Continuing Education Program
Center for Computing and Information Technology
Fakultas Teknik Universitas Indonesia

Information Search and Analysis Skills

(ISAS)

The Implementation of Fingerprint Security for iOS

Developed by:

1. Christian Frans Mukuan / 1920010040
2. Deyaninta Ekabriela Permata / 1920010050

Faculty: Mr. Fachran Nazarullah, S.Kom

Class: 4SC3

Gedung Engineering Center Fakultas Tenik Universitas Indonesia
Kampus Baru UI Depok 16424

June, 2021

PREFACE

In the name of ALLAH SWT. Whose gave his grant to the writer so that the project of could be finished. In part of, the writer would like to express his thanks for those take a part directly or indirectly to setting up the project.

This paper contains a comparison of matter specifically discuss about Fingerprint Security for iPhone. The paper is expected to provide information to us all about understanding the implementation of fingerprint security for iPhone.

We realize that this paper is far from perfect, therefore, criticism and suggestions from all parties that we always expect to be building for the perfection of this paper.

Finally, we extend our thanks to all those who have participated in the preparation of this paper from start to finish.

Depok, June 2021

(Authors)

Table of Contents

TABLE OF FIGURE

CHAPTER I

INTRODUCTION

I. PROBLEM BACKGROUND

Modern biometric technology began in the 1960s, evolving into high-tech scanners that read bio-markers with an accuracy touching 100%. In 2020, biology-based science is disrupting the authentication industry at speed. The future is now passwordless.

It's important to understand how fingerprint login and other biometric systems work, before we use them. A biometric is a unique biological characteristic which can be used to identify and verify a person's identity. Apart from fingerprints, we see this in facial recognition scans, DNA tests, and less commonly in palm prints, and iris and retina recognition.

Fingerprint security systems are a good option for companies to put into place because they tend to be difficult to hack, as there is not a password or any sort of data to input. Rather, fingerprint security systems utilize biometric technology.

Biometric access control is a system that prevents intruders from accessing certain areas or resources by verifying them as unauthorized persons. Biometric authentication refers to the recognition of individuals by certain physical uniqueness, such as a fingerprint. Access control biometric fingerprint readers scan a person and match his or her biometric data with what is previously stored in the database. If the information matches, the individual can access the secured area or resources. Today, biometric access control systems are among the most secure authentication systems.

It's much harder to fake a physical attribute like a fingerprint than it is to fake an identity card, thus fingerprint security systems are arguably more secure. On a similar note, it's impossible to guess a fingerprint pattern in the same way that an intruder or unwanted person could try to guess a code. Finally, individuals can't misplace or forget a fingerprint in the same way that one might lose their security card or forget the passcode numbers.

Human fingerprints are detailed, nearly unique, difficult to alter, and durable over the life of an individual, making them suitable as long-term markers of human identity. In this era,

almost all people use smartphone in their daily life. And smartphone is considered as something that is very important to some people because smartphone can do so many tasks, like communicate with other people using social media, save file, do some transaction, etc. Because of that, security is very needed in smartphone. Some of the smartphone security systems are pin, password, pattern, fingerprint security system, etc.

I.2 Problem Domain

In this ISAS, we would like to discuss about fingerprint security system in iPhone, as we called Touch Id.

I.3 Writing Objective

The author's purpose in writing Information Search and Analysis Skill (ISAS), among others:

1. To know what is Fingerprint Security.
2. To know what is Touch Id.
3. To know technology behind Touch Id.
4. To know the security safeguards on Touch Id.
5. To know how to set up touch Id.
6. To know the advantages and disadvantages of using Fingerprint Security.

I.4 Writing Methodology

The authors uses the method of library research (literature), which the authors find books and gathers information related to the discussion of the Information Search and Analysis Skill (ISAS), which will be added to the opinion of the writer or thought. The authors will not forget to write the name of the books or journals and articles used in the process of making Information Search and Analysis Skill (ISAS).

I.5 Writing Framework

In this Information Search and Analysis Skill (ISAS), the authors compiled systematic writing in 4 (four) chapters. Each chapter will try to describe the parts of the problem that embodies a theory in this Information Search and Analysis Skill (ISAS). For more details, description chapters are organized as follows:

CHAPTER I INTRODUCTION

This chapter contains an explanation of the background of the title selection, problem domain, writing objective, writing methodology, writing framework. Description:

CHAPTER I INTRODUCTION

I.1. Problem Background

I.2. Problem Domain

I.3. Writing Objective

I.4. Writing Methodology

I.5. Writing Framework

CHAPTER II BASIC THEORY

In this chapter the author discusses the basic theory of the topic.

CHAPTER III THEORITICAL DISCUSSION

In this chapter the author analyzes the problem related to the topic.

CHAPTER IV CLOSING

This chapter is the conclusion of the writing Information Search and Analysis Skill (ISAS) and advice from the author to all readers.

CHAPTER II

BASIC THEORY

II.1 Introduction of Fingerprint

A fingerprint is an impression left by the friction ridges of a human finger. The recovery of partial fingerprints from a crime scene is an important method of forensic science. Moisture and grease on a finger result in fingerprints on surfaces such as glass or metal. Deliberate impressions of entire fingerprints can be obtained by ink or other substances transferred from the peaks of friction ridges on the skin to a smooth surface such as paper. Fingerprint records normally contain impressions from the pad on the last joint of fingers and thumbs, though fingerprint cards also typically record portions of lower joint areas of the fingers. (Fingerprint, 2021)

II.2 Definition of Fingerprint Security System

Human fingerprints are practically unique, which is why they're successful at identifying individuals. It's not just law enforcement agencies that collect and maintain databases of fingerprints. Many types of occupations that require professional licensing or certification (e.g. financial advisors, stockbrokers, real estate agents, teachers, doctors/nurses, security, contractors, etc.) mandate fingerprinting as a condition of employment. It's also typical to provide fingerprints when having documents notarized.

Advancements in technology have been able to incorporate fingerprint scanners (can also be referred to as 'readers' or 'sensors') as another (optional) security feature for mobile devices. Fingerprint scanners are one of the latest in an ever-growing list—pin codes, pattern codes, passwords, face recognition, location detection, iris scanning, voice recognition, trusted Bluetooth or NFC connection—of ways to lock and unlock smartphones. Why use a fingerprint scanner? Many enjoy it for the security, convenience, and futuristic feel.

II.3 The Types of Fingerprint Security

a. Optical Fingerprint

Optical fingerprint scanners are the oldest to come by of capturing the fingerprints and then comparing them. Firstly, an image is captured as in a photograph,

unique algorithms are then used to detect patterns on the finger's surface to mark off any marks and ridges. This is done by differentiating the dark and light areas of the captured image. The sensors are designed to have a specific resolution. If the resolution is higher, the sensor can capture finer details of your finger. They essentially capture a two-dimensional picture. The Suprema Realscan G10 is a portable scanner that employs advanced optical technology to capture the patterns and ridges in dry and wet fingers.

b. Capacitive Scanners

This technology is commonly found in scanners these days. This technology uses many arrays of small capacitor circuits to collect differentiating data about fingerprints. Capacitors can store charge and therefore if they are connected to conducting plates on the surface, they and track the fingerprint details. The presence of an air gap will not bring about any change in the stored charge. The changes are tracked using an op-amp integrator which is further converted using an analog-to-digital converter. The data can be saved for later comparisons. For higher resolution pictures, more capacitors must be connected.

c. Ultrasonic Scanners

This is the latest technology to be used in fingerprint scanners. The hardware used in these scanners consists of an ultrasonic transmitter and a receiver. An ultrasonic pulse is transmitted against the finger placed on the scanner panel. Whereas some of it is absorbed, the rest is echoed back. This is dependent on the valleys, ridges, pores and other marks found on the finger. These are unique to every finger.

The mechanical stress measured by a sensor is used to calculate the intensity of the reflected ultrasonic pulse. This happens at different points on the scanner. If the time period of scanning is longer, the depth of data that is captured is more and enables a 3D rendering of the surface. (Different Types of Fingerprint - Optical, Capacitive, and Ultrasonic, 2017)

II.4 The Benefits of using Fingerprints

a. Two Fingers Cannot Be Same

Patterns formed by dermal ridges results in the formation of fingerprints. It takes shape during fetal development. You can find these lines on palms, fingers, toes and soles. The ridge pattern is unique for every individual. Even twins cannot have the same

fingerprints. This pattern on fingers does not change with age, physical growth or any disease. This feature makes it a secured device for authentication.

b. Requires Less Storage Space:

Storage requirement per capita generally increases. Most of the file formats require large storage amount. But it takes very less storage space to store the templates of fingerprints. It is difficult to carry ID and access cards in your wallet. But with a fingerprint system, you can store thousands of biometric templates in tiny space. Most of the products nowadays use fingerprint scanning technology.

c. Quick and Easy to Use:

It is time-consuming and frustrating to pull out the card from the wallet every time for verification. There are also cases when you can be granted or denied access. No one would want to face such a doubtful scenario when you are already rushing for boarding a flight or appointment. A casual fingerprint scan saves lots of time.

You do not need any special training for using fingerprint scanning device. It is a one-time process to enroll in it and you can start using the fingerprint authentication instantly.

d. Audit Trail-Clear and Definable:

Fingerprint authentication is a reliable source that creates a clear and definable audit trail. This is possible because the user presents fingerprints for a live scan. But there are higher chances of manipulation and forgery in the audit trails based on passwords and user ID.

e. Privacy is Ensured:

The threat to our personal information is increasing with rapidly increasing digitalization. Anyone can easily retrieve our information. You might have noticed, that every time you visit a website, you click on the accept button and agree to their policies. In this way, the bulk of the information is saved on their systems. Fingerprint authentication can provide a good solution to the privacy issue.

Companies like IBM and SecureKey are working on an innovative solution. Central repositories such as credit agencies and banks will send notification alert to the users if any service provider asks for their personal details. Users can utilize a fingerprint authentication system to enable the sharing of personal information.

f. Cost of Maintenance is Low:

If you maintain the fingerprint scanner properly, it can keep your data secure for years. You can easily clean the surface of the scanner without using any special

equipment. Scratches and smudges can deplete the quality of scanning. It must be installed away from adverse conditions to ensure proper working.

Mentioned above are some of the benefits of Fingerprint Scanning Technology. These scanning devices are portable, easy to maintain, save your time, and ensure your privacy. You can visit Don’t pay all to get offers from various retailers to get scanning devices at discounted prices. (Benefits of Fingerprint Scanning Security, 2019)

CHAPTER III

ANALYSIS ISSUES

III.1 Definition of Touch ID

Figure 1

(https://macpoin.com/12239/seperti-ini-cara-menggunakan-touch-id/)

Touch ID is a fingerprint reader on newer iPhone devices that enables users to quickly sign in to their device as well as authorize transactions without needing to enter a passcode.

Apple's Touch ID "fingerprint identity sensor," as the company calls it, uses capacitive touch technology to detect a user's fingerprint, and then uses the authorization to efficiently unlock the user's smartphone, tablet or notebook; purchase apps or other digital content within iTunes and other Apple digital media stores; authenticate Apple Pay purchases or in-app purchases and more.

III.2 The Technology behind Touch ID

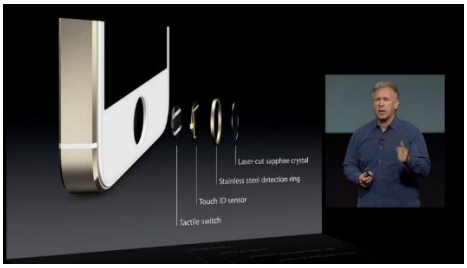

Figure 2

(https://www.imore.com/how-touch-id-works)

A sensor sits beneath the sapphire crystal home button or power button, depending on the Touch ID device you have, and the home button or power button double as a lens, allowing the sensor to focus on your fingerprint.

The sensor uses advanced capacitive touch to capture high-resolution images of your fingerprint. Touch ID reads fingerprints in 360-degrees of orientation, analyses the sub epidermal layers of the skin and categorizes each fingerprint into arch, loop or whorl categories.

Touch ID then maps individual details of fingerprint ridges, including variations like pores, and compiles all of the data together. Touch ID then uses this data to match and recognise fingerprints. (Tilman, 2020)

III.3 Security Safeguard on Touch ID

Every fingerprint is unique, so it's rare that even a small section of two separate fingerprints are alike enough to register as a match for Touch ID. The probability of this happening is 1 in 50,000 with a single, enrolled finger. And Touch ID allows only five unsuccessful fingerprint match attempts before you must enter your password. By comparison, the odds of guessing a typical 4-digit passcode are 1 in 10,000. Although some codes, like "1234," might be more easily guessed, there is no such thing as an easily guessable fingerprint pattern.

To start using Touch ID, you must first set up a passcode on your iPhone. You must enter your passcode or password for additional security validation:

- after you restart your iPhone, iPad, or Mac;
- when more than 48 hours have passed from the last time you unlocked your device;
- to add or delete a fingerprint to use with Touch ID;
- to change the iPhone or iPad passcode or Mac system password, and for other security settings like FileVault on your Mac;
- when there have been more than five unrecognized Touch ID authorization attempts in a row; and
- after you log out of your Mac.

If your device is lost or stolen, you can prevent Touch ID from being used to unlock your device with Find My iPhone Lost Mode. Starting with iOS 7, your iPhone and iPad offer additional protection against theft with Activation Lock, which requires an Apple ID and

password to turn off Find My iPhone, erase data, or reactivate your device. If your MacBook Pro with Touch ID is lost or stolen, erasing your Mac remotely also disables Touch ID. You can also use Touch ID to purchase content from the iTunes Store, App Store, and iBooks Store, instead of entering your Apple ID password.

Touch ID can be used by multiple users on a MacBook Pro, making it easy to share a system securely. Each user account can have up to three enrolled fingerprints, and a total of five fingerprints can be enrolled across the system. (About Touch ID advanced security technology, 2017)

III.4 How to Set Up Touch ID

Before you can set up Touch ID, you need to create a passcode for your device.* Then follow these steps:

1. Make sure that the Touch ID sensor and your finger are clean and dry.
2. Tap Settings > Touch ID & Passcode, then enter your passcode.
3. Tap Add a Fingerprint and hold your device as you normally would when touching the Touch ID sensor.
4. Touch the Touch ID sensor with your finger—but don't press. Hold it there until you feel a quick vibration, or until you're asked to lift your finger.

Figure 3

(https://support.apple.com/en-us/HT201371)

5. Continue to lift and rest your finger slowly, making small adjustments to the position of your finger each time.
6. The next screen asks you to adjust your grip. Hold your device as you normally would when unlocking it, and touch the Touch ID sensor with the outer areas of your fingertip, instead of the center portion that you scanned first. (Use Touch ID on iPhone and iPad, 2020)

Figure 4

(https://support.apple.com/en-us/HT201371)

III.5 Advantages and Disadvantages of using Fingerprint Security

Advantages :

- Secure, it means there is a security improvement more than just a password or even identity card. Fingerprints are much harder to fake, they also change very little over a lifetime, so the data remains current for much longer than photos and passwords.
- Ease of use, as a user you don't need to remember your password or cannot open your devices due to forgetting your lock screen pattern in house or something. You just need to put your finger on the fingerprint readers.
- Non-transferrable, by using password or any pattern you can just share it to your friend if you want to. But by using this, it means they need more effort since you need to put your own finger to unlock the devices. It provides more security against the theft or sensitive materials.

Disadvantages

- System failures, this security really depends on one part. It is the fingerprint scanner. Like the other electronic identification systems, there are same technical failures and limitations. Such as power outages, errors and environmental factors.
- Cost, Fingerprint Recognition System are cost more than the other security. But this disadvantage can be lesser as the devices become more cost effective and affordable for the users.
- User Exclusions, it is kinda hard to explain. As an example older people with a history of manual work may struggle to register worn prints into a system or people who have suffered the loss of fingers or hands would be excluded.

CHAPTER IV

CONCLUSION and SUGGESTION

IV.1 Conclusion

For security propose fingerprint place an important role in human recognition from past years and biometric system only be present at the recent years. The combined protection of your physical or behavioral signatures with other authentications gives some of the strongest known security. Until now, this kind of security can be concluded better than a character-based password as a standalone verification.

IV.2 Suggestion

As we have observed that Touch ID is an automated system to identify a person in real time and the no of chances to grant false access is less in this system as it works on the physical or biological characteristics of a person that remains with him or her. For us, it is better to use because Touch ID is more quickly and easier than face recognition.

REFERENCES

About Touch ID advanced security technology. (2017, September 11). Retrieved from Apple: https://support.apple.com/en-us/HT204587

Benefits of Fingerprint Scanning Security. (2019, September 10). Retrieved from Glaad Blog: https://www.glaadblog.org/7-benefits-of-fingerprint-scanning-security/

Different Types of Fingerprint - Optical, Capacitive, and Ultrasonic. (2017). Retrieved from AutoID System: https://autoidindia.com/different-types-of-fingerprint-scanners-optical-capacitive-and-ultrasonic/

Fingerprint. (2021, May 29). Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Fingerprint

Tilman, M. (2020, September 28). *Apple's Touch ID fingerprint sensor explained*. Retrieved from Pocket-Line: https://www.pocket-lint.com/phones/news/apple/123832-apple-s-touch-id-fingerprint-sensor-explained-here-s-what-you-need-to-know