possible methods since it is hard to obtain the iris image.
Keystroke-dynamics based [64]	Yes	Medium	High	Not always	Yes	Smartphone	Reliable and less hackable	Time taken to authenticate is not as quick as fingerprint or iris.
Accelerometer Biometrics [26]	Yes	High	Medium	Not always	No	Wearable device to detect motion	Not much reliable due to less significant difference between user	Useful for Continuous authentication
Power Consumption [30]	Yes	Medium	Low	Yes	No	Smartphone	Useful for continuous authentication	Requires huge amount of data gathering
Touch Gestures [22]	Yes	Low	High	Yes	Yes	Smartphone	No additional input required from user	Too many features to select so either selecting a few fea
Single Sign-On [55],[24]	High	low	low	High	Yes	Smartphone	Easy to Authenticate multiple applications with single sign	Compromising the main authentication will put privacy threat on the rest of the

								application
Multi-Factor [56],[17],[4]	No	High	High	High	No	Depending on the technique used, might require a wrist watch.	Highly secure and reliable	Authentication is not fast
Continuous Authentication [6],[21],[46]	Yes	High	High	Yes	No	Depending upon the biometric technique used.	Doesn't hinder user's work. Highly secure.	Uses more computation power.
Transparent Authentication [41], [21], [11], [23], [34]	Yes	High	High	Sensor and algorithm dependent	No	Technique dependent	Doesn't hinder user's work.	High computations, Privacy issues in storing data
Behavioural Profiling [65]	Yes	Medium	High	Yes	Yes	No additional hardware needed	Useful for continuous authentication. Highly secure.	Requires large amount of data to train to have enough confidence in result
Gait Recognition [26]	yes	High	Medium	Yes	No	Sensors required to detect motion	User friendly	High computations needed
Gesture Based Biometric authentication [76]	No	High	High	No	No	Requires high depth camera to capture gestures	Highly secure, combined with biometrics, it is more secure.	Time taken to authenticate and resources used for authentication are high.
Adaptive authentication [11], [34], [12]	Yes	HIgh	High	High	Depends on user's context parameters	Adaptive authentication system	Makes application usable, reliable, secured	Overhead of adding adaptive authentication mechanisms to the application.

Biometrics serve as an important modality to identify a user and many of the biometrics can effectively and uniquely help distinguish a person from another person. We have researched about usage of biometrics to authenticate users.
Regarding physical biometrics, we have analyzed different aspects of Biometric authentication systems and their vulnerabilities. We have analyzed methods like Liveness detection, Watermarking and Biometric cryptosystems which can be used to enhance the integrity of the authentication systems and found that there is no security technique which can satisfy all the aspects of an ideal biometric template protection scheme. An establishment of efficient and foolproof security technique needs further research work in physical biometric- based authentication systems.

With the analysis on various behavioral biometrics systems, it can be concluded that unique biological and behavioral features of the user like voice, typing pattern, mobile phone usage pattern, gait, touch and many more can be used to authenticate the user. With the analysis of these systems, we have studied various challenges and solution to challenges which would encounter to authenticate the user.

Unimodal authentication is secure because the features of virtual typing can only be extracted from the typing habit, finger muscle and finger size. Touch pressure is hard to observe and mimic. And features such as typing time interval and pressing time are quite user dependent and hard to mimic. Since the virtual key typing authentication is a continuous context-free mechanism, it is very difficult for intruder to avoid it or using replicate to attack.

For further security, multiple modalities for authentication can be used. Hacking is hard - Bots can’t hack voice if password voice is hacked, a person can’t hack password if voice is hacked. Using multiple modalities, error rate is reduced and security is increased. The whole process is cumbersome and takes a lot of user’s time - ideally this can be used in places where speed is less important and security is more important. Speed is not the important factor here.

To avoid the issues with authenticating the user only once, the device usage and the user’s traits needs to be continuously monitored to verify if the person using the phone is still a legitimate user. Continuous authentication has the potential to modernize an often-neglected process: determining if a person attempting to access or use a device, application, server or system, is who they claim to be, throughout their entire interaction with the system. With careful planning and oversight, continuous authentication would thwart attacks that exploit compromised credentials in a way that creates a frictionless user experience to better protect enterprise information systems and the data they contain. The technology building blocks exist. Operationalizing and implementing is the next step.

Location based authentication is easy to integrate into the system and transparent to the user. Since allsmartphones come

with a built-in Global Positioning System (GPS), it does not require any separateinfrastructure. While versatile, authentication done usinglocation information is vulnerable to spoofing on theoperating system level, hardware as well as application level if developer is not cautious.

Transparent authentication is recently developed for mobile devices. Transparent authentication enhances the security of the mobile devices by continuously verifying the user when the phone is being used. It is different from continuous authentication from the way it authenticates the user, in a non-intrusive manner that doesn't affect the user experience. Energy and CPU consumption is an issue with transparent authentication but with the advent of new energy efficient sensors and algorithms, those issues will be resolved in the near future. The privacy issues of storing the user traits is also being solved by the recent techniques.

With all the above-mentioned methods being fixed, the future relies on a type of authentication namely, adaptive authentication. Organizations are moving towards it not only to make applications more secure but also to make online applications more usable. Static multi-factor authentication makes the authentication process more tedious to users than necessary. Adaptive authentication customizes authentication process for each login and stores the login parameters to analyze the future logins making applications usable and secure.

Every technique discussed above is somehow breakable and requires improvement in some way or the other. In this paper, by reviewing the pros and cons of various available authentication schemes, we provided a substantial overview on the authentication solutions for the mobile devices. In present, there are numerous researches on cell phone security, yet there is a lack of effort to analyze all security threats of mobile devices.

5. References:

1. Yang, Wencheng & Wang, Song & Hu, Jiankun & Guanglou, Zheng & Valli, Craig. (2019). Security and Accuracy of Fingerprint-Based Biometrics: A Review. Symmetry. 11. 141. 10.3390/sym11020141.
2. Joshi, Mahesh, Bodhisatwa Mazumdar, and Somnath Dey. "Security vulnerabilities against fingerprint biometric system." arXiv preprint arXiv:1805.07116 (2018)
3. Z. Hills, D. F. Arppe, A. Ibrahim and K. El-Khatib, "Compound Password System for Mobile," 2018 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), Glasgow, 2018, pp. 1-4.
4. Aaron Dale SANDERS, COMPARTMENTALIZED MULTI - FACTOR AUTHENTICATION FOR MOBILE DEVICES in United States (12) Patent Application Publication Jan 4 ,2018
5. Sepczuk, Mariusz, and Zbigniew Kotulski. "A new risk-based authentication management model oriented on user's experience." Computers & Security 73 (2018): 17-33.
6. Y. Li, H. Hu, G. Zhou and S. Deng, "Sensor-Based Continuous Authentication Using Cost-Effective Kernel Ridge Regression," in *IEEE Access*, vol. 6, pp. 32554-32565, 2018.
7. Usman Shafique, Hikmat Khan, Sabah-ud-din Waqar, Asma Sher, Adnan Zeb, Uferah Shafi, Rahim Ullah and Rehmat Ullah, “Modern Authentication Techniques in Smart Phones: Security and Usability Perspective” International Journal of Advanced Computer Science and Applications (IJACSA), 8(1), 2017.
8. Sharma, Manisha, Raju Baraskar, and Shikha Agrawal. "A Comparative Analysis of Unimodal and Multimodal Biometric Systems." International Journal of Advanced Research in Computer Science 8.5 (2017).
9. Parreno Centeno, Mario & van Moorsel, Aad & Castruccio, Stefano. (2017). Smartphone Continuous Authentication Using Deep Learning Autoencoders. 147-1478. 10.1109/PST.2017.00026.
10. Toan Van Nguyen, Napa Sae-Bae, Nasir Memon,DRAW-A-PIN: Authentication using finger-drawn PIN on touch devices, Computers & Security, Volume 66,2017,Pages 115-128.
11. Hatin, Julien, et al. "Privacy Preserving Transparent Mobile Authentication." ICISSP. 2017.
12. Arias-Cabarcos, Patricia, and Christian Krupitzer. "On the design of distributed adaptive authentication systems." (2017): 1-5.
13. Misbahuddin, Mohammed, B. S. Bindhumadhava, and B. Dheeptha. "Design of a risk based authentication system using machine learning techniques." 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI). IEEE, 2017.
14. M. Argyriou, N. Dragoni, and A. Spognardi, "Security Flows in OAuth 2.0 Framework: A Case Study", 2017, SAFECOMP 2017 Workshops, LNCS 10489, pp. 396–406.
15. Jamdar, C. and Boke, A., 2017, August. Multimodal biometric identification system using fusion level of matching score level in single modal to multi-modal biometric system. In 2017 International Conference on Energy,

Communication, Data Analytics and Soft Computing (ICECDS) (pp. 2277-2280). IEEE.

16. M. Al-Rubaie and J. M. Chang, "Reconstruction Attacks Against Mobile-Based Continuous Authentication Systems in the Cloud," in IEEE Transactions on Information Forensics and Security, vol. 11, no. 12, pp. 2648-2663, Dec. 2016.
17. Yohan, Alexander et al. “Dynamic multi-factor authentication for smartphone.” 2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC) (2016): 1-6.
18. Z. Sitová, J. Šedeˇnka, Q. Yang, G. Peng, G. Zhou, P. Gasti, and K. S. Balagani, “HMOG: New behavioral biometric features for continuous authentication of smartphone users,” IEEE Trans. Inform. Forensics Security, vol. 11, no. 5, pp. 877–892, May 2016.
19. Waggett, Peter. "Risk-based authentication: biometrics' brave new world." Biometric Technology Today 2016.6 (2016): 5-7.
20. N. Z. Gong, M. Payer, R. Moazzezi, and M. Frank, “Forgery-resistant touch-based authentication on mobile devices,” in Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security. ACM, 2016, pp. 499–510.
21. V. M. Patel, R. Chellappa, D. Chandra and B. Barbello, "Continuous User Authentication on Mobile Devices: Recent progress and remaining challenges," in IEEE Signal Processing Magazine, vol. 33, no. 4, pp. 49-61, July 2016.
22. Buriro, Attaullah et al. “Hold and Sign: A Novel Behavioral Biometrics for Smartphone User Authentication.” 2016 IEEE Security and Privacy Workshops (SPW) (2016): 276-285.
23. Saevanee, Hataichanok, et al. "Continuous user authentication using multi-modal biometrics." Computers & Security 53 (2015): 234-246.
24. Ye, Quanqi et al. “Formal Analysis of a Single Sign-On Protocol Implementation for Android.” 2015 20th International Conference on Engineering of Complex Computer Systems (ICECCS) (2015): 90-99.
25. J. Sedenka, S. Govindarajan, P. Gasti, and K. S. Balagani, “Secure outsourced biometric authentication with performance evaluation on smartphones,” Information Forensics and Security, IEEE Transactions on, vol. 10, no. 2, pp. 384–396, 2015.
26. Meng, Weizhi et al. “Surveying the Development of Biometric User Authentication on Mobile Phones.” IEEE Communications Surveys & Tutorials 17 (2015): 1268-1293.
27. T. Neal, D. Woodard, and A. Striegel, “Mobile device application, Bluetooth, and Wi-Fi usage data as behavioral biometric traits,” in Proc. IEEE Int. Conf. Biometrics Theory, Applicat. and Syst., Sept. 2015, pp. 1–6.
28. H. Zhang, V. M. Patel, and R. Chellappa, “Robust multimodal recognition via multitask multivariate low-rank representations,” in Proc. IEEE Int. Conf. Automatic Face and Gesture Recognition, May 2015, vol. 1, pp. 1–8.
29. Temper, Marlies et al. “Touch to Authenticate — Continuous Biometric Authentication on Mobile Devices.” 2015 1st International Conference on Software Security and Assurance (ICSSA) (2015): 30-35.

30. Murmuria, Rahul et al. “Continuous Authentication on Mobile Devices Using Power Consumption, Touch Gestures and Physical Movement of Users.” RAID (2015).
31. Hoang, Thang et al. “Gait authentication on mobile phone using biometric cryptosystem and fuzzy commitment scheme.” International Journal of Information Security 14 (2015): 549-560.
32. L. Fridman, S. Weber, R. Greenstadt, and M. Kam, “Active authentication on mobile devices via stylometry, GPS location, web browsing behavior, and application usage patterns,” IEEE Syst. J., 2015.
33. Lafkih, M., Lacharme, P., Rosenberger, C., Mikram, M., Ghouzali, S., El Haziti, M., Abdul, W. and Aboutajdine, D., 2015, November. Application of new alteration attack on biometric authentication systems. In Anti-Cybercrime (ICACC), 2015 First International Conference on (pp. 1-5). IEEE.
34. S. Alotaibi, S. Furnell and N. Clarke, "Transparent authentication systems for mobile device security: A review," 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), London, 2015, pp. 406-413.
35. Bakar, Khairul Azmi Abu, Nor Izyani Daud, and Mohd Shafeq Md Hasan. "ADAPTIVE AUTHENTICATION: A Case STUDY FOR UNIFIED AUTHENTICATION PLATFORM. (2015)"
36. H. Sun, K. Sun, Y. Wang, and J. Jing, "TrustOTP: Transforming Smartphones into Secure One-Time Password Tokens", 2015 ACM. ISBN 978-1-4503-3832-5/15/10
37. Jain, Rubal & Kant, Chander. Attacks on Biometric Systems: An Overview. International Journal of Advances in Scientific Research. 1. 283. 10.7439/ijasr.v1i7. 2015.
38. Aronowitz, Hagai, et al. "Multi-modal biometrics for mobile authentication." Biometrics (IJCB), 2014 IEEE International Joint Conference on. IEEE, 2014
39. Galbally, J., Marcel, S. and Fierrez, J., 2014. Image quality assessment for fake biometric detection: Application to iris, fingerprint, and face recognition. IEEE transactions on image processing, 23(2), pp.710-724.
40. Amin, Reham & Gaber, Tarek & Eltaweel, Ghada & Hassanien, Aboul Ella. (2014). Biometric and Traditional Mobile Authentication Techniques: Overviews and Open Issues. 10.1007/978-3-662-43616-5_16.
41. M. Tanviruzzaman and S. I. Ahamed, "Your Phone Knows You: Almost Transparent Authentication for Smartphones," 2014 IEEE 38th Annual Computer Software and Applications Conference, Vasteras, 2014, pp. 374-383.
42. "Bakar, Khairul Azmi Abu, and Galoh Rashidah Haron. ""Adaptive authentication based on analysis of user behavior."" Science and Information Conference (SAI), 2014. IEEE, 2014.
43. X. Zhao, T. Feng, and W. Shi, “Continuous mobile authentication using a novel graphic touch gesture feature,” in Proc. IEEE Int. Conf. Biometrics: Theory, Applicat. and Syst., Sept. 2013, pp. 1–6.
44. Feng, Tao, et al. "Continuous mobile authentication using virtual key typing biometrics." 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications. IEEE, 2013.

45. S. Indu, T. N. Sathya and V. Saravana Kumar, "A stand-alone and SMS-based approach for authentication using mobile phone," 2013 International Conference on Information Communication and Embedded Systems (ICICES), Chennai, 2013, pp. 140-145.
46. M. Frank, R. Biedert, E. Ma, I. Martinovic and D. Song, "Touchalytics: On the Applicability of Touchscreen Input as a Behavioral Biometric for Continuous Authentication," in *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 1, pp. 136-148, Jan. 2013.
47. H. M. Thang, V. Q. Viet, N. D. Thuc, and D. Choi, "Gait identification using accelerometer on mobile phone," in Proc. Int. Conf. Control, Automation and Inform. Sci., Nov. 2012, pp. 344–348.
48. C. Nickel, T. Wirtl, and C. Busch, "Authentication of smartphone users based on the way they walk using k-NN algorithm," in Proc. IIH-MSP, 2012, pp. 16–20.
49. Paul, S., Gupta, D. and Tiwari, A., 2012, September. Indexed search strategy for an automated biometric identification system. In Biometrics Special Interest Group (BIOSIG), 2012
50. F. Zhang, A. Kondoro, S. Muftic , "Location-Based Authentication and Authorization Using Smart Phones" ,TRUSTCOM '12 Proceedings of the 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications
51. S. Li and A. C. Kot, "An improved scheme for full fingerprint reconstruction," Information Forensics and Security, IEEE Transactions on, vol. 7, no. 6, pp. 1906–1912, 2012.
52. T. Feng, Z. Liu, K.-A. Kwon et al., "Continuous mobile authentication using touchscreen gestures," in Proceedings of the IEEE Conference on Technologies for Homeland Security (HST), pp. 451–456, IEEE, Waltham, MA, USA, November 2012
53. F. Juefei-Xu, C. Bhagavatula, A. Jaech, U. Prasad, and M. Savvides, "Gait-ID on the move: Pace independent human identification using cell phone accelerometer dynamics," in Proc. IEEE Int. Conf. Biometrics: Theory, Applicat. and Syst., Sept. 2012, pp. 8–15.
54. Carullo, Giuliana et al. "Towards Improving Usability of Authentication Systems Using Smartphones for Logical and Physical Resource Access in a Single Sign-On Environment." (2012).
55. V. Radhaa, D. Hitha Reddya, A Survey on Single Sign-On Techniques, aInstitute for Development and Research in Banking Technology,Road #1, Castle Hills, Masab Tank, Hyderabad – 500 067 (A.P), INDIA, 2012.
56. Corella, Francisco and Karen P. Lewison. "Strong and Convenient Multi-Factor Authentication on Mobile Devices." (2012).
57. K. Il Shin, J. S. Park, J. Y. Lee, and J. H. Park, "Design and Implementation of Improved Authentication System for Android Smartphone Users," pp. 2–5, 2012
58. H. Ketabdar, M. Roshandel, and D. Skripko, "Towards implicit enhancement of security and user authentication in mobile devices based on movement and audio analysis," in Proc. 4th Int. Conf. Advances in Comput.-Human

Interactions, 2011, pp. 188–191.

59. B. Cha, N. Kim, and J. Kim, "Prototype Analysis of OTP Key-generation based on Mobile Device using Voice Characteristics", 2011
60. Omelina, Ľ. and Oravec, M., 2011, June. Universal biometric evaluation system: Framework for testing evaluation and comparison of biometric methods. In Systems, Signals and Image Processing (IWSSIP), 2011 18th International Conference on (pp. 1-4). IEEE.
61. Delac, G., Silic, M. and Krolo, J., 2011, May. Emerging security threats for mobile platforms. In 2011 Proceedings of the 34th International Convention MIPRO (pp. 1468-1473). IEEE.
62. C. Nickel, C. Busch, S. Rangarajan, and M. Mobius, "Using Hidden Markov Models for accelerometer-based biometric gait recognition," in Proc. IEEE Int. Colloq. Signal Processing and Its Applicat., March 2011, pp. 58–63.
63. P. Tanvi, G. Sonal and S. M. Kumar, "Token Based Authentication Using Mobile Phone," 2011 International Conference on Communication Systems and Network Technologies, Katra, Jammu, 2011, pp. 85-88.
64. Maiorana, Emanuele et al. "Keystroke dynamics authentication for mobile phones." SAC (2011).
65. Li, Fudong et al. "Behaviour Profiling for Transparent Authentication for Mobile Devices." (2011).
66. M. Derawi, C. Nickel, P. Bours, and C. Busch, "Unobtrusive user-authentication on mobile phones using biometric gait recognition," in Proc. Int. Conf. Intelligent Inform. Hiding and Multimedia Signal Processing, Oct. 2010, pp. 306–311.
67. Aviv, Adam J., et al. "Smudge Attacks on Smartphone Touch Screens." *Woot* 10 (2010): 1-7.
68. A. Hadid, J. Heikkila, O. Silven, and M. Pietikainen, "Face and eye detection for person authentication in mobile phones," in Proc. ACM/IEEE Int. Conf. Distributed Smart Cameras, Sept. 2007, pp. 101–108.
69. P. Abeni, M. Baltatu, and R. D'Alessandro, "Nis03-4: Implementing biometrics-based authentication for mobile devices," in Proc. IEEE Global Telecommun. Conf., Nov. 2006, pp. 1–5.
70. J. Mantyjarvi, M. Lindholm, E. Vildjiounaite, S. M. Makela, and H. Ailisto, "Identifying users of portable devices from gait pattern with accelerometers," in Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing, March 2005, vol. 2, pp. ii/973–ii/976.
71. P. A. Viola and M. J. Jones, "Robust real-time face detection," Int. J. Comput, Vision, vol. 57, no. 2, pp. 137–154, 2004.
72. T. Ojala, M. Pietikainen, and T. Maenpaa, "Multiresolution gray-scale and rotation invariant texture classification with local binary patterns," IEEE Trans. Pattern Anal. and Mach. Intell., vol. 24, no. 7, pp. 971–987, 2002.
73. E. Bertino, C. Bettini, E. Ferrari, and P. Samarati, "An access control model supporting periodicity constraints and temporal reasoning," ACM Transactions on Database Systems, vol. 23, no. 3, pp. 231–285, 1998.
74. Auth0.com, "Common Threats and How to Prevent Them" [Online]. Available: "https://auth0.com/docs/security/common-threats#replay-attacks" [Accessed: 23- March- 2019]

75. Protectimus.com “Hardware Or Software Token- Which One to Choose?” [Online]. Available:“https://www.protectimus.com/blog/hardware-or-software-token-which-one-to-choose/” [Accessed: 21- March- 2019]
76. Wang, Xuan, and Jiro Tanaka. "GesID: 3D Gesture Authentication Based on Depth Camera and One-Class Classification." Sensors 18.10 (2018): 3265.
77. Serwadda, Abdul, et al. "Toward robotic robbery on the touch screen." ACM Transactions on Information and System Security (TISSEC) 18.4 (2016): 14.