ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

NEUMANN JÁNOS
FACULTY OF INFORMATICS

DEGREE PROJECT

THESIS

OE-NIK Student's name: **Eziz Sahetmyradov**
2022 Student's registration number: **T/007198/FI12904/N**

Óbuda University
Neumann János Faculty of Informatics
Institute for Cyber-physical System

THESIS
WORKSHEET

Student's name: **Eziz Sahetmyradov**
Registration number: T/007198/FI12904/N

Title of study:

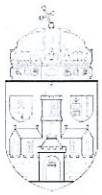
Investigation and demonstration of user authentication methods using an informative android mobile application developed for this purpose

Institutional supervisor: Dr. Eszter Balázsné Kail

External supervisor: Dr.Phuoc Dai Huu Nguyen

Submission deadline: 2022.May.15

Subject of the final examination: Cloud Computing System and Mobile Application I-II



ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Neumann János Faculty of Informatics

STUDENT'S DECLARATION

I the undersigned student hereby declare that this thesis is the result of my work; I have disclosed the references and tools used in an identifiable manner. The results indicated in my thesis completed may be used by the university and the institution announcing the task for their poses free of charge.

Dated: Budapest, Hungary 2022-05-14

student's signature

Eziz Sahetmyradov

Óbuda University
John von Neumann Faculty of Informatics
Institute for Cyber-physical Systems

DIPLOMA THESIS
TOPIC DESCRIPTION

Student name: **Eziz Sahetmyradov**
Registration number: T/007198/FI12904/N
Neptun's code: [redacted]

Title of diploma thesis:

Investigation and demonstration of user authentication methods using an informative android mobile application developed for this purpose
Felhasználói hitelesítési módszerek vizsgálata és bemutatása egy erre a célra fejlesztett informatív androidos mobilalkalmazás segítségével

Internal supervisor: Dr. Eszter Balázsné Kail
External supervisor Dr. Phuoc Dai Huu Nguyen

Deadline: 15th of May, 2022.

Topic description:

Over the past year, the importance of the internet in our daily lives has become more evident than ever. The COVID-19 pandemic has forced millions of people to stay at home, forcing us to rely on the internet for everything from work and school to doctor appointments and socializing. However, while we can all be grateful for this connection, another side to this story is Cybercrime. Putting much information online can allow people to steal vast amounts of data. Cybercrime is a growing issue that is getting worse every year.
When it comes to security and privacy, it is critical to determine whether or not a user is whom he or she claims to be. The lack or poor authentication can lead to data leakage or compromise.
The aim of the thesis is to investigate the threats of poor or not adequate authentication in our daily lives and to increase the awareness of authentication processes.

The diploma thesis should cover:

- a thorough investigation and classification of User Authentication Methods,
- price, complexity, and security comparison of User Authentication Methods,
- an investigation of the main threats to User Authentication Methods,
- the design and implementation of an informative android mobile application about User Authentication Methods,
- testing the mobile application of the developed android mobile application and its results.

ÓBUDAI EGYETEM * Neumann János Informatikai Kar * 1. Budapest Ph.

Fleiner R.
.....
Dr. Rita Fleiner
head of institute

Term of limitation: **15th of May, 2024.**

The diploma thesis is adequate and can be submitted:

.....
external supervisor

.....
internal supervisor

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Neumann János Faculty of Informatics

CONSULTATION LOG

Student's name: Eziz Sahetmyradov

Neptun code: [redacted]

Specialty: Mobile application and game development

Phone number: [redacted]

Mailing address (e.g. domicile): [redacted]

Degree project / thesis[1] title in Hungarian:

Felhasználói hitelesítési módszerek vizsgálata és bemutatása egy erre a célra fejlesztett informatív androidos mobilalkalmazás segítségével

Degree project / thesis[2] title in English:

Investigation and demonstration of user authentication methods using an informative android mobile application developed for this purpose

Institutional supervisor:
Dr. Eszter Balázsné Kail

External supervisor:
Dr. Phuoc Dai Huu Nguyen

Please write the data in printed capital letters!

Occ.	Date	Content	Signature
1.	20.04.2022	THE EVOLUTION OF AUTHENTICATION TECHNOLOGIES	Kail
2.	27.04.2022	DESIGNED AND IMPLEMENTED AN INFORMATIVE ANDROID MOBILE APPLICATION	Kail
3.	03.05.2022	APPLICATION ARCHITECT & SYSTEM DESIGN	Kail
4.	10.05.2022	APPLICATION ICON AND USER INTERFACE. TEST THE DEVELOPED APPLICATION.	Kail

The Consultation log is required to be countersigned by either supervisor on a total of 4 occasions of consultation.

The student has complied with the requirements of the subject titled Degree project I / Degree project II (BSc) or Thesis 1 / Thesis 2 / Thesis 3 / Thesis 4[3], and is allowed to proceed for reporting / defense[4].

Dated: Budapest, 10.05.2022

Kail
.....
institutional supervisor

[1] Underline as appropriate
[2] Underline as appropriate
[3] Underline as appropriate
[4] Underline as appropriate

Table of contents

Abstract

Over the past year, the importance of the internet in our daily lives has become more evident than ever. Because of the COVID-19 pandemic, millions were compelled to stay at home, forcing us to rely on the net for everything from work and school to medical visits and socializing. But while we can all be grateful for this connection, there is another side to this story—cybercrime. When it comes to data protection, identifying whether a user is a claimant is critical, and authentication occurs. Authentication is vital when dealing with security.

During this thesis work, I investigated and answered two main questions: 1) What are the main threats in our daily life to user authentication methods? 2) How can we increase awareness of authentication security? I did a systematic literature review.

In the first chapter, I did a thorough investigation and classification of user authentication methods and their price, usability, and security comparison.

After that, I investigated the main threats to user authentication methods and prevention methods for them.

In the concluding chapter, I designed and implemented an informative Android mobile application about user authentication methods and security risks that will help increase awareness of authentication security. Users can read and learn comprehensive information about user authentication methods and security risks, then evaluate their skills.

Introduction

If we want to talk about safety, identifying whether a user is a claimant is critical, and authentication occurs. Authentication is critical when dealing with security. The lack of poor authentication can lead to data leakage or compromise. In the digitalized world we live in, we often must use authentication at many points in our lives. Let us analyze together how many times per day we use authentication methods on average. We need to use authentication to access the phone and computer we use, to enter the buildings we live and work in, in our social media accounts, to do our shopping on the internet, and many more. Because of these factors, authentication is the most essential aspect of security.

There are numerous user authentication methods available today. Some require a password, some require identification, and some require a fingerprint. As technology advances, more methods will inevitably be created to provide more new authentication options. It is critical to have an effective user authentication system in place to protect information and system safety.

During this thesis work I will investigate and answer two main questions:

1) What are the main threats in our daily life to user authentication methods?

2) How can we increase awareness of authentication security?

This thesis work consists of three parts and six chapters. The first chapter investigates and categorizes user authentication methods and a comparison of their usability, price, complexity, and security. I will do a systematic literature review. I will use electronic databases and scientific resources to reach the information. Following that, I'll analyze the relevant articles and present the categories researchers apply for user authentication methods.

In the later part, I will explore the main threats to user authentication methods and their prevention methods. This helps us to learn about the most common risks associated with user authentication methods and prevention methods. I will do my research as I did in the first chapter.

For the third part of my work, I will develop an informative android mobile application about user authentication methods. This application uses the information found in the first and second parts of the work and additionally, the application user can check him/her knowledge about user authentication methods and security risks, and it will help increase awareness of authentication security.

Chapter 1: Importance of authentication in our daily life

Over the past year, the importance of the internet in our daily lives has become more evident than ever. Because of the COVID-19 pandemic, millions were compelled to stay at home, forcing us to rely on the net for everything from work and school to medical visits and socializing. But while we can all be grateful for this connection, there is another side to this story - cybercrime. Putting a lot of information online can allow people to steal massive amounts of data. Cybercrime is a growing issue that is getting worse every year.

Let us check some cyber statistics:

Figure 1- Live cyber threat map according to the [1].

As you can see Figure 1 shows the daily live cyber threat map if we look carefully at more than seven million attacks that happened this day and it is half of the day. More than sixty million attacks happened per day. The top targeted industries are education, government, and the healthcare system.

As you can see Figure 2 shows the report of McAfee shows us cybercrime costs the global economy about $1trillion and it is 50% more than that predicted in 2018. [2]

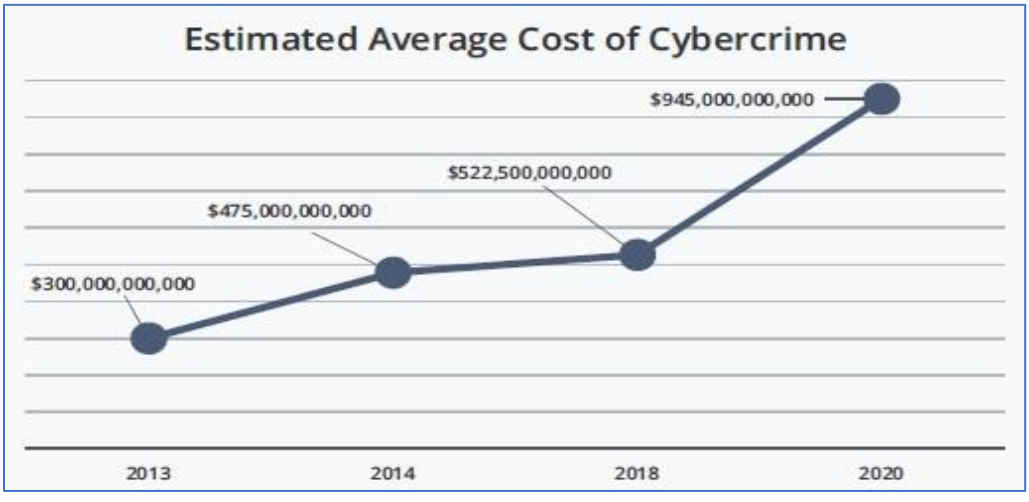


Figure 2- The average cost of cybercrime according to [2].

Some researchers show us that almost 90% of cybersecurity breaches are due to human error. It is meaning that if we can learn how to protect ourselves and businesses from cybercrimes, we can reduce cybercrime. [3]

Over the last decade, technological improvements have contributed to the greater access to and preservation of personal information in electronic devices. Because of that, we need more secure authentication systems.

1.1 Authentication concepts and definitions

Before we get into the various existing methods, we will go over some definitions and concepts.

- To use the services, the claimant must authenticate with the system.
- The tracker is the service that provides authenticating services. Verifies the claimant's identification or, if improperly authorized, denies it and decides if he/she is eligible for the needed service.
- The system gives services including login to social media accounts, and PR programs and allows the user to use them provided they are checked appropriately by the tracker. [4]

The cornerstone of a security system is made up of three interconnected concepts: identification, authentication, and authorization.[4] Identification is the process of communicating one's identity to an information system. Before authentication, the user often presents an identifier to the information system, which the tracker validates. Authentication is evidence presented by a claimant to demonstrate to a tracker that it belongs to the given identity. The tracker then confirms the user's identity with the information system. Last, authorization relates to the user's rights.

1.2 Authentication procedures

Initial step: The claimant's identity is unknown.

Step of connection: The claimant includes the utilization of an information system process that provides authentication. The monitor is requested to authenticate the claimant by the information system.

Step of authentication: The client gets validated, and the discussion begins. An information system presents the client with the necessary functions.

Step of disconnection: When the user disconnects or is removed from the monitor, the status reverts to the initial stage. A delay or a client interaction can initiate this stage. [4]

Chapter 2: Systematic Literature Review.

2.1 Methods authentications are classified by the user.

The author addresses authentication mechanisms in this paper. Entity authentication entails conclusively establishing the claimant's identity. The author categorizes authentication techniques into three distinct categories. [5]

Something you are aware of: The claimant establishes its identification by establishing possession of a secret, such as a password, PIN, or a cryptographic key.

Possession of something: The claimant establishes their identity through the ownership of a physical device, such as a magnetic card, a smart card, or a Personal Digital Assistant (PDA)

There is something innate: The claimant establishes its identification through the demonstration of a physical trait or involuntary action, such as a signature, a fingerprint, a retinal pattern, or the rate of writing on a keyboard. It is critical to note that these strategies are frequently combined to simplify their use and maximize their unique benefits. [34]

The author of this journal article discusses Pass Points, a technique for authenticating users using graphical images.[6] As shown in Figure 3, this research classifies authentication systems into three categories:

- Authentication based on tokens
- Authentication based on biometrics
- Authentication based on knowledge

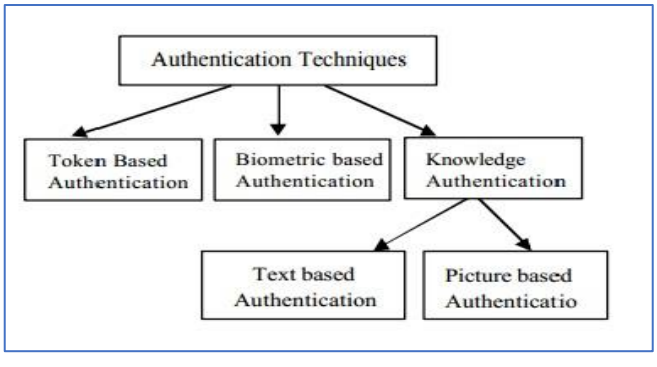


Figure 3- Authentication techniques are classified according to [6].

The article presents a method for an effective authentication process that uses keystrokes and brief static texts that can take place concurrently with the monitoring operation. The article analyzes the latest advances in keystroke authentication, covering terminology, information gathering, extraction, the framework of keystroke biometric data, and notable publications in the field.

[7] Summarize the researchers' proposed approach, the empirical findings and recommendations, and areas for further research.

These authentication processes covered in this article are categorized as follows:

- Authentication based on memory
- Authentication based on tokens
- Authentication based on biometrics [34]

The Bayesian Model Averaging (BMA) method was used to analyze the reliability of data mining-related decisions. The goal of this journal article is to talk about how decision tree structures from the BMA technique might be used to improve authentication in multifunctional biometric techniques. [8]

As you can see the Table 1 shows the authors divide authentication methods into three distinct categories in this section:

- Authentication based on tokens
- Authentication based on knowledge
- Authentication based on biometrics [34]

Classification	Example
Biometrics-based	
- static	Physical attribute, e.g. fingerprint, iris scan
- dynamic	Behavioral attribute, e.g. keystroke dynamics, signature dynamics
Token-based	Something you possess, e.g. swipe card, key
Knowledge-based	Something you know, e.g. password, PIN

Table 1- Categorization of authentication methods based on [8].

The author discusses various authentication techniques, their advantages, and disadvantages, and presents. [9] The computational complexity impacts this. The author classed authentication according to the following criteria:

- What someone owns: Smart cards, token
- What somebody is aware of: Passwords, PIN
- What someone is: Retina, fingerprint
- Any of these in combination

The authors of this article present a question-based authentication process that is effective for small environments. This article describes an investigation in which they attempted the evaluate if the archives generated by intelligent settings

regarding respective inhabitants' circumstances should be used to differentiate direct and participative from frauds as a result, they provide a fresh collection of knowledge for the authenticating model. [34] This example proves potential scenarios indicated by data should be used in a system that can process that differentiate authorized customers from frauds, and various difficulties must be solved before such an authentication system can be deployed. [10]

This article's authors present an overview of biometric factor approaches as well as a few emerging opportunities. A biometric can fulfill 2 purposes. Verification and authentication. Thus, the biometric authentication mechanisms must be sufficiently stringent to enable the simultaneous usage of both functionalities. Additional biometric solutions, including those relying on walking way, the retinal, arm veins, the inner ear, the face recognition, Genetics, smell and taste, and fingerprint, will be designed. Shortly, these biometric techniques may provide a solution to the world of information security's existing concerns.[11]

Biometrics are classified into two types by the authors:

- Physiological traits were linked to physical form and so differ from person to person.
- Behavioral is a term that refers to a person's behavior. Signatures, keystroke dynamics, and voice are all manifestations of this. Occasionally, because the voice is unique to each individual, it is also considered a physiological biometric. [34]

In this paper, the authors explore how a graphical password is a possible alternative to text-based passwords. According to human psychology, humans have an innate ability to recall images. The authors of this paper present a novel hybrid graphical password-based system that combines identification and memory approaches, giving extra improvement over conventional systems while also being better user-friendly. [12]

The classification provided by the authors:

- Method based on tokens
- Method based on biometrics
- Method based on knowledge

In this study, the authors discuss how unit authenticating corresponds to consistently relying on the respondent's identity. The author raises an essential point about how strategies are frequently combined to make them easier to use or more secure.[13] The author categorizes authentication mechanisms into three categories, as illustrated in Table 2:

- Something you are aware of
- You own something

- Something about you

	Authentication Factor			Risk Mitigated			Appropriate for Transitions			
	Something You Know	Something You Have	Something You Are	Stolen Device	Borrowed Device	Infected Device	UDUU → UDAU	UDUU → ADUU	UDAU → ADAU	ADU → UAD AU
Authenticating to Server										
Require User to Enter Strong Password	●	○	○	●	●	□	●	○	○	●
Require User to Enter Weak Password	●	○	○	□	□	□	○	○	○	●
Image-Based Authentication	●	○	○	□	□	□	○	○	○	●
Retrieve Password Stored on Device	○	●	○	○	○	○	○	○	○	○
Retrieve another Secret from the Device	○	●	○	○	□	○	○	●	●	○
Retrieve another Secret from the Device	○	●	○	□	□	○	○	●	●	○
SMS OTP	○	●	○	□	□	□	○	○	●	○
Device Generated OTP	○	●	○	○	□	□	○	●	●	○
Phone call	□	●	□	□	□	□	○	●	●	○
Hardware Tokens	○	●	○	●	●	□	●	○	○	●
Biometric	○	○	●	●	●	□	●	○	○	●
Rely on Another App for Authentication	□	□	□	□	□	□	□	□	□	□

Table 2- Different types of authentication methods according to the [13]

2.2 Discussion

In this section, I collected and combined the preceding results. Table 3 was constructed to track the categories attained by the different researchers. Reading the many categories used in previous publications reveals that several of the reference a certain topic under er alternative titles.

Classification	Sub-classification	Group	Method
Knowledge Factor	Depending on text		PIN
			Login Password
	Depending on image		Graphical Password
	Depending on gesture		Pattern Lock
			Gestural Passwords
Ownership Factor	Token of devices		Swipe card
			Key
	Computer/Smartphone		Retrieve the password stored on the device
			Retrieve another secret from the device
			SMS one-time passwords
			Phone calls
Biometric Factor	Physiological	Contact	Fingerprint
			DNA Analysis
			Finger-Knuckle-Print
			Vascular Patterns
			Palm Print
			Hand Geometry
		Contactless	Face Recognition
			Body Odor
			Ear Shape
			Retina Scanning
			Lip Shape
			Iris
	Behavioral	Contact	Keystroke Dynamics
		Contactless	Gait
			Voice

Table 3- A summary of the classifications of user authentication methods according to the literature reviews based on relevant articles. [34]

2.3 Knowledge factor

Knowledge-based authentication is an authentication method that relies on a sequence of knowledge questions to authenticate a person's identity to prevent an unauthorized individual from gaining access to a location or, more typically today, an account. As the term knowledge-based authentication implies, this method of authentication is based on information knowledge. That is, it is predicated on the assumption that only the legitimate owner of an account would be able to answer the questions presented.

2.4 Personal Identification Number

A PIN, often known as a PIN code, is an alphanumeric code which used to validate the authenticity using a platform. The PIN has been critical in allowing confidential data transfer between massive data centers in the networked computers of banking firms, organizations, and corporations. PINs are used to verify banking with merchants, authorities with residents, corporations with workers, and devices with clients, among other things. PINs are commonly used in ATM and POS payments, protected access control, internet transactions, and entering a restricted website. [14]

As you can see in Figure 4 for the PIN usage in ATM and a simple flowchart of how it is processed in the real life.

Figure 4- PIN usage in ATM and flowchart according to the [15].

2.5 Login password

Stable identity was remembered for its fundamental execution: Identification and password method authentication, which is a fashionable way of confirming the identity of a requester. In general, static authentication requires the claimant to show the monitor that he or she is aware of a private key, via exposing it. The monitor then analyzes the information contained in a confirmation database to determine if it is accurate. A password: is a string of characters, meaningful or not, that is typically between six and ten characters long. [16]

As you can see the Figure 5 When a user creates a password, the system or website retains a copy of that credential in a passcode repository, that might be compared to subsequent login attempts. Because all those credentials are maintained in a centralized location, password-based authentication systems must validate the

security of such databases. Passwords are typically encrypted and even if an attacker gets access to the database, the data they see is meaningless to him.

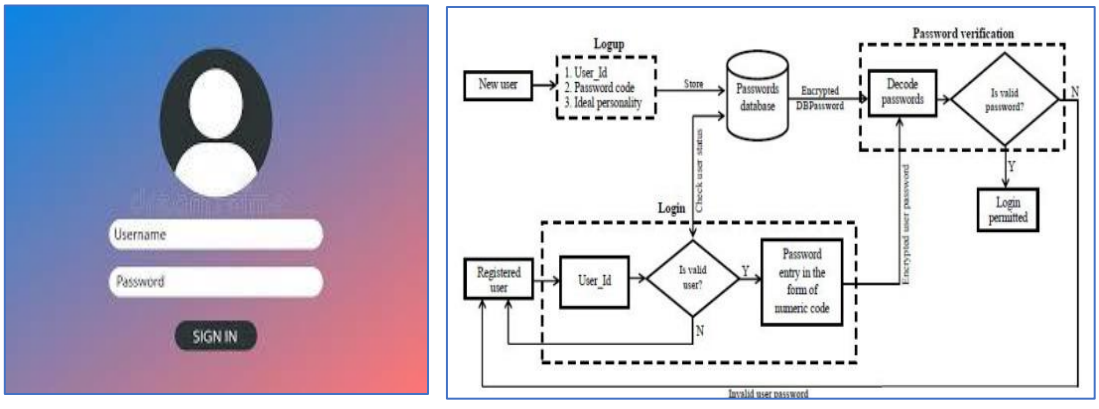


Figure 5- Login password authentication and simple flowchart according to the [16].

2.6 Graphical password

In a graphical password authentication system, the user must choose from a series of images given in a graphical user interface (GUI) in a certain order. According to a study, the human brain is better at remembering what it sees (images) than it is at recalling alphanumeric characters. Thus, graphical passwords solve one of the alphanumeric passwords. Graphical Password Authentication is classified into three major kinds based on the activity used to verify the password:

- Authentication by recognition: A user is presented with a series of photos and is required to identify the image he selected during registration. For instance, pass faces is a graphical password method based on facial recognition. Users are presented with a broad selection of photos to choose from throughout the password generation process. To authenticate, users must recognize the pre-selected image from a series of photos displayed to them.
- Authentication by the recall: A user is prompted to recreate whatever he made or selected during the registration stage. For instance, with the passport point scheme, a user can click any point in a picture to generate a password, and tolerance is calculated around each pixel. To log in, the user must select the points inside the tolerance in the correct order. [18]

Advantages:

It is simple to use. It is more secure than other common password methods. Dictionary attacks are physically impossible.

Disadvantages: Registration and login take an excessive amount of time.

2.7 Ownership factor. Token and one-time password authentication

A user owns or possesses an ownership component, such as a key, certificate, or token. Unlike a knowledge factor, which may be easily shared, whether intentionally or unintentionally, an ownership element is harder to communicate.

Token-generated OTP is typically used in addition to the static username and password. What makes OTP secure is that it must be used within a specified period; hence, if an attacker obtains access to an old OTP, the attacker will be unable to utilize it. OTPs are generated using a secure and random technique; there should be no correlation between one OTP and the next so that the attacker cannot predict what the next OTP will be. Additionally, another technique to secure the OTP algorithm is to hash it after it is generated; this makes it impossible for an attacker to deduce a pattern between the OTPs. It enables the conversion of legacy programs that were built to be password-only. [17]

2.8 Biometric factor

Biometrics is used in computer science as a method of managing identity access and access control. However, biometrics is an ancient Greek term that combines two terms: **bio** which means life, and **metric** which means measurement. [19] Biometrics is a branch of study concerned with developing ways for uniquely identifying persons based on one or more intrinsic physical or behavioral characteristics. Biometrics approaches have been created to automate the verification of a person's identity. The properties of biometrics can be classified into three broad categories: 'Morphological', 'Behavioral', and 'Biological'. Morphological features include the retina, voice, fingerprints, iris, hand geometry, facial identification, ear, height, weight, skin, veins, and gender. The term "behavioral" refers to a person's behavior, such as gait, signature, keystroke dynamics, voice, driving, and gaming. The term "biological" refers to the interior workings of a live organism, such as heartbeat, odor, DNA, and blood. Because everyone has a unique vocal tract, the voice might be defined as morphological or behavioral. However, because voice recognition is mostly focused on the way a person speaks, it is frequently classified as behavioral. Certain scholars coined the word behavior metrics to refer to the behavioral subset of biometrics.

Biometric recognition is a field of study that is heavily researched in computer science. Biometric techniques such as face, fingerprints, iris, and ears can be used to create a safe means of personal authentication. Biometrics makes use of authentication factors, which are ways depending on the user's qualifications and abilities. The fundamental advantage of such authentication systems is that they create a strong interaction between the person and the verifier. Additionally, unlike many other authentication techniques, it is impossible to duplicate an individual's biometric traits. [4]

In Figure 6 you can see the afferent kinds of characteristics.

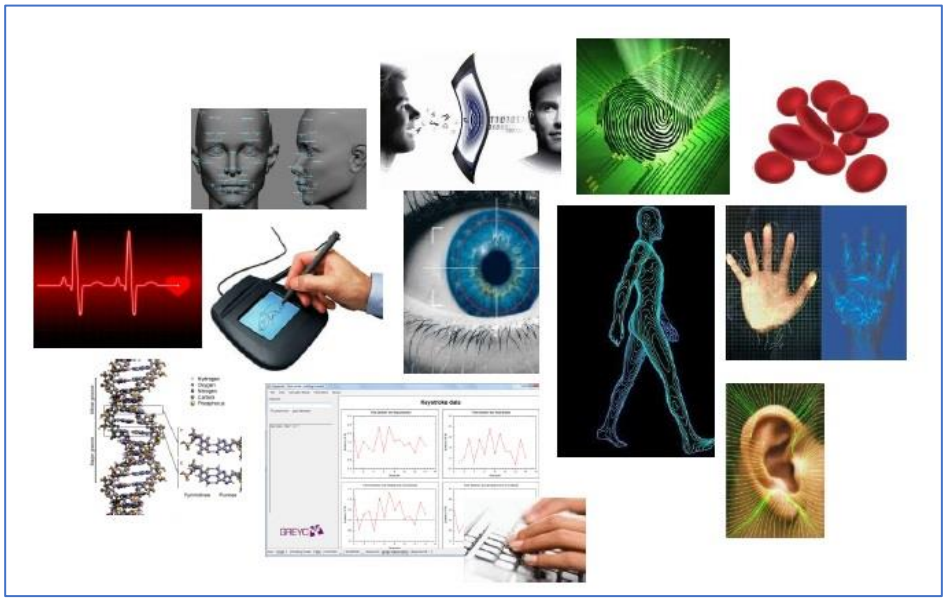


Figure 6-Biometrics characteristics. [4]

2.9 Multi-factor authentication

Originally, always one aspect is employed to validate the legitimacy of the item. Because of its flexibility and ease of use, the community had mainly accepted Single-Factor Authentication (SFA) by that point. For instance, the use of a password to verify the user ID's ownership could be considered. It is considered the simplest authentication option. An account could be quickly compromised by exposing the passcode. Furthermore, an unauthorized party may try to get an entry by using a dictionary attack, a rainbow table, or social engineering tactics. Typically, while implementing this method of authentication, the minimum password complexity requirement is considered. [20] Furthermore, it became discovered that how authenticating with a specific factor is able to continue providing sufficient security again different risks. Two-factor authentication (2FA) has been described as a natural progression that integrates the relevant sample with a personalized possession aspect, such as a token or a cellphone. Following that, Multi-Factor Authentication (MFA) was created to add an extra layer to the insecure city and to enable continued defense of hardware and software as well as other vital services from unauthorized by utilizing over two types of passwords. As shown in Figure 7, MFA is largely dependent on biometrics, which refers to the automated recognition of persons based on their behavioral and biological traits.

This step increased security by requiring users to show evidence of their identification, which is based on two or more distinct variables.

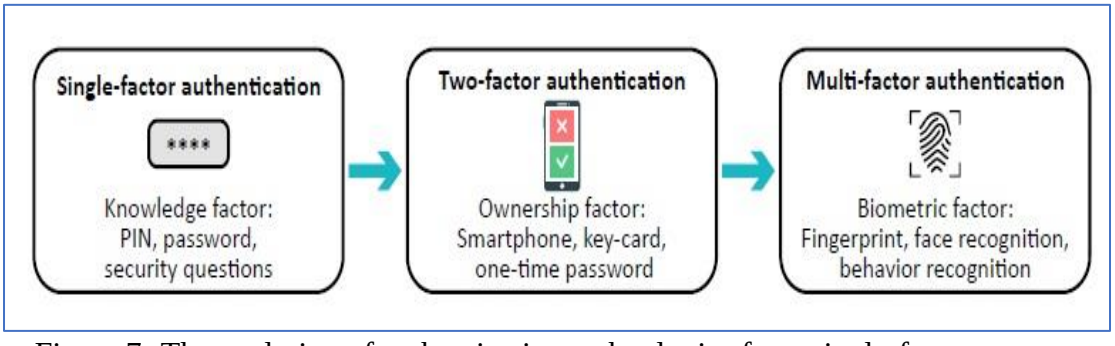


Figure 7- The evolution of authentication technologies from single-factor authentication to multi-factor authentication. [20]

Chapter 3: Comparison of usability, price, complexity, and security of user authentication methods.

User-friendliness is explained as the extent to which a service may be used effectively, efficiently, and satisfactorily by certain users in each situation.

Satisfaction can be further classified into the sub characteristics listed below.

Acceptability is a state of cognitive contentment.

Pleasure is emotional fulfillment.

Physical well-being is defined as comfort.

Confidence is a satisfaction to protection. [34]

The writers of this article compared three types of authentications: standard text-based passwords, Mnemonic-based passwords, and graphical-based passwords. The authors concluded that text-based authentication is faster than graphical authentication.[21] The size of the authentication key and the quantity of the authentication page largely impacted the length of time necessary for authentication.

When it comes to usability, login information is relatively old equipment that people find quite simple to use. Graphic passwords are a relatively new type of authentication.

Detailed analytical evidence was conducted by the researchers to examine the accessibility of 3 distinct forms of authenticating in a real-world internet scenario. According to the findings, complex passwords take significantly more time to establish than textual or memorizing passwords. Textual credentials, like graphical passwords, are equally remembered. Mnemonic passwords had a greater average failure rate than the other two types of passwords. By and large, graphical passwords necessitated a greater amount of labor than text or mnemonic passwords. We will do additional studies to corroborate the findings using a much larger sample size. Additionally, we intend to investigate whether there are differences in performance and workload when other user populations, such as those with a cognitive disability or senior citizens, utilize the authentication methods.

The authors of this article discuss several authentication approaches from a security standpoint as well as their general usage. Several strategies were discussed, including the following:

- Passphrase: A client must memorize the passphrase, which could have a character limit.
- Authentication tokens: One drawback is that users may be made to take numerous smartcards, which can be lost and must be replaced at the user's

expense.

- Biometric authentication: There is no need for the user to memorize a Security code. They can be extremely safe, but there is difficulty with initial enrollment and setup. [22] [34]

Feature/ Acquisition Device	Pass-words (PW)	PIN	Proximity card	One Time Generators	Challenge-Response	Multifunction Card	Public Key (PK)	Kerberos	Finger print	Voice	Signature	Retina/Iris	Keystroke recognition	Under the Skin ID chip
Definition	Knowledge-Based 8 to 12 digits	Knowledge-Based 4 digits	Authentication Token	Authentication Token	Authentication Token	Authentication Token	Cryptography	Key Distribution Center	Biometrics, User Scanning	Biometrics User Voice when speaking	Biometrics Length/Width pen pressure	Biometrics Pattern of blood vessel	Biometrics User Typing Rhythm	RFID based
Advantages	Ease of deployment	Network less	Last Longer (Contactless)	PW is difficult to guess	No Synchronization	Built-in Dynamic data processing	User Credentials once per login session	Mutual Authentication	Ease to collect	No PW's	High-definition Graphic	Unchangeable (Lifetime)	No enrollment	Forger, stealing a chip is hard
Disadvantages	Can be forgotten	Can be forgotten	Theft, Fraud	Brute Force, Dictionary attacks	Users shares their access permisions	Need for a smart card reader	PK is a single point of attack	Seal ability	Criminal affiliation	Changes over time	Can change signature at any time	Excessive user cooperation	Spoofing	Spoofing
Security	2	2	3	3	3	5	5	5	4	1	3	5	3	4
Usability	2[1]	2	3	3	3	3	3	3	3	5	3	2	3	3

Table 4- Methods of authentication: A comparative analysis of authentication methods according to the [23].

The authors conducted a comparative analysis of the many characteristics of authentication systems as part of this project, as shown in Table 4. They utilize subjective rating scales to define the following features: "Safety" and "User experience" (scaled from 1 to 5 to measure the intensity of difficulties associated with each authenticator). In this case, – defined as simplicity of use. [23]

This article examines graphic credentials, which have been recommended as more remembered and reliable authentication techniques because they capitalize on the natural proclivity to detect and remember pictures faster than text. [24]

The writers of this article investigated the usability and feasibility of biometric technologies among the elderly. Researchers point out that, although fingerprint identification methods are the most often used biometric technology, numerous studies show that its performance deteriorates with age. The goal of this study was to find out how accessible and acceptable biometric technologies are to an elderly population. [25]

The people preferred veins technology to fingerprint technology. The vein method was chosen because it was more user-friendly, and faster. Attendees said they would like to use vein-based biometrics than fingerprint technology at an ATM. Figure 9 summarizes these distinctions. There was a link between participant age and device preference, with the elderly preferring vein-based devices. The increased performance of the venous system in older users explains this impact.

Ease of use	Vein > Fingerprint
Speed of use	Vein > Fingerprint
Security	Vein = Fingerprint
Stressfulness	Vein > Fingerprint
Preference	Vein > Fingerprint
Willingness to use	Vein > Fingerprint

[34]

Figure 8- According to [25], there are connections among fingerprint identification metrics.

The authors studied the comparative requirements on realizing, work, mistake, and job disturbance imposed by 3 biometric factor authentication methods – speech, facial, and motion – as well as smartphone passcode, and entering. [27]

This was the first study to quantify the time necessary for a user to conduct an authentication action on a smartphone utilizing various biometrics. This collects data on user satisfaction when these tactics are used under favorable conditions. The study looked at the following:

1. The amount of time required to give an authentication sample (password, biometric, or a combination of the two).
2. Error rates in giving a representative group with a good enough standard for evaluation by validating methods. An impact on required actions on reca performance.
3. Client responses to authentication techniques.

The authors reported the findings of a field investigation in which they compared Android-like graphical passwords against PINs in terms of performance, usability, and likeability. Additionally, they provided a taxonomy that aids in delving deeper into the causes of reported errors. They acquired generalizable data by examining Android-conformant patterns while evaluating their more sophisticated counterparts providing insight into the impacts of having an unrestricted password space.[27]

The study discovered that the idea of error restoration is a substantial difference between the two strategies. Although a PIN model allows for error recovery through reverse procedures, template clients were compelled to enter every try exactly as it was. This is identical to the strategy used in existing real-world implementations. The results indicate that the idea of error recovery influences the input speed and rate of success. While PIN users' average entry speed was faster, we were able to show that undo actions had a significant impact on their capacity to contribute. The majority of the design party's mistakes were created by slips, meaning that many of these errors might have been avoided with the usage of undoing processes. However, as indicated previously, the pattern prototype did not permit undo actions. However, if they might have been avoidable, our qualitative findings indicate that they would not have occurred very frequently.

The findings indicated that a greater proportion of participants in the pattern group claimed that they recovered quickly or very quickly from errors. This implies that users place a higher premium on rapid error recovery than on error avoidance, casting doubt on the utility of undo operations in such an approach.

3.1 Memorability

Table 5 summarizes whether memorability has been evaluated in the literature. As illustrated in Table 5, various research confirms that graphic authentication is more recallable than text authentication verification. Performance appears mostly due to clients' improved ability to recall graphics. Additionally, people select the visuals that they must recall in many circumstances. Additionally, we can see how the Iris scan is more memorable than a PIN, as it does not need to memorize anything. Other writers have examined memorability generally for the three major authentication technique classes. These authors discovered that token-based authentication and biometrics had a greater capacity for memorization than knowledge-based authentication. Additionally, under biometrics, we have behavioral authentication, which is more memorable than Knowledge-based authentication.

Article of research	**Method**	**Category**	**Comparative**	**Another method**
[21]	Graphical authentication	Knowledge factor	Preferable to	Text authentication
[30]	Graphical authentication	Knowledge factor	Preferable to	Text authentication
[24]	Graphical authentication	Knowledge factor	Preferable to	Text authentication

[29]	Graphical authentication	Knowledge factor	Preferable to	Text authentication
Classifying Compare				
[22]		Ownership factor	Preferable to	Knowledge factor
		Biometric factor	Preferable to	Knowledge factor
		Psychological	Preferable to	Knowledge factor

Table 5- A comparison between authentication systems was assessed by findings gathered on their recognizability features. [34]

3.2 Usability

As illustrated in Table 6, the usability accessibility attribute was the most prevalent in our research. I discovered that behavioral approaches are more user-friendly than every authentication mechanism available. Keystroke authentication is more user-friendly than knowledge-based systems and comparable to face authentication techniques. Voice recognition is more user-friendly than knowledge factor solutions, according to the authors' comparative analysis of numerous aspects present in authentication systems. Furthermore, it is founded on comparison research. Biometrics technology such as fingerprint/hand/face recognition is more user-friendly than knowledge-based systems. Proximity Card Authentication is as user-friendly as fingerprints, hand, face, keyboard, and iris authentication. Each one is supported by a comparative analysis. Both text passwords and PIN passwords are equally simple to use. They are, however, more difficult to utilize than biometrics and token-based methods. Iris recognition technology is more user-friendly than knowledge-based solutions. This is partly because biometrics and token-based authentication require users to engage with the system less than knowledge-based authentication does.

Research Paper	**Method**	**Classification**	**Comparison**	**Other Method**
[23]	Smart Card	Ownership factor	Preferable to	Fingerprint/Hand/Face
	Fingerprint	Biometric factor	Preferable to	Knowledge-Based
	Iris	Biometric factor	Preferable to	Knowledge-Based

	Keystroke	Biometric factor	Preferable to	Knowledge-Based
[28]	Keystroke	Biometric factor	Equal to	Face time
[23]	Password	Knowledge factor	Less to	Biometric, Token
[27]	Pattern-based authentication	Knowledge factor	Preferable to	PIN-based Authentication
[23]	PIN	Knowledge factor	Less to	Biometric factor, Ownership factor
[25]	Vein	Biometric factor	Preferable to	Fingerprint
[23]	Voice	Biometric factor	Preferable to	Knowledge factor
Categorization Comparative				
[22]		Psychological	Preferable to	Biometric factors, Smart cards, the knowledge factor

Table 6- A comparison between authentication techniques was assessed by findings gathered on their user-friendliness features. [34]

Each authentication method is unique. None of them are interchangeable, and each will answer to unique requirements. Each authentication method retains inherent advantages and disadvantages. On various distinct criteria, Table 7 provides a comparative examination of broad authentication methods. The following criteria apply:

- Confirmed acceptance is the proportion of the authentications deployed in general.
- The infrastructural cost is the cost of implementing such an authentication technique in an IT architecture, as well as the cost of maintaining the authentication system's operation. It comprises costs associated with user support, device replacement, new user enrollment, and user revocation;
- Ease of use refers to the general availability of authentication mechanisms such as customer satisfaction, tokens, formal element, and effective involvement. In important circumstances, general privacy is an objective assessment of the authentication technique. This is a purely debatable rating that should only be used as a tool for authenticating. The analysis offers useful information about authentications & configurations. As we can see, the stated popularity of authentication techniques is closely tied to their extensive use, and low infrastructure costs also contribute to their widespread use. It is also inversely related to the level of protection offered,

at least for that exact small range of authentication methods. The clear relationship between acceptance and usability indicates why important usability is for the installation of any authentication process. The expense is relative to the quantity of safety given. [4]

Technique	The attraction was noticed.	The technology of average quality	Structure cost	Usability	Fundamental safety	Cons	Pros
Simple one-time passcode	*** ***	-	*	** **	*	With several credentials, safety is quite low, and efficiency falls.	User-friendliness
Dynamic passcode that is secure	** **	-	**	*	**	That replay ability is a threat to efficiency.	More secure than a basic password.
A token with a certification	***	**	*** **	** **	** **	Installation costs, tokens price	Physical authentication offline
Token for synchronized OTP generator	***	***	***	** **	** **	Price of the equipment, shape aspect	Excellent privacy and usefulness
Biometrics	*	**	**	*** **	*** **	Approval, difficult rejection, and increased price	Excellent overall protection.

Table 7-Comparative analysis of several authentication methods according to the researchers. [4]

Chapter 4: Investigation of the main threats to user authentication methods

Numerous websites and portals on the internet, including academic institutions, should restrict unauthorized users' access to their materials such as commercial secrets, confidential information, intellectual property, as well as other sensitive data. For instance, remote education universities must ensure accurate verification of students when doing evaluation assignments. Banking organizations should only offer consumers access to their accounts when their identity has been credibly validated. A protection access technique has a meaningful effect on such an information system's overall security, particularly in the case of online education systems, on the dependability of the results of students conducting educational activities. One of the steps in the login procedure is to verify the logged-in user's name.

There are well-known methods for confirming information service users. The first class of such techniques is based on validating the user's knowledge using some remembered keys, such as the private mixture passcode. An authenticating method confirms that this key was recognized. That another kind of authentication process establishes possession of a piece of equipment that functions as an object, such as the user's identification or tokens. The gadget keeps the customer's core confidential, such as the cryptographic key signature, which the client would not need to learn. Final authenticating techniques rely on determining if a client possesses flawless characteristics. These characteristics could include pressing a finger, a face, or a voice. These are techniques of biometric authentication.

4.1 User authentication with secret knowledge validation

The main benefit of knowledge factor for client confidential reuse login is its flexibility and setup including using. Password authentication, on the other hand, has various drawbacks:

- A possibility for committing a violation by using widely accessible software tools enabling password cracking.
- Because of their small size, ease, and recurrence, several clients use passwords that are easy to guess.
- An ability of the offender to mislead the client and steal credentials through social engineering techniques.
- An ability to capture or block a passcode when typed on a keyboard or communicated across an intranet.

4.2 Method of user authentication using tokens

Authentication with verification equipment is based upon that device's memory's uniqueness and privacy. As a result, information such as the customer's digital signature's private key is used.

For authentication, the various technologies are typically used:

- A token that links to the computer via USB but also functions as a minicomputer.
- Smart cards, like microcomputers, require the deployment of card machines.

Reusable passwords, which are information that certifies use by the device's rightful owner, provide further fraud prevention to operational USB devices. Additionally, authentication devices have no limitations on the amount or complexity of data that can be stored in the device's memory, as well as the ability to detect.

However, there are several disadvantages to using authentication devices:

- The potential that the equipment will break down or be damaged accidentally.
- Additional fees are applied by registered devices and viewers.
- A available USB port on your computer is required, otherwise, you must acquire extra devices to join your gadgets to the PC.
- An ability can duplicate digital techniques, perpetrate crime, and build program simulations.
- When a user's private key is used as an authenticator saved on their hidden gadget, a public key must be generated.

4.3 User authentication through biometrics

Biometrics confirms that the client is distinct and interconnected from character traits, which include physiological or deterministic habits of fingerprints, biometric features, retina, and facial structure, as well as psychosocial or dynamic timbres such as signature, keypad, or keypad rhythmic message input and so on. These advantages of biometrics include its legitimacy, user-friendliness, the elimination of the need to always learn lengthy and complicated passwords or transport authenticating equipment, as well as the difficulties of tampering with the criminal's biometric characteristics.

The following are the drawbacks of biometric authentication:

- The increased expense associated with the technology required to read biometric parameters.
- Standards for the storage of biometric traits in plaintext, posing a risk of violating the user's privacy.
- Failure of a registered user due to an accidental significant deviation from the checked property of the standard.
- The prospect of intercepting biometric data as it is transmitted through a network.

Despite the growing number of unique user authentication techniques, password-based authentication stays among the most effective. Passwords are simply memorized, and people can use them in their everyday routines for free. On the other hand, passwords can be forgotten because of the combination of multiple passwords for various accounts. Different kinds of authentication have been gradually introduced throughout time, including biological and graphical passwords. Combining two or more techniques is becoming more common in authentication systems. This combination is used by these systems to identify genuine users from fraudsters. There are three types of authentication methods: what you know, what you do have, and what you are.

Due to the nature of knowledge-based authentication, there are known and novel dangers that make this kind of authentication less reliable. The first disadvantage of a knowledge-based method is that it requires memory, which might confuse when dealing with many passwords. The second disadvantage is shoulder surfing, which allows a passerby to eavesdrop on the keyboard from a close or quite a distance. Numerous brute-force and dictionary attack tools are capable of cracking passwords and PINs. Additionally, keyloggers that intercept pressed keys are intentionally designed to steal users' passwords; some of the more complex ones can capture the entire screen if a virtual keyboard is enabled. It's worth noting that several graphical passwords are also susceptible to screen capture. [31] As a result, the software or onlookers would jeopardize procedures that require inputting a password, clicking on certain areas of an image, or picking several photos from a collection. On the other hand, the Biometric-based model, which is divided into 2 sub-categories physiological and behavioral, would be more difficult to penetrate than the knowledge-based model. However, this model's shortcomings, such as expensive implementation costs, scars, sunglasses, and surgery, can be problematic and affect the system's accuracy. Above all, replay attacks and some forgeries techniques can simply overcome biometric authentication methods including placing a photograph of someone's face in front of a detection camera. Finally, the ownership model demands.users to carry extra physical items such as a security token or smart card continuously. As a result, if the person has lost his physical device, security concerns arise, as anyone who finds the device can log into the system. Additionally, man-in-the-middle attacks pose a concern by gathering data exchanged between users and servers. It should be noted that two-factor authentication systems typically do not protect against man-in-the-middle attacks. As illustrated in Table 8, each authentication mechanism introduces various risks and disadvantages that must be evaluated during the design phase.

Knowledge Factor	Ownership Factor	Biometric Factor
Keylogging	Man-in-the-Middle (MITM) attack	Forgery method
Shoulder Surfing	Losing Devices	Replay attack
Guessing	Usability	MITM attack
Brute Force	Stealing token	High costs
Dictionary attack	High costs	Accuracy issue
Screen capturing		Surgery and scars
MITM attack		Lights and clothes
Memorability		

Table 8-Threats and disadvantages summaries for each model according to the researchers. [31]

Numerous authentication schemes that are widely used in modern security engineering are vulnerable to certain types of attacks, including denial-of-service, replay, and deceptive attacks. As described in the Introduction, standard username/password-based authentication suffers from several issues. According to researchers, a home computer can guess around 80% of typical passwords in a week. This exercise became more difficult because of the addition of different symbols to a passphrase. By contrast, as hardware was becoming more powerful each year, password cracker software deployed a variety of techniques to accelerate the cracking process.

The following are three techniques for mitigating passwords' shortcomings:

- To overcome dictionary attacks, it is recommended to use a long string of words that are not included in commonly used password dictionaries, such as this research article is about authentication systems.
- Mixed symbols: Password security mechanisms require users to include capital letter characters, special symbols, and other characters to improve the entropy of the password and make brute-force attacks less possible.

4.4 Brute force attacks

Simply explained, a brute-force attack is when a computer software attempts every possible password combination until it finds one that matches. The algorithm will cycle through all one-digit and two-digit possibilities until it breaks your password. Some algorithms merely consider the commonest dictionary terms, while some compare frequent passphrases to a collection of plausible credentials. As technology advances, so do the methods used by hackers to crack people's

passwords. Apart from guessing your password, the most prevalent tactic used by hackers is a brute-force attack. To compound matters, these algorithms are capable of processing thousands of possibilities in under a second, which implies that a shorter password can be broken in a matter of seconds.

There are numerous brute force attack techniques that attackers might use to obtain unauthorized entry and steal user information. A brute-force attack occurs when an attacker attempts to guess the user's login credentials by hand rather than utilizing the software. This is often accomplished by conventional password variations or PIN passwords. These threats are straightforward because many users continue to use weak passwords including "password123" or "1234" or engage in poor password ethics, such as using the identical password for many websites. Hackers can also guess passwords by performing minor reconnaissance work on an individual's prospective password, such as the name of their celebrity names.

Dictionary attacks

A dictionary attack is a form of brute-force attack in which the attacker chooses a victim and then compares potential passwords to the victim's username. Although the assault method is not technically a brute-force attack, it can be a critical component of a bad actor's password cracking process. The term "dictionary attack" refers to hackers poring over dictionaries and substituting special alphanumeric characters for words. This form of attack is often lengthy and has a poor success rate in comparison to modern, more effective attack tactics.

Hybrid brute force attacks

The hacker begins by obtaining a username and then employing dictionary attacks and basic brute force methods to acquire account login combinations. The attacker begins with a list of possible words and then tries various characters, letters, and possible combinations to discover the proper password. Hackers can use this technique to uncover passwords that include common or trendy phrases with dates, and random symbols, including "NewYork123" or "Liverpool2022."

Reverse brute force attacks

The reverse brute - force begins with a known credential that is often found because of a network breach. They utilize the password to search through lists of dozens of usernames for a matched login credential. Additionally, attackers would use a frequently used simple password, including "Password123," to seek a match in a database of usernames.

Credential stuffing

Credential stuffing exploits users' poor password management. Attackers collect stolen login/password combinations and test them on other websites to determine

whether they can allow entry to more user accounts. This strategy is successful if individuals use the same login and password for several services and social media pages.

4.5 How to protect yourself against brute force attacks?

Organizations and individuals can take a variety of measures to safeguard themself against known vulnerabilities such as those in the Remote Desktop Protocol (RDP). Cryptanalysis, or the research of encryption methods and crypto, can also assist businesses in strengthening their system security and defending against brute force attacks.

Utilize more secure password practices

The best defense from brute force attacks on credentials is to make them as difficult to crack as possible. By choosing stronger passwords and adhering to stringent password best practices, end users may play a critical part in securing their own and their organization's data. This increases the difficulty and time required for hackers to guess their credentials, which may cause them to give up.

Among the best practices for creating stronger passwords are the following:

- Make strong, multicharacter passwords: As a general guideline, passwords should be longer than ten characters and contain capital and lower-case letters, symbols, and numerals. This significantly increases the complexity and duration of cracking a password, from several minutes to several decades, until an attacker has access to a supercomputer.[33]
- While adopting longer passwords is a good idea, some websites may put rules on the size of a credential. As such, use complicated passwords to avoid attackers using basic dictionary attacks. Passes are composed of many words or parts that contain special characters that enable guessing them more difficult.
- Create rules for password creation: Another effective password strategy is to truncate words to make them appear nonsensical to others who read them. This can be accomplished by eliminating vowels or utilizing only the first two words and then constructing a meaningful sentence from a string of abbreviated syllables. For instance, reducing the phrase "take" to "tk" or the word "pain" to "pn."
- Avoid frequently used passwords: Passwords that are often used, such as a user name, a soccer club, or simply "key," are particularly hazardous. Hackers are aware of frequent phrases and words that users use in their credentials and utilize these words to get access to people's accounts.
- Utilize unique passwords for each account: Credential stuffing involves hackers testing previously used passwords on websites to determine if they are being used anywhere. Regrettably, this strategy is extremely effective,

as people commonly repeat their credentials for personal emails, social networking accounts, and news websites. It is critical to avoid using the same passwords for many websites or accounts.

- Utilize privacy tools: A password manager enables individuals to establish secure, unique passwords for each website to which they log in. It establishes and tracks users' logins to various websites automatically, allowed to access all their profiles by just logging into the password manager. A password manager enables users to establish lengthy and complicated passwords, safely store them, and minimize the possibility of deleting, missing or having credentials stolen.

Improve the security of user passwords

It is pointless for users to adhere to strong password practices if their employer is incapable of defending against brute force attacks. Additionally, the business is responsible to protect its users and enhancing network security through measures such as:

- Utilize multi-factor authentication (MFA): By incorporating authentication into a user log-in, you remove the reliance on passwords. After a person enters in with their credentials, they will be required to provide further verification, including a code given by SMS or stored on their device, or a biometric scan. This can prohibit a hacker from accessing a user's account or company system, even if the hacker has the user's login credentials.
- Restrict login attempts: By limiting the number of times a user can re-enter their password credentials, brute force attacks' success rate is decreased. During two or three invalid login attempts, preventing another attempt can stop a potential hacker, while blocking an account after several failed login attempts prevents the hacker from trying login/password combinations repeatedly.
- Implement an IP blacklist: Using a blacklist of IP addresses associated with assaults enables commercial networks and their users to be protected from known attackers. It is critical to maintain this blacklist current to avoid future assaults.
- Eliminate unused or neglected accounts: Inactive or neglected accounts provide an easy entry point for cyber thieves to conduct an attack against a company. Businesses must guarantee that unused accounts are deleted regularly or, ideally, as soon as personnel leaves the firm to avoid them being utilized in brute-force attacks. This is particularly critical for employees who have elevated permissions or access to sensitive organizational information.

Provide Ongoing Support for Security and Passwords

1. Give password teaching: Users must know what constitutes sound privacy and password usage habits, as well as the clear indicators of a cyberattack. They also require ongoing education and training to stay informed of emerging hazards and to reinforce good practices. Additionally, corporate password manager solutions or vaults enable users to save complicated passwords and prevent the possibility of password loss, which could jeopardize business data.
2. Real-time monitoring of networks: Brute-force attacks can be identified by telltale activities such as repeated authentications and login information to new devices or unexpected locations. Organizations must continuously check their network systems for odd or suspicious behavior and swiftly shut off any harmful activity.

4.6 Keyloggers

Keyloggers have grown in importance because of their largely undetected nature by many antiviral methods. Keyloggers, surveillance programs, desktop traffic monitoring tools, input detection functions, input reporters, keypad watchers, and surveillance software are all names that are used interchangeably. While keyloggers' primary job is to monitor a device's keypad operations, they are progressed to offer extra features. They are capable of tracking nearly anything that runs on a computer. Certain keyloggers, referred to as "screen scrapers," enable visual surveillance of a targeted device by capturing frequent screen photos. Once saved, the photographs can be utilized to acquire vital personal data. Modern keylogging software can track internet activity, file operations like playing, creating, renaming, altering, and deleting files, and output, as well as cut, copy, and paste operations. Keyloggers are also used to monitor users' activities and to collect information including personally identifiable information or other sensitive or private data. Keyloggers are not the same as other forms of spyware or malware, such as viruses or worms.

Most keyloggers are classified into two groups:

- Keylogger hardware
- Keylogger software

Keylogger hardware

Tiny electronics that track information exchanged among a typing device as well as an input/output connector is known as hardware keyloggers. They save entries in their internal memory once installed on a personal computer. On the market, there are many various commercial hardware keylogger products. Most versions connect to the ends of the keyboard cable. This hardware consumes no system resources. It is undetectable by anti-virus software or scanners because it operates

on the hardware. Additionally, it does not save keystroke logs on the computer's hard disk. The recorded keystrokes can be encrypted and kept in the device's internal memory, which often surpasses 2MB.

Keylogger software

Keylogger software watches systems inside this targeted OS that gather keyboard input, keep it in memory or isolated places, and then pass it on to a keylogger threat. Remote access keylogging software allows remote access to data stored locally. This communication might occur in several ways: [34]

- Uploading data to a webpage, database, or file transfer protocol (FTP) server.
- Sending data via email to a predetermined address periodically.
- Wireless data transmission via a hardware system attached.
- Remote login software that enables you to access your local computer from a remote location.

More functionalities included with some software keyloggers allow for the acquisition of additional data without requiring the user to enter any keyboard key presses. In Figure 9 we can see the process of the keylogger. They include the following:

- Clipboard logging — This feature captures anything that could be duplicated to the clipboard.
- Screen logging - Screenshots of your computer's screen are taken at random intervals.

The capture of control text - The Windows API enables programs to obtain the textual value of certain controls, which means that your credentials may be collected even if it is hidden behind such a password shield. Tracking activity Keeping track of which folders, programs, and windows are opened, as well as maybe taking screenshots of each.. Search engine inquiries, instant messaging exchanges, FTP downloads, and any other online activity are all recorded.

4.7 Detecting and removing keyloggers

There are numerous methods to monitor a keylogger, but none are foolproof, therefore if you have cause to believe your computer contains a keylogger, we suggest experimenting with the following tactics:

- To begin, launch your antivirus software, which will frequently discover a keylogger on the computer.
- To check for certain forms of malware, run a tool such as Spybot Search and Destroy or Malwarebytes.
- In Windows, you can access your task scheduler by pressing Ctrl+Alt+Del. Examine the jobs that are now executing, because if you're unaware of any

one of them, use a search engine to find them up.

- Conduct a scan of your computer's hard drive for the most recently stored files. Examine the details of any folders that are frequently updated, as they may contain logs.
- To determine which apps are launched at computer startup, use your configuration management utility. This list can be accessed by typing "MSConfig" into the command prompt.

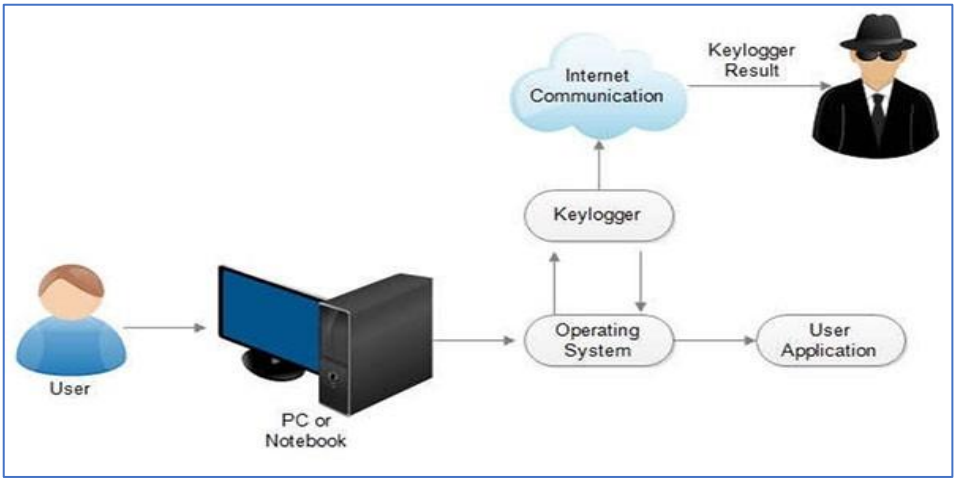


Figure 9- Process of the keylogger according to the [32].

4.8 Shoulder surfing

Shoulder surfing is a form of identity theft in which thieves acquire your personal information by eavesdropping on you as you use a notebook, ATM, public kiosk, or another electrical gadget in public. Despite the amusing moniker, this is a serious security issue that can result in financial ruin. Shoulder surfing may occur if you share private information, especially in a public area. This covers not just ATMs, payment kiosks, and PIN pads, but also virtually every location where you can input personal data using a laptop, tablet, or smartphone. Typically, the early shoulder surfers did not hang over their targets' shoulders to get information. Rather than that, they stayed a long distance away and read people's finger motions while they typed numbers onto a keyboard. Similarly, shoulder surfers of today frequently go unnoticed as they silently monitor others in public spaces such as lounge access and shopping centers, pubs and restaurants, trains and subways, or anywhere else people gather. While you would feel secure from shoulder surfing at the ATM because no one is directly behind you, sophisticated cybercriminals frequently snoop from afar. They may stare at your screen or keypad with high-powered binoculars, small cameras, or the cameras with their phone or tablet. They could be listening in as you read out credit card numbers or deliver personal Social Security number information over the phone.

4.9 How to avoid shoulder surfing?

- Take a physical checkup: If you are in public and you are asked to enter a password on a mobile device, sit upright with your backside against a wall. While using an ATM or PIN pad, use your body and the other hand to conceal the keys. If it is impossible to avoid providing credit card details or other sensitive information over the phone, walk away from others and talk quietly, hiding your lips with your hands. Protect your laptop, tablet, and smartphone with privacy protector screens. While this will not prevent thieves from monitoring your typing, it will restrict them from ever seeing what account you are logged into.
- Passwords should not be reused: This increases the likelihood of fraud occurring if the password is compromised. If a shoulder surfer obtains your password and email address, they may attempt it on dozens of sites and services. This may result in them acquiring access to more accounts of yours. Create complex passwords and store them securely using a password management system to make sure you never reused a password. Because the password manager automatically signs you in, there is nothing for shoulder surfers for seeing be sure to secure your master password well.
- Integrating technology: It makes absolutely no difference how safe your credentials are if they can be seen being typed. Utilize the face recognition or fingerprint authentication features offered by several apps on computers and mobile devices to gain access to your data without entering PINs or passwords. Pay with contactless payment applications and avoid entering PINs.
- Avoid using public Wi-Fi or sharing devices to access critical accounts: Apart from shoulder surfers, it's never a great idea to connect to private accounts or order online using free Wi-Fi or accessible devices. Open Wi-Fi networks are at risk of being hacked, allowing hackers to intercept the transmission and steal your information.
- Two-factor authentication should be used: Two-factor authentication requires an additional method of confirming your identity in addition to your password. For instance, your bank may send you a one-time login code that is valid for only a few minutes. Even if a thief obtains your password or PIN, they cannot access your bank account without entering the code. While two-factor authentication may slow down account access, securing critical data is worth the wait.

4.10 Man-in-the-middle (MITM) attack

In today's environment, the internet has surpassed all other aspects of our lives. Most of our daily routine is dependent on cellular networks and the internet. Social media is in the lead. Additionally, internet banking and online shopping have become easier to use every day and are not achievable without using an internet

connection.[35] With the emergence of the internet, hackers gained an easy target. Hackers primarily target businesses to try to steal confidential information, which can result in financial loss. MITM attack is the most popular type of attack in this scenario, making them the greatest danger to network security. The most typical scenario for such an operation includes victims, two users, and an attacker who is a third party. The attackers operate as a middleman between the two users, and the users are unsuspecting that a third party is participating. The assailant gains access to the communication channel and can send and receive messages between the two users. MITM attacks can be launched over a variety of communication channels, including GSM, Wi-Fi, UMTS, and Bluetooth. The attacker's purpose is to infect the specific data moving between endpoints, as well as the data's reliability and discretion. The attacker can compromise both discretion and veracity through eavesdropping and message manipulation via communication interference. Additionally, attackers have the potential to redirect, modify, or eliminate messages to prevent communication with one of the users, resulting in a compromise of availability.

Consider two individuals communicating with one another, Alex, and Banu. Eziz is the MITM attacker. Alex and Banu begin communicating and after an initial handshake authorize one another. However, if the authentication procedure is weak, Eziz can pose as another communication party to Alex and Banu. Eziz will begin connectivity for both Alex and Banu during the MITM attack. Alex's and Banu's messages will be routed through Eziz, who will pose as Banu then Alex as Banu. Alex and Banu will be unaware that Eziz has intercepted their messages. As a result, Eziz exploits Alex and Banu without their knowledge and gains important information.

MITM attacks based on spoofing

Spoofing is a method derived from spying. The attackers intercept interaction between two targets and take control of the data transmission between them because the victims are unaware. When a user connects with another user over an encrypted network and their connection is like the unknown MAC address, the server sends an address resolution protocol request, also known as an ARP request, to all users has access to the identical network. Users who have announced their Internet protocols only can answer predictably using their MAC address. However, when ARP cache is implemented dynamically, cache entrances can simply be fabricated using forgery ARP messages, and a reliable verification technique is unavailable. The MITM acts as a message filter, allowing the attacker to focus exclusively on the actual message that will be sent by another user. Additionally, this threat has a significant impact on the network because the message's content may contain sensitive and secret information. Numerous authors demonstrate the

state of the art in exploiting security flaws to conduct an error-free man-in-the-middle attack.

4.11 Defend yourself against a man-in-the-middle attack

Without taking the necessary measures, detecting a man-in-the-middle threat can be difficult. If you are not actively searching for signs that your communication has been monitored, a man-in-the-middle attack may go unreported until it is too late. While ensuring correct page authentication and applying some form of tamper detection are often the primary strategies for detecting a prospective attack, these procedures may require further post-attack forensic analysis.

Access Points with Strong WEP/WAP Encryption

Wireless access points with a powerful encryption mechanism prevent unauthorized users from accessing your networks just by being nearby. A vulnerability in the encryption technique may enable hackers to brute-force their own into a network and launch a man-in-the-middle attack. Stronger an encryption method, the more secure it is.

VPN (Virtual Private Network)

VPNs are used to create a safe environment within a LAN for sensitive data. They provide a secure communication subnet using key-based encryption. In this manner, when an attacker gains access to a shared network, he will be unable to decrypt the VPN traffic.

HTTPS should be made mandatory.

HTTPS enables secure communication over HTTP using the public-private key exchange. This stops an attacker from obtaining any benefit from the data he is sniffing. Websites should utilize HTTPS exclusively and should not supply HTTP alternatives. Users can install browser extensions to compel all queries to use HTTPS.

4.12 Social engineering

Information and system security, along with data security, are not only achievable with technological solutions in information systems. Because, behind these most secure technologies, there is a human being to consider. Because of changing behaviors at different times, humans, the weakest link in the security chain, might reveal numerous weaknesses in the security process. [33] As a result of detecting and exploiting these weaknesses, the term "social engineering" was introduced. It is possible to preserve information security by simultaneously considering the technological and social components of information protection. The use of information and information systems is increasingly felt in our daily lives. As the number of users of information systems grows, so does the number of malicious

users who wish to access users' private information by exploiting weaknesses in information systems. Individuals who build up and utilize information systems, recognizing the security vulnerabilities and the necessary steps to fill these gaps, will prevent both information systems from hacker attacks and users who use information systems from falling into dangerous user traps. Many different types of knowledge are created, edited, used, processed, and shared in business and everyday life. Security systems are used to keep vital information out of the hands of unauthorized individuals. In technical terms, it is nearly hard to bypass these security mechanisms in today's environment. However, when it comes to bypassing these systems, human vulnerabilities come into play.

Humans can be found at the head of even the most modern security systems. It can be considered a more successful means of penetrating systems in some circumstances by using the person(s) personal weaknesses. Because, when security is viewed as a structure made up of chainrings, the weakest link in the security system is human. The concept of social engineering was introduced by getting confident information through the exploitation of this weak link. Social engineering recognizes that humans are the weakest link in security and use a variety of ways and approaches to exploit this. The following concepts can be proposed for social engineering:

- It refers to all of the low-tech and human-based approaches used by attackers to obtain access to sensitive/important data and network systems via legitimate users.
- It is the skill of collecting knowledge that would be impossible to obtain under regular circumstances, with or without the help of technology.
- It is the skill of getting individuals to do things they would never do for a stranger.
- It is the method of obtaining information through deception rather than through the use of technology.

Some of the social engineering concepts that are mostly mentioned in the literature are given below:

1) Shoulder surfing- It is to observe and steal the password or other user information of someone who enters data using the keyboard.
2) Reverse social engineering- It is a social engineering procedure in which the victim meets an issue and seeks assistance from the attacker.
3) Dumpster diving- It is the task to search the target's trash for important information.
4) Identity theft- It is a type of fraud that involves the unauthorized use of another person's personal information.
5) Phishing- To obtain sensitive information, a fake e-mail, chat, or website is created and sent as a link to the victim's e-mail address by spoofing the real

system. To confirm user details, an email is sent from a bank or well-known institution. These fake sites are duplicates of the original sites that have been gathered in such a way that they appear to have all legal rights.

6) Vishing- Vishing, which is formed from the terms voice phishing, is a type of phishing in which a phone number is included instead of the fake link in the e-mail delivered to the victim and the information is updated by calling this number. As a result, the victim's information is obtained.
7) Impersonation- It is the behavior of the social engineer as an employee in an institution or as a user with system rights.

4.13 How can we act against social engineering?

The following are some of the steps that can be done both personally and organizationally against the strategies and practices exploited by social engineers:

- The document or documents thrown into the trash should be passed through the clippers or torn so that they cannot be read.
- Screen savers with password protection should be applied.
- Personal passwords should never be shared with anyone.
- It should be known that the most effective way to be taken against social engineering is the human-firewall, that is, the firewall to be implemented with their behavior in their own life.
- Information security testing, including social engineering attack tests, should be performed regularly, and it should be understood that with information technologies, the person who will cause the greatest harm is the person who does not know what he is doing.
- Personal and credit card information should not be given to anyone, especially on the phone, if the voice of the person making a request is not recognized and there is no reason to request it.

Chapter 5: Design and implementation of an informative android mobile application

The evolution of mobile learning techniques has recently attracted a lot of attention, with some studies pointing to that as the future of teaching. Such learning applications are one substitute for traditional methods of learning, but with additional benefits such as the ability to learn anywhere, at any time. As a result, it is critical to focus on this new trending technology to create a learning application to teach persons about user authentication methods and security risks.

5.1 The mobile application development lifecycle

Mobile application development is not an easy process. We need to pass through the main stages. The first stage of mobile application development is the planning stage. The first step in developing a mobile application is to understand why you are developing one. Beginning by asking the following questions:

Who is the mobile application's intended audience?

I developed this informative mobile application for those who want to learn about user authentication methods and security risks and test their knowledge.

What function does the application serve?

Mobile learning application. It provides comprehensive information about user authentication methods and security risks and multiple-choice questions based on given information.

Why is developing the application advantageous to you or your company?

To fulfill my master's thesis requirements and gain hands-on experience in developing Android mobile applications.

How do you intend to construct the application?

Android application development. Android is a multi-faceted open-source platform built for mobile devices. It is supported by Google and is controlled by the Open Handset Alliance. The alliance's purpose is to accelerate mobile computing innovation and provide consumers with richer, inexpensive, and better mobile experiences. Android is the platform for accomplishing this. Android is a Linux-based operating system that is mostly used to operate mobile devices like smartphones and tablet computers. An Android mobile application software program that is intended for usage on devices that run Google's Android operating system. A multitude of programming languages can be used to construct an Android mobile application.

5.2 Software programs used during Android application development

Android Studio Bumblebee version 2021.1.1

The official Integrated Development Environment (IDE) for building Android apps is Android Studio, and it includes everything you need to create high-quality Android applications. In addition, Android Studio Bumblebee, also defined as version 2021.1.1, is a significant release that offers several additional functionality and improvements.

Kotlin Programming Language

JetBrains created Kotlin, a comparatively recent programming language for modern multiplatform applications. Kotlin, rather than Java, is now extensively utilized for Android development. Kotlin is secure, compact, and worth reading and writing.

Figma

Figma is a graphic edit and user interface design program that runs on the web. It can be used for everything from wireframing websites to building mobile application interfaces, sketching designs, creating posts on social media, etc.

Firebase

Firebase is a Backend-as-a-Service provider (Baas). It offers many tools and resources to developers to help them create high-quality applications, expand their base of users, and profit. It is based on the infrastructure of Google.

5.3 Mobile application icon

Once we have the application planned, we can get into design. It is commonly known that "the first impression is the last impression," and we could not agree more when it comes to mobile application icons. The mobile application icon is the first thing a user notices when they launch the application. As a result, your application symbol must captivate, tell a storyline, and, more significantly, elicit certain feelings in the users, pique their interest, and entice them to learn about your application. It must visually express your brand and what you aim. In Figure 10, you can see the mobile application icon of the developed application.

As you can see, this application icon that I implemented looks like traffic lights that represent authentication procedures. As we know, authentication procedures have four main steps. The first step is that the claimant's identity is unknown, as the red color. The second one is the step of connection. The claimant demands the use of a service that needs information system authentication, such as yellow. The third step is authentication. The claimant is verified, and a session is started. The information system, such as the green color, supplies the user with the necessary

functionality. The fourth step is disconnection. When the user disconnects from the monitor, the status reverts to the first step.

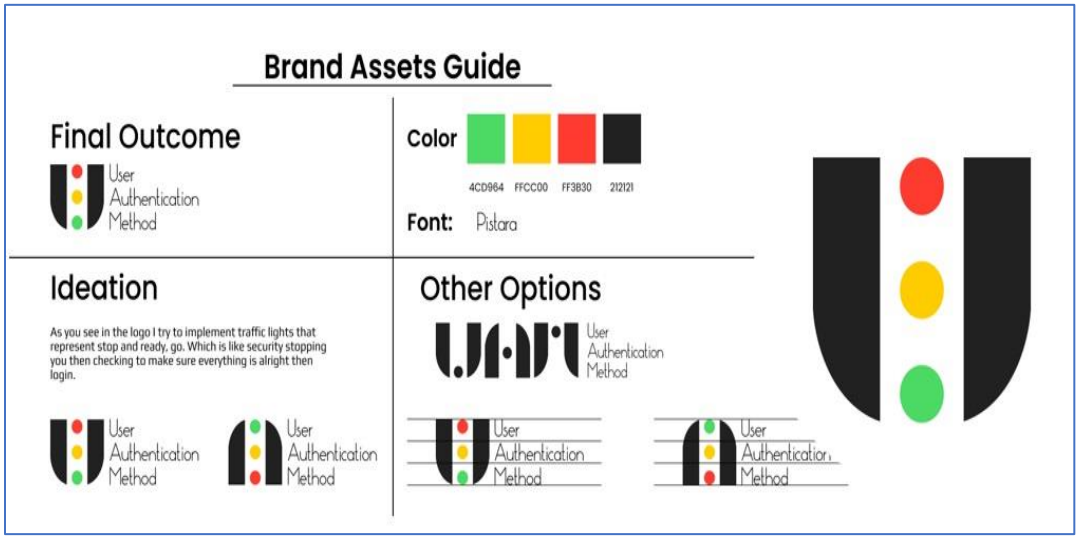


Figure 10- Mobile application icon

5.4 User interface (UI) for developed mobile application

The interface via which a computer, website, or program interacts with a human user is known as the user interface. The purpose of the successful user interface is to provide the user's experiences simple and intuitive, requiring as little effort on the user's behalf as possible to achieve the greatest desired result. The user interface is a link connecting users and applications. It contains the fundamental design features that must be perfect for someone to explore your application and make decisions. It is the ever-changing relationship that exists between a user and the system that they use. It encompasses the way your application interacts with users, as well as the general design and information presentation. There are numerous approaches to UI, but the fundamentals always include interaction from an application to the user and conversely. Structure, user manipulation, and communication are all important aspects of UI Design. That was one of the reasons why you must pay special attention to it. It is the main component of how your application is set up and functioning when your target audience visits it. In Figure 11, you can see the mobile User Interface of the developed application. As you can see the Figure 11 Mobile application user interface consists of 5 different components.

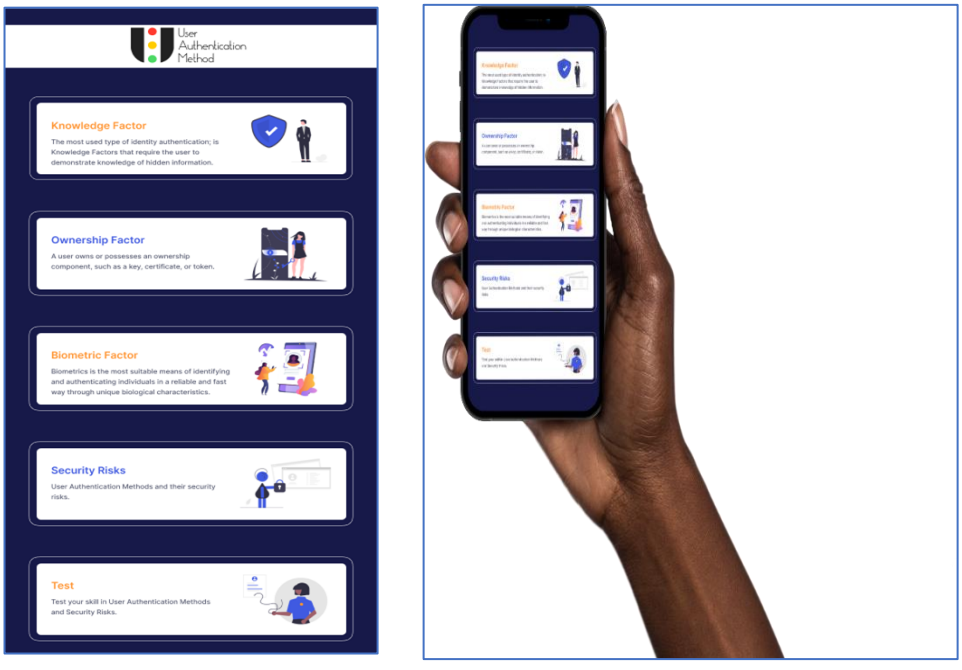


Figure 11- Mobile application user interface

a) Knowledge Factor

Users can read a brief description of the knowledge factor and see a small logo for it. After getting inside the knowledge factor, users can read comprehensive information about the knowledge factor. If users want to increase or decrease the text size, they can do it inside the settings icon. Figure 12 shows us the Knowledge factor's user interface.

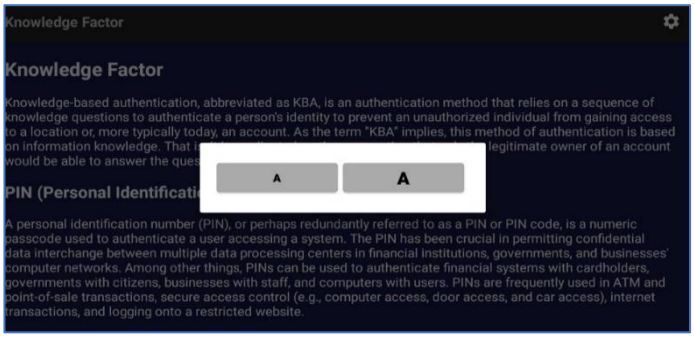


Figure 12- Knowledge factor user interface

b) Ownership Factor

Users can read a brief description of the ownership factor and see a small logo for it. After getting inside the ownership factor, users can read comprehensive information about the ownership factor-like tokens and OTPs. If users want to increase or decrease the text size, they can do it inside the settings icon.

c) Biometric Factor

Users can read a brief description of the biometric factor and see a small logo for it. After getting inside the biometric factor, users can read comprehensive information about the biometric factor-like Iris recognition, hand geometry, and fingerprints. If users want to increase or decrease the text size, they can do it inside the settings icon.

d) Security Risks

Users can read a brief description of the security risks and see a small logo for it. After getting inside the security risks, users can read comprehensive information about the security risks, like keylogging, a man in the middle attack, and brute-force attacks. If users want to increase or decrease the text size, they can do it inside the settings icon.

e) Test

Users can test their skills in user authentication methods and security risks. Each time 5 questions will appear randomly on the screen, after finishing solving questions, users need to submit the answers and they can learn true and wrong questions after submission. Figure 13 shows the Testing side user interface.

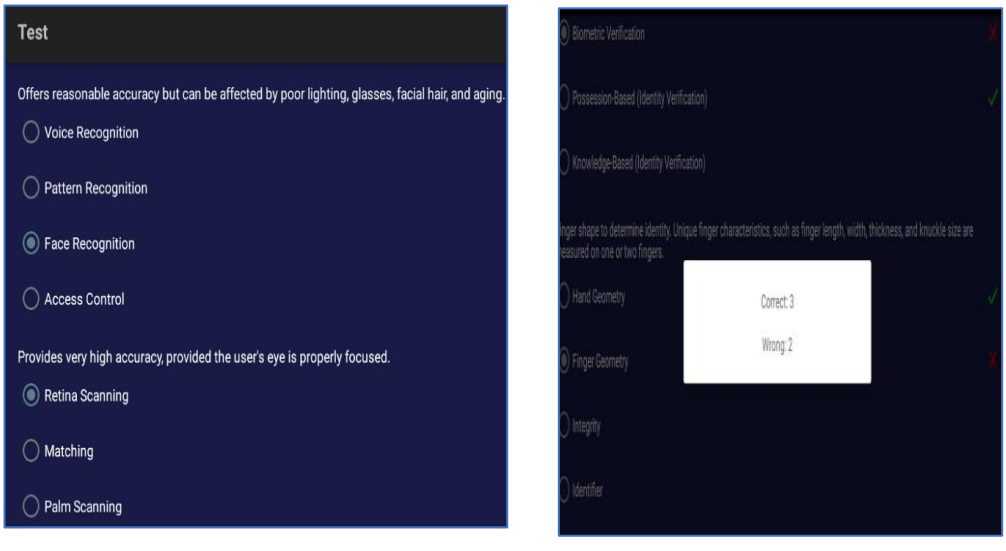


Figure 13- Test user interface.

5.5 Mobile application development. Back-end side.

As previously said, I used Firebase for the back-end of my application. Because of Firebase provides a variety of alternatives for developing a compact back-end side of a mobile application.

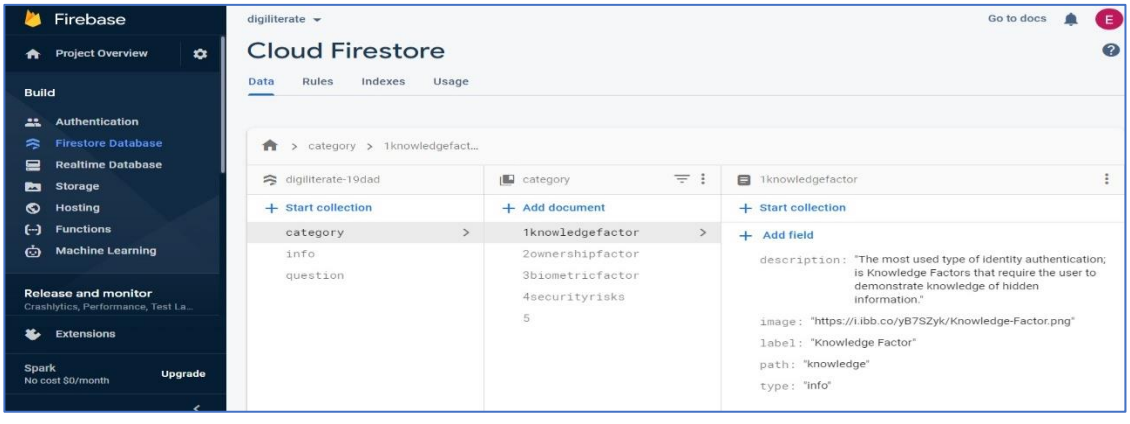


Figure 14- Application back-end side. Firebase category

You can see the Figure 14, that the application back-end consists of 3 different parts.

a. Category- 1knowledge factor, 2ownershipfactor, 3biometricfactor, 4securityrisks,5test. 1knowledgefactor combines inside description (string) about knowledge factor, image (link) the logo's image, label (string) name of the knowledge factor, path (string) of the information about knowledge factor, type (string) of the information. Figure 15 shows us the Firebase info side.

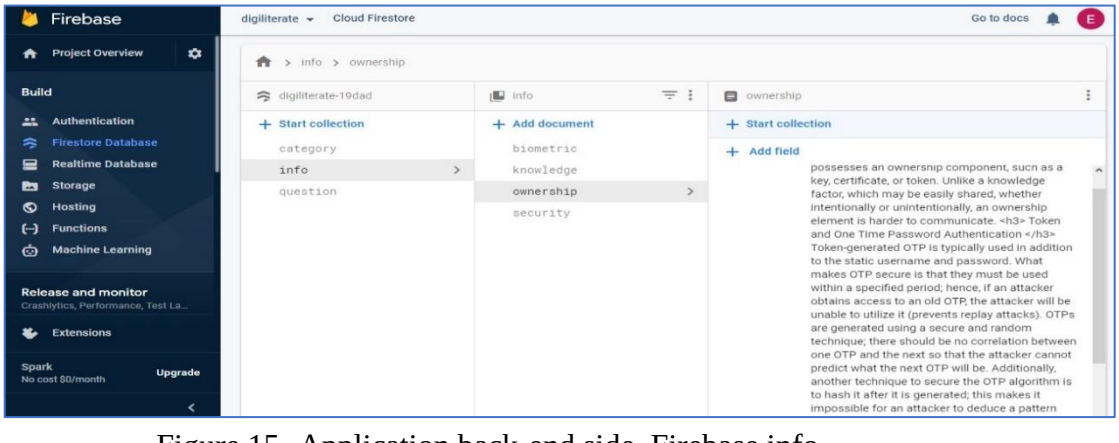


Figure 15- Application back-end side. Firebase info

b. Info-biometric, knowledge, ownership, security. This info application takes the content through the path. Biometrics consists of content (string) writing inside comprehensive information about the biometric factor. Also, Firebase accepts several HTML commands inside the container. Figure 16 shows us the Firebase's question side.

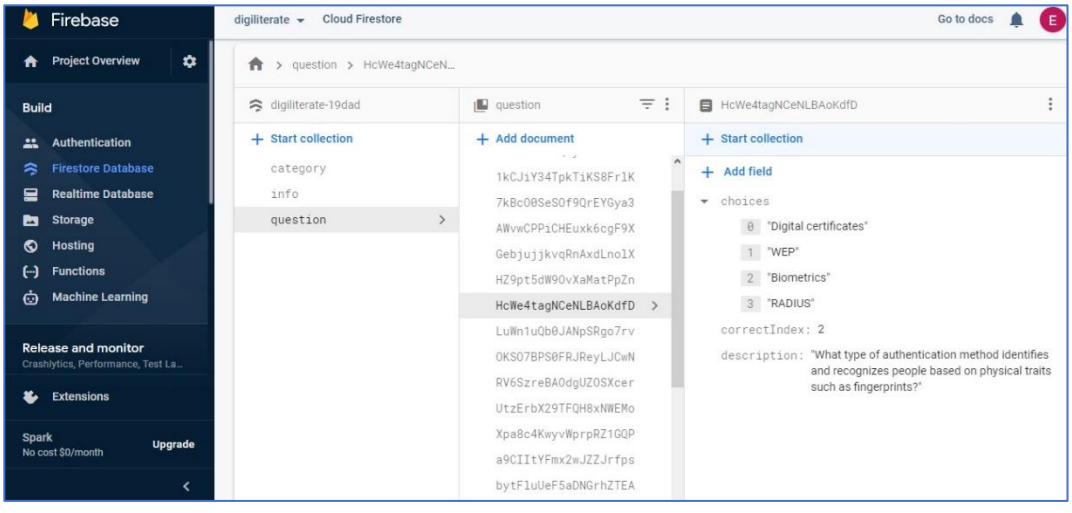


Figure 16- Application back-end side. Firebase question

c. Question-Test side of the application. I added more than 30 multiple-choice questions inside the questions. Every time, a user can solve five randomized questions. I gave the questions' identification automatically. Questions consist of choices (array) of 4 different answers, correctIndex (number) of the true answer to the question, and description (string) of the question's description.

5.6 Testing the developed android mobile application

I tested the mobile application with several Android emulators for PC, like BlueStacks X and NoxPlayer. The application worked perfectly, and all the functions of the applications worked correctly. After checking the application for android emulators, I send the developed application and related questions to android phone users. After that, I gather their feedbacks form them. The feedback and advice will help me develop a more compact android mobile application.

User Authentication Method I developed an informative android mobile application. Android mobile is an application that will help the users to understand the user authentication methods and security risks. Users can read and learn comprehensive information and they can test their skills with this application.				
Testers	**1**	**2**	**3**	**4**
How many years have you been using android?	+7 years	15 years	10 years	12 years
What is the model of your android mobile phone you are using?	Samsung S9+	Samsung Galaxy A41	Samsung Galaxy A52	Huawei P50 Pro
Do you like the application icon?	Yes	Yes	Yes	Yes
Does the application make you wait too long when it opens?	Not so much	No	No	No
Do you like the application user interface (UI)?	Fair enough	Yes	Fair enough	Medium
Are all the functions of the application working? (Settings, test, results).	Yes, all of them worked well	Yes	Yes	Yes
What are your feedbacks and advice for application?	Simple, user-friendly, I liked it.	Easy and practical to use	Simple, Add pictures and videos	User friendly

Table 9- Mobile application testers' feedback

Chapter 6: Conclusion and future work

I discovered several authentication methods and classified them into three groups using this thesis work: a knowledge factor, ownership factor, and biometric factor. Every authentication factor has its subcategories and groups. During my investigation, I found through different authentication systems with which I was uninformed.

When classifying authentication mechanisms, I discovered that many authors use various terms for the same topic. This outlined the value of defining the requirements for these groups. With these categories, it will be easier for users to understand where specific strategies fall. Many procedures are not yet extensively used, and there is little research available on them.

In the second part of the work, I investigated the main threats of user authentication methods in our daily life. There are many other forms of threats, such as brute force, keylogging, social engineering, shoulder surfing, dictionary attacks, and so on. I also investigated how can we prevent this threat in our daily life and found that we need to update our information and skills because it is a rapidly changing process.

I developed an informative android mobile application. Android mobile is an application that will help the users to understand the user authentication methods and security risks. Users can read and learn comprehensive information and they can test their skills with this application.

I tested the developed application for several emulators and among the different android phone users. I asked them several questions about the application, and after that, I collected their feedback and advice from them.

In the future business can use this application to train their employees about the security policies of the company and annual training for cybersecurity by adding some more functions inside the application like authentication. Also, we can develop the iOS and desktop versions of this application.

References

[1] Threat map checkpoint.: (https://threatmap.checkpoint.com), last viewed: 11.05.2022

[2] Report of McAfee.: (https://www.business-standard.com/article/technology/mcafee-report-says-cybercrime-to-cost-world-economy-over-1-trillion-120120700249_1.html), last viewed: 10.05.2022

[3] Ross Kelly.: Almost 90% of Cyber Attacks are Caused by Human Error or Behavior (https://chiefexecutive.net/almost-90-cyber-attacks-caused-human-error-behavior/), last viewed: 10.05.202

[4] Syed Zulkarnain Syed Idrus, Estelle Cherrier, Christophe Rosenberger, Jean-Jacques Schwartzmann.: A Review on Authentication Methods. *Australian Journal of Basic and Applied Sciences*, Vol.07., 2013, pp. 95-107.

[5] Riccardo Focardi.: Static Analysis of Authentication. *In: Aldini, A., Gorrieri, R., Martinelli, F. (eds) Foundations of Security Analysis and Design III. FOSAD. Lecture Notes in Computer Science,* Vol.3655., 2005, pp. 109-132.

[6] M.Samuel John, V.Siva Parvathi, M.Raja Sekhar, P.Raveendra Babu.: Enhancing security of Pass Points system using variable tolerance. *Int. J. of Advanced Networking and Applications,* Vol. 01., 2010, pp. 270-274.

[7] Rybnik, M., Panasiuk, P., & Saeed, K.: User Authentication with Keystroke Dynamics Using Fixed Text. *International Conference on Biometrics and Kansei Engineering*, 2009, pp. 70-75.

[8] Maple, C., Schetinin, V.: Using a Bayesian averaging model for estimating the reliability of decisions in multimodal biometrics. *First International Conference on Availability, Reliability, and Security (ARES'06),* Vol.07., 2006, pp. 935.

[9] Saxena, A.: Dynamic authentication: Need than a choice. *3rd IEEE/Create-Net International Conference on Communication System Software and Middleware, COMSWARE*, 2007, pp. 214-218.

[10] Nosseir, A., Connor, R., Revie, C., Terzis, S.: Question-based authentication using context data. *Proceedings of the 4th Nordic Conference on Human-Computer Interaction: Changing Roles. ACM International Conference Proceeding Series, 189, ACM Press, Oslo, Norway,* Vol.04., 2006, pp. 429-432.

[11] Bhattacharyya, D., Ranjan, R., Alisherov, F., Choi, M.: Biometric authentication: a review. *International Journal of u-and e-Service, Science and Technology,* Vol. 02., 2009, pp. 13-28.

[12] Patil, K. I., Shimpi, J.: A Graphical Password using Token, Biometric, Knowledge Based Authentication System for Mobile Devices. *International*

Journal of Innovative Technology and Exploring Engineering (IJITEE), Vol.02., 2013, pp. 155-157.

[13] Chen Wang, Yan Wang, Yingying Chen, Hongbo Lui, Jian Liu.: User authentication on mobile devices: Approaches, threats, and trends. *Computer Networks*, Vol.170., 2020, pp. 1-26.

[14] ISO 9564-1:2017. Financial services — Personal Identification Number (PIN) management and security — Part 1: Basic principles and requirements for PINs in card-based systems.: (https://www.iso.org/standard/68669.html), last viewed: 11.05.2022

[15] Pritchard, J.: What Is a Personal Identification Number (PIN)? (https://www.thebalance.com/pin-number-definition-and-explanation-315344), last viewed: 10.05.2022

[16] Conklin, Wm, Dietrich, Glenn, Walz, Diane.: Password-Based Authentication: A System Perspective. *Proceedings of the Hawaii International Conference on System Sciences,* Vol.37., 2004.

[17] Ishak, Mostafa.: A Comparative Study on Authentication Strategies of Various Online Banking Platforms. *Bachelor Thesis,* 2021, pp. 8-11.

[18] R. Shantha Selva Kumari, S.Viji.: Cued Click Points Password Authentication using Picture Grids. *International Journal of Computer Science and Network,* Vol.04., 2015, pp. 911-917.

[19] Wikipedia.: Biometrics (https://en.wikipedia.org/wiki/Biometrics), last viewed: 11.05.2022

[20] A. Ometov, S. Bezzateev.: Multi-factor authentication: A survey and challenges in V2X applications. *9th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT),* Vol. 09., 2017, pp. 129-136.

[21] Yao Ma, Jinjuan Feng.: Evaluating Usability of Three Authentication Methods in Web-Based Application. *Ninth International Conference on Software Engineering Research, Management and Applications,* Vol.09., 2011, pp. 81-88.

[22] Hamilton, Stephen, Carlisle, Martin, John.: A Global Look at Authentication. *Information Assurance and Security Workshop,* Vol.10., 2007, pp. 1-8.

[23] Christina Braz, Jean-Marc Robert.: Security and usability: the case of the user authentication methods. *Proceedings of the 18th Conference on l'Interaction Homme,* Vol.06., 2006, pp. 199-203

[24] Forget, Alain, Chiasson, Sonia, Biddle, Robert.: Shoulder-surfing resistance with eye-gaze entry in cued-recall graphical passwords. *Proceedings of the 28th international conference on Human factors in computing systems*, Vol.10., 2010.

[25] Riley. C, Heather. M, Buckner. K.: Fingers, veins, and the grey pound: accessibility of biometric technology. *Proceedings of the 14th European conference on Cognitive ergonomics*, Vol.07., 2007, pp. 149-152.

[26] Trewin S, C. Swart, L. Koved, J. Martino, K. Singh,S. Ben-David.: Biometric Authentication on a Mobile Device: A Study of User Effort, Error and Task Disruption. *Proceedings of the 28th Annual Computer Security Applications Conference*, 2012, pp. 159-168.

[27] Emanuel von Zezchwitz, Dunphy. P, De Luca. A.: Patterns in the wild: a field study of the usability of pattern and pin-based authentication on mobile devices. *Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services*, 2013, pp. 261-270.

[28] El-Abed, M., Giot, R., Hemery, B., & Rosenberger, C.: A study of users' acceptance and satisfaction of biometric systems. *44th Annual 2010 IEEE International Carnahan Conference on Security Technology*, 2010, pp. 170-178.

[29] Tari. F, Ant Ozok. A Holden. S. H.: A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords. *Proceedings of the second symposium on Usable privacy and security*, 2006, pp. 56-66.

[30] Schlöglhofer. R, Sametinger. J.: Secure and usable authentication on mobile devices. *Proceedings of the 10th International Conference on Advances in Mobile Computing & Multimedia*, 2012, pp. 257-262

[31] M.H. Barkadehi et al.: Authentication systems: A literature review and classification. *Telematics and Informatics*, Vol. 35., 2018, pp. 1491-1511.

[32] Robbi Rahim et al.: Keylogger Application to Monitoring Users Activity with Exact String Matching Algorithm (https://iopscience.iop.org/article/10.1088/1742-6596/954/1/012008/pdf), last viewed: 12.05.2022

[33] Happ, C., Melzer, A., Steffgen, G.: Trick with treat – reciprocity increases the willingness to communicate personal data. *Computers in Human Behavior*, 2016, pp. 372-377.

[34] Josué Matías García.: Usability Analysis of Authentication Techniques. *Master Thesis*, 2014, pp. 7-54.

List of figures

List of tables

List of Abbreviations

API	Application Programming Interface
ATM	Automated Teller Machine
ARP	Address Resolution Protocol
BMA	Bayesian Model Averaging
CCP	Cued Click Points
CPU	Central Processing Unit
FKP	Finger Knuckle Print
FTP	File Transfer Protocol
GUI	Graphical User Interface
GSM	Global System for Mobile Communications
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ID	Identification
IDE	Integrated Development Environment
ISO	International Standardization Organization
IT	Information Technology
IS	Information System
IP	Internet Protocol
LAN	Local Area Network
LCD	Liquid Crystal Display
MFA	Multi-Factor Authentication
MAC	Media Access Control address
MITM	Man-in-the-Middle attack
OTP	One Time Password
PIN	Personal Identification Number
PC	Personal Computer
RDP	Remote Desktop Protocol
SMS	Short Message Service