International Journal of Engineering Trends and Technology
ISSN: 2231 – 5381 /doi:10.14445/22315381/IJETT-V69I1P211
Volume 69 Issue 1, 74-80, January 2021

Digital Authentication Methodologies for Mobile Devices

Jyothy Joseph[1], Dr.K Nirmala[2]

[1]*Research Scholar, Dept of Computer Science, University of Madras, Quaid-E-Millath Government College for Women (Autonomous)Chennai, Tamil Nadu, India.*

[2]*Associate Professor, Department of Computer Science, University of Madras, Quaid-E-Millath Government College for Women (Autonomous)Chennai, Tamil Nadu, India.*

[1]jyothyjoseph@gmail.com, [2]nimmimca@yahoo.co.in

Abstract *— In the android mobile ecosphere, data loss and financial loss are the two potential threats facing the current epoch. Both threats have multiple subdivisions and impacts many of the mobile users and organizations. Many users are passionate and thrilled to use various new features introduced by various mobile companies and applications. Without properly evaluating the security capabilities and vulnerabilities, many of them use the various extensive features available in the system. By default, all the devices and applications have different levels of built-in security features, but many of them do not utilize this appropriately or are not aware of these in the right sense. This study has attempted to list the various secured authentication features available in different layers and the type of protection that enables these features. Here, the analyses chart security features in hierarchical order starting from device-level security and then moves on to the application level security and finally fragments itself into an activity or transaction level of security features.*

Keywords *— Device Level Authentication, Application Level Authentication, Transaction Level Authentication, Biometric Authentication, Multi-Factor Authentication*

I. INTRODUCTION

Authentication is the process of validating the user's arguments against what they claim about who they are. It is a process to validate a user's individuality and identity-based on the information/ credential that the user knows or has. Digital Authentication is a deal between a human and machine, wherein the machine explores the digital authentication methodologies to validate the human's identity. With the passage of time and the development of technology, new authentication mechanisms are introduced, and few existing options get obsolete. As mobile devices migrated from feature devices to smart devices, digital Authentication became sensational as the user always prefers a simplified and secured authentication. When the authentication mechanism becomes complicated, users start to overlook or ignore the Authentication, which brings about vulnerabilities. Nowadays, many users rely on their mobile devices for their professional activities and daily routine activities. Nowadays, mobile devices contain varying degrees of personal and secured information such that it is possible even to get the horoscope details about an individual. Consequently, the secured authentication mechanism is a mandatory and inevitable measure for a smart mobile device. This study explains the evaluation of authentication methodologies from traditional to digital and how to authenticate and authorize a user for an activity or a transaction. Modern-day users prefer mobile devices as it enables them anytime anywhere mobile computing, which provides convenience to the user. Subsequently, the authentication process has become more challenging because the users prefer a more convenient and easier authentication mechanism and do not want to carry complicated credentials or follow complex authentication processes. There are multiple levels of mobile device authentications available; these levels are deployed depending on various users' usage intensity.

II. RESEARCH METHODOLOGY

The below figure (Fig.1) explains the methodology followed in this study. First, we look into the different Authentication levels available for mobile devices, followed by a detailed analysis or retrospection into the various Authentication methods. And at the end, we conclude our study by understanding how effectively we can utilize each of these methods. Each of these analyses is covered in the following sections

Fig.1. Research Methodology

III. AUTHENTICATION LEVELS

Authentication happens at different hierarchical levels. Each level deploys a different type of security measure. Mainly there are three hierarchical levels as listed below:

1. Device-level authentication
2. App-level authentication
3. Activity level authentication

A. Device Level Authentication

Device-level authentication is the first step to get inside the device. It utilizes the different options which are pre-equipped on the device. Android OS itself has multiple options, and the features vary depending on the OS versions. Mainly there are three types of device-level authentications, namely:

1. Traditional Methods
2. Biometric Methods
3. Smart Methods

a) Traditional Methods

Traditional methods cover the commonly used device locking features. These methods are very simple to use; hence, most users prefer to utilize these options. Below are the key traditional methods:

- **Swipe**: This is the simplest phone locking method; it is a commonly used technique to avoid accessing the device by mistake. Below figure (Fig-2) visualizes the swipe option.

- **Pattern**: The pattern option provides some structured line patterns to store and use the same to unlock the device. Below figure (Fig-3) shows its visualization.

- **PIN**: This option provides a feature to save a secret number and use the same for unlocking the device. Below figure (Fig-4) shows its visualization.

- **Password**: This option provides the user to set and save a password to access the device and use the same for unlocking the device. Below figure (Fig-5) shows its visualization

Fig-2 Swipe

Fig-3 Pattern

Fig-4 PIN

Fig-5 Password

b) Biometric Methods

Biometric metric methods enable the user's biometric identities to enable mobile device access. This feature offers an identity assurance than any other methodologies, and the mechanism is very easy to set up and use. Fraudulent practices or usage would be comparatively lesser with this feature enabled.

- **Facial Recognition**: This option provides a facility to identify the device user based on face recognition. Here the system stores the different attributes of the user's face and validates against other users. This feature is comparatively less secure as high-quality photos or a person with facial features similar to the real user can unlock the device.

Fig-6 Facial Recognition

- **Voice Recognition:** Here, the system captures the user's different voices, and it creates a unique voice template for that particular user. When the user speaks to the device, it compares and identifies the actual user based on the voice patterns.

- **Retina & Iris Scanning:** This mechanism emits light to the eye and captures its irregularity and uniqueness based on the color surrounding the eye's pupil. This color uniqueness always differs from person to person.

Fig-7 Voice Recognition

Fig-8 Retina & Iris Scanning

- **Fingerprint Sensing:** Fingerprint sensing mechanism has had a huge growth in mobile device user experience. Here the system stores different dimensions of the user's fingerprint, and it proceeds to validate the user's identity to grant access to the device. The different types of fingerprint sensing used in mobile devices areas listed below:

    - Capacitive
    - Optical
    - Ultrasonic

Fig-9 Fingerprint Sensing

c) Smart Methods

Android devices provide various smart lock & unlock device features. There is an instance of security compromise to this situation, which is up to the user to decide based on the convenience aspect. By convenience, there is a trade-off in the security features as this feature is enabled based on user confidence. It provides quick access to the device based on some trusted feature considerations that are to be specially taken into note during one-off situations. Except for the enabled few trusted scenarios, the rest of the situations enables another security mechanism. Android provides multiple smart lock features (Fig-10); all those features might not be available on all android devices.

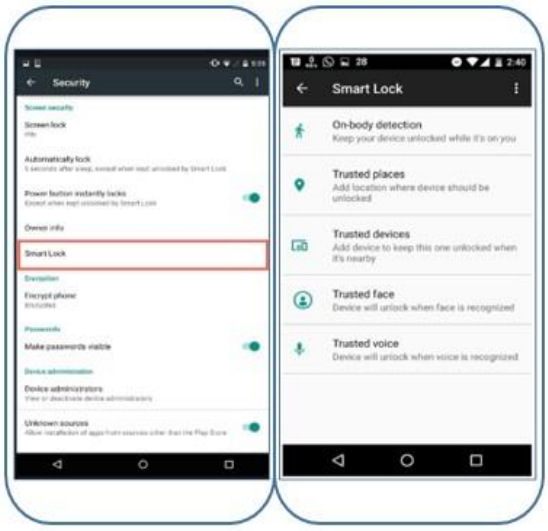

Fig-10 Smart Methods

- **On-body Detection:** This feature helps keep the device unlocked when the user holds the device in hand or is kept in pocket\handbag. It is enabled with the help of an accelerometer sensor. This feature support is devised to avoid frequent device unlock difficulties when the user holds the device. The main caveat of this feature is that when the user gives the device to someone else in unlocked mode, it will stay the same state until it is manually locked. Fig-11 shows the option to enable this feature.
- **Trusted Places:** This feature helps to keep the device unlocked when the user is in trusted places. It helps the user keep the device unlocked in trusted geographic locations like home, work, or user-confident places. This feature works with the help of a GPS component in the device. Fig-12 shows the option to enable this feature.
- **Trusted Devices:** This feature helps to keep the device unlocked when the user has connected any trusted devices with the phone. Trusted devices might be a car speaker, headphones, key tag, smartwatch, fitness equipment, etc. Once the user adds the external device to the trusted device list, this feature would help the user keep the phone unlocked. Fig-13 shows the option to enable this feature.
- **Trusted Face:** This feature is one of the most convenient and the least secure. The device owner can use trusted faces to unlock the device. When the user holds the device in front of his face, it will unlock automatically if the user has added his face as a trusted face. The system uses the device camera to recognize the user and enable the feature. Fig-14 shows the option to enable this feature.
- **Trusted Voice:** This feature helps the user to unlock the device based on the user's voice. When this feature is enabled, it captures the user's unique voice intonation

and validates against the same before unlocking the device. Fig-15 shows the option to enable this feature.

Fig-11 On-body detection

Fig-12 Trusted Places

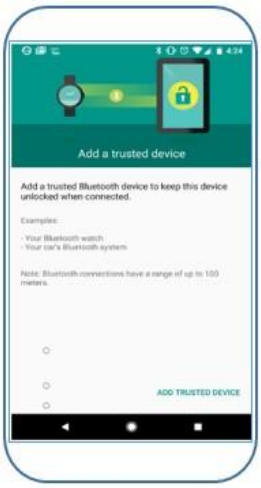

Fig-13 Trusted device

Fig-14 Trusted face

Fig-15 Trusted voice

B. App Level Authentication

Users always set up and enter the device with device-level authentication and then open the applications with app-level authentication. There are multiple types of app-level authentication, and depending on the application criticality, various methodologies are implemented. Below are the key app-level authentication methodologies

1. Single Factor Authentication
2. Multi-Factor Authentication
3. Continuous Authentication
4. Periodic Authentication
5. Background Authentication

a) Single Factor Authentication: Whenever any application is opened, it asks for basic authentication to access the application. Below are the commonly used authentication features, and any one of these features will trigger to ensure user validity.

- **Integrated Login:** Nowadays, many mobile apps provide integrated login options with popular user accounts like Google, Facebook, Microsoft, Line, etc. This functionality is normally available in the first interface of the application itself. One sample integrated login image is given in Fig-16

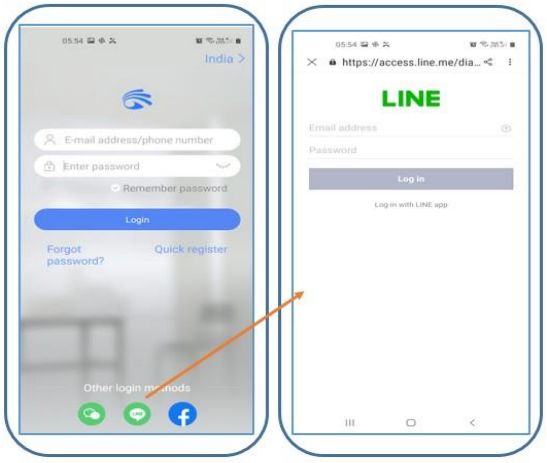

Fig-16 User ID/Password Authentication

- **User ID/Password:** This is one of the traditional authentication methods used in many places. Here the user validation is done with a username and Password. In most of the scenarios, the user name would be a unique name\ID\number, and the Password would be a secret alphanumeric value. A sample of app-level authentication image given in Fig-17

- **PIN:** Personal Identification Number (PIN) is a commonly used device unlock method (Fig-4). It is also used for application authentication as well. In various cases, the device PIN itself is considered an application-level PIN. The below image (Fig-18) shows PIN-based Authentication for a banking app.

- **Pattern:** Pattern is another commonly used device unlock method (Fig-3). This, too, can also be used for application authentication. The device pattern itself can be considered as an application-level pattern. Many of the applications provide access to add new and unique patterns specifically for each application. The below

image (Fig-18) shows a pattern-based authentication for a social media app.

- **Biometric:** Fingerprint biometric is also a commonly used application biometric authentication method. Facial recognition, IRIS recognition, and voice recognition are some of the biometric app authentication methods. Most of the financial and banking apps use fingerprint-based app-level verification. The below image (Fig-20) shows pattern-based Authentication for a social media app.

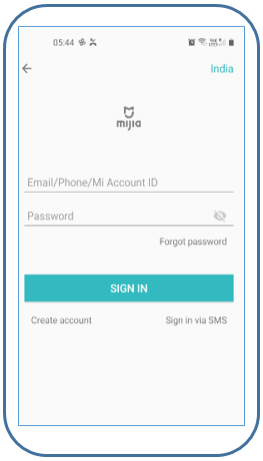

Fig-17 User ID/password

Fig-18 PIN Authentication

Fig-19 Pattern Authentication

Fig-20 Biometric Authentication

b) Multi-Factor Authentication: Multi-factor authentication (MFA) is a highly secured user authentication option, which considers two or more authentication factors to verify a user's genuineness. Currently, many mobile applications have enabled two-factor Authentication. However, this is majorly enabled in web-based applications rather than two factors enabled mobile apps. Nowadays, there are different multi authentication apps available like Google Authenticator, Microsoft Authenticator, Secure AUTH, etc.

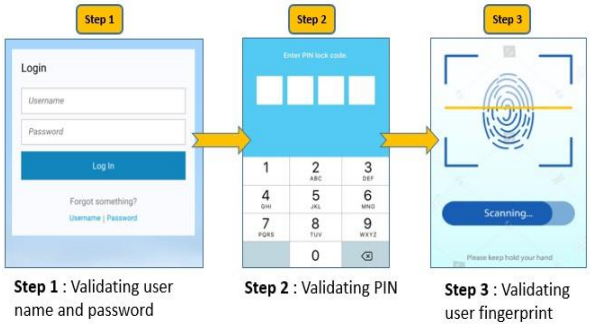

Fig-21 Multi-factor Authentication

c) Continuous Authentication: This type of Authentication is relatively a new authentication method. Here the system continuously measures the user's genuineness and controls user access. This feature functioning is based on AI support. The system continuously collects user information and validates user actions and behaviors like physical movement, finger pressure, user voice, key management patterns, facial validation, etc. If any misbehavior is noticed in between, the system validates the user authenticity again.

Fig-22 Continuous Authentication

d) Periodic Authentication: This method is very similar to the continuous authentication method, but user authentication is done at certain predefined intervals.

***e) Background Authentication*:** In this method, the application validates the user at the initial stage. A next level validation is enabled in the background and triggered without user intervention, and this can be either a hardware authentication or behavioral Authentication.

C. Activity Level Authentication

Activity level authentication enables transaction-level security. Nowadays, most financial applications like banking apps, e-commerce apps, money transaction apps, etc., use this type of feature. This feature is triggered when any money transaction/ transfer is

initiated. The image below (Fig-23) shows activity level authentication for a banking app.

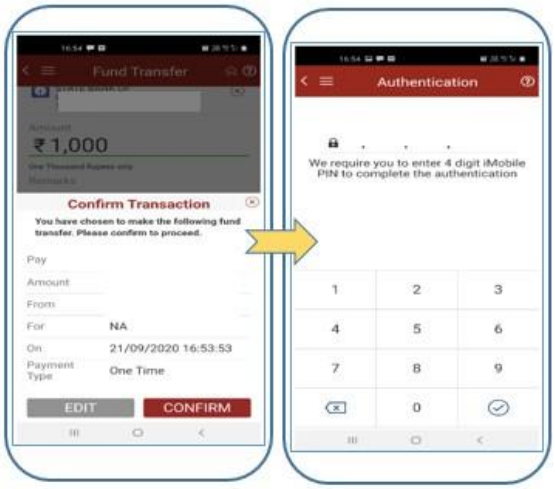

Fig-23 Activity level authentication

In the image shown here, the application has enabled PIN-based Authentication. Similarly, various types of authentication options can be enabled at the activity level. Below are the commonly used activity level authentication options. Few of them are reused in the device level or application level securities.

a) PIN-based Authentication: PIN-based Authentication asks the user to enter personal identification (PIN) before triggering the activity.

b) Password-based Authentication: Password-based authentication password is requested before triggering the activity.

c) OTP based Authentication: One-time Password (OTP) authentication asks the user to enter OTP details shared to the user registered mobile or email ID before triggering the activity.

d) Biometric-based Authentication: Biometric authentication probes the user to validate biometric details like fingerprint or IRIS before triggering the activity. Facial recognition or voice recognition is not secure enough for critical transactions, so normally these are not recommended for activity level authentication.

e) History based Authentication: This type of Authentication validates the user's previous transaction details to trigger the next transactions.

***f) Alternate Device Authentication*:** This type of Authentication sends out a notification to the same user's secondary registered device, and the user is supposed to accept the same on the other device.

g) AI-based Authentication: AI-based Authentication validates the user's current behavior with previous activities and behaviors. The system triggers a list of questions and validates the user responses.

IV. RESULT AND FINDINGS

Combined device-level security, application-level security, and activity level security can prevent a certain level of mobile-based cyber-attacks. Currently, most of the applications provide both app-level and transaction-level securities. Always ensure utilizing these features and avoid any application if these security attributes are not provided. Let's take a classic example of a widely used and popular financial app- Google Pay, which enforces three security levels. The first step is to log in to the device with a security measure, as shown in Fig-24 (the device login with a PIN). The user then logs in to the application using a fingerprint biometric feature (Fig-25). A financial transaction is made only after entering a UPI PIN(Fig-26). As such, all three levels of security are implemented here.

Fig - 24 Device-level Authentication

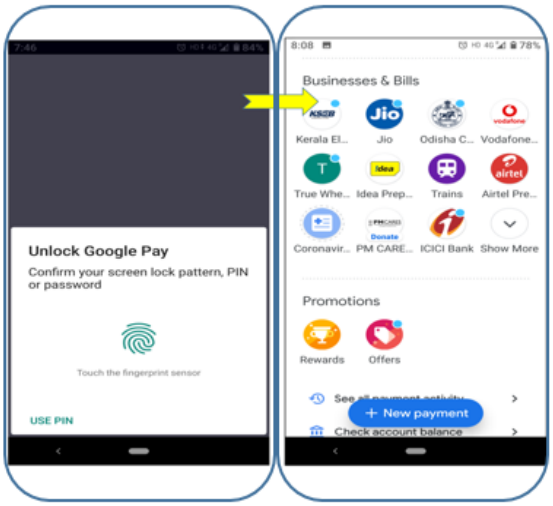

Fig - 25 App-level Authentication

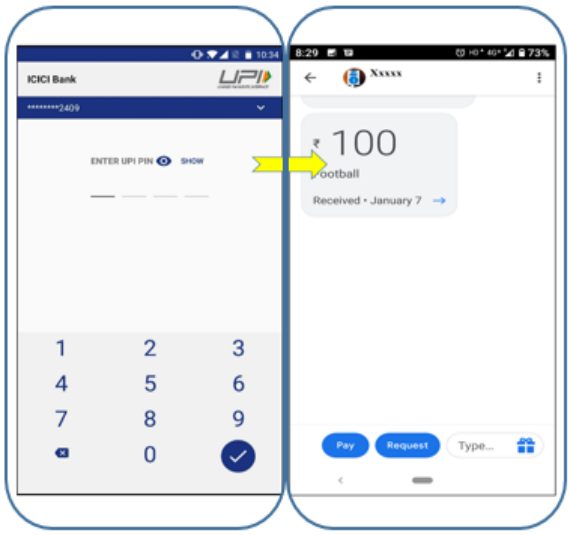

Fig - 26 Activity level Authentication

V. CONCLUSION

Data level security and financial transaction-level security are the two basic safety expectations from a mobile device. This study walks through the various features that can be opted on a device level, application level, and activity level. With time and new technological developments, the mobile ecosystem incorporates the latest security features to prevent newly identified vulnerabilities. Understanding the available security features and enabling these in the right place is an essential task that cannot be compromised during mobile usage. This analysis helps to understand the various security features available in the mobile security ecosystem. Prevention is better than cure, so enable the right and apt security feature to prevent mobile-based threats and thereby avoid the consequences.

References

[1] Sandeep Gupta, Attaullah Buriro, and Bruno Crispo (2018) [Ways and Types to Secure Access] https://www.hindawi.com/journals/misy/2018/2649598/

[2] Abdulaziz Alzubaidi and Jugal Kalita (2019) [Authentication of Smartphone Users Using Behavioral Biometrics] https://arxiv.org/pdf/1911.04104.pdf

[3] Oriana Riva, Chuan Qin, Karin Strauss, and Dimitrios Lymberopoulos (2012) [Progressive authentication] https://homes.cs.washington.edu/~kstrauss/publications/pa.pdf

[4] Matthew Haughn and Margaret Rose (2014) [Mobile authentication] https://searchsecurity.techtarget.com/definition/mobile-authentication

[5] John Powers (2019) [Authentication with modern methods] https://searchmobilecomputing.techtarget.com/feature/Tackle-mobile-device-authentication-with-modern-methods

[6] Secure Technology Alliance Mobile Council (2017) [Mobile Identity Authentication] https://www.securetechalliance.org/wp-content/uploads/Mobile-Identity-Authentication-WP-FINAL-March-2017.pdf

[7] Jim Haviland (2019) [Existing authentication options] https://insights.samsung.com/2019/09/06/which-authentication-method-is-best-for-your-business-phones/

[8] National Cyber Security Center UK (2020) [Mobile Device Guidance] https://www.ncsc.gov.uk/collection/mobile-device-guidance/enterprise-authentication-policy

[9] Robert Triggs [Two factor authentication] (2019) https://www.androidauthority.com/two-factor-authentication-explained-971653/

[10] Alice MJ (2020) [Screen lock] https://drfone.wondershare.com/unlock/android-lock-screen-settings.html

[11] Merry Marwig (2020) [Password less Authentication] https://research.g2.com/insights/guide-to-passwordless-authentication

[12] Android Central (2018) [Smart Lock] https://www.androidcentral.com/smart-lock

[13] Simon Hill (2018) [Smart Lock Working] https://www.digitaltrends.com/mobile/how-to-use-android-smart-lock/

[14] Dean Nicolls (2019) [Biometric Authentication] https://www.jumio.com/what-is-biometric-authentication/

[15] OneSpan (2020) [Multi Factor Authentication] https://www.onespan.com/topics/multi-factor-authentication.