SIGNSAFE: SIGNATURE AUTHENTICITY SYSTEM FOR CONFIDENTIAL DOCUMENTS USING WEB-BASED SECURE ACCESS

NUR AZILA BINTI MUHAMMAD

UNIVERSITI SAINS ISLAM MALAYSIA

SIGNSAFE: SIGNATURE AUTHENTICITY SYSTEM FOR CONFIDENTIAL DOCUMENTS USING WEB-BASED SECURE ACCESS

NUR AZILA BINTI MUHAMMAD
(1190507)

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE BACHELOR OF COMPUTER SCIENCE WITH HONOURS (INFORMATION SECURITY AND ASSURANCE)

FACULTY OF SCIENCE AND TECHNOLOGY
UNIVERSITI SAINS ISLAM MALAYSIA

JUNE 2022

AUTHOR DECLARATION

I hereby declare that the work in this thesis is my own unless specified and duly acknowledged by quotation.

Date: 19th June 2022

Name: Nur Azila Binti Muhammad
Matric No.: 1190507

APPROVAL FOR SUBMISSION

I certify that this report entitled "**SIGNSAFE: SIGNATURE AUTHENTICITY SYSTEM FOR CONFIDENTIAL DOCUMENTS USING WEB-BASED SECURE ACCESS**" was prepared by **NUR AZILA BINTI MUHAMMAD** has met the required standard for submission in partial fulfilment of the requirements for the award of Bachelor of Computer Science with Honours (Information Security and Assurance).

Approved by,

DR. MURTADHA ARIF BIN SAHBUDIN
Faculty of Science and Technology
Universiti Sains Islam Malaysia
Date: 19th June 2022

ACKNOWLEDGMENT

In the name of Allah, all praises and thanks to Him, the Almighty, for showering His blessings during my research journey, allowing and helping me to overcome any hurdles and trials until I was able to complete this thesis proposal successfully.

Firstly, I would want to express my heartfelt gratitude to my research supervisor, Dr Murtadha Arif Bin Sahbudin, senior lecturer at Universiti Sains Islam Malaysia's Faculty of Science and Technology, for his invaluable guidance, inexhaustible patience, and compassion throughout my research development process. Working and studying under his direction was a wonderful honour and privilege. Undeniably, it has been challenging for me during the thesis journey, but it has been worthwhile, and I have learned a lot from him and my thesis coordinator, Dr Nurzi Juana Mohd Zaizi.

Furthermore, there are no words to express my deepest gratitude and appreciation to the pillar of strength in my life, my family, which includes both my parents and siblings, who have always been there for me to support me financially, morally, and physically, as well as for their love, understanding, prayers, care, and sacrifices in educating me until I can finish this research proposal work to the best of my ability.

Moreover, I might not be more thankful enough to all of my friends and colleagues for their great assistance as well as for always being available to help, encourage and motivate me when I need it. In addition, I would like to express my appreciation to all of my references researchers and everyone else who has participated in the successful completion of this project and making this endeavour a reality, whether directly or indirectly. May Allah’s blessings be upon each one of you. Thank you very much.

Last but not least, I hope that this thesis is one of the best and highest-quality works I have ever completed and that all of the knowledge and experiences I have gained along the way will benefit both others and myself.

ABSTRACT

Today, most governments and legal offices still do not use technology to accomplish some simple tasks like signing confidential documents because they still rely on face-to-face verification of the signatory's identity. Paper-based documents, such as birth certificates, driver's licences, and passports, are still required in some situations when electronic documents cannot adequately replace them. The existence of modern scanning and printing technologies, on the other hand, makes it simple to commit paper-based document fraud at a low cost. These issues are solved in this study by developing a web-based secure access authentication system which is SignSafe that uses a quick response code (QR code). Confidentiality, authentication, non-repudiation, and integrity are the core security goals of the SignSafe system. This QR code can be used to verify the document's integrity as well as the author's. Therefore, during the project's development, the Waterfall Model of the Software Development Life Cycle (SDLC) is being applied as the methodologies. PHP, HTML5, and phpMyAdmin will be used to develop the SignSafe system. As a result, it will have a positive impact on society and corporate environments by reducing fraud and forgery and assisting in the control of the signing process for contracts or private documents.

Keywords: paper-based documents, authentication, integrity, QR code, security.

ABSTRAK

Pada masa kini, kebanyakan kerajaan dan pejabat undang-undang masih tidak menggunakan teknologi untuk melaksanakan beberapa tugas mudah seperti menandatangani dokumen sulit kerana mereka masih bergantung pada pengesahan secara bersemuka bagi identiti penandatangan. Dokumen berasaskan kertas, seperti sijil kelahiran, lesen memandu dan pasport, masih diperlukan dalam beberapa situasi apabila dokumen elektronik tidak dapat menggantikan dengan secukupnya. Kewujudan teknologi pengimbasan dan percetakan moden, sebaliknya, memudahkan untuk melakukan penipuan dokumen berasaskan kertas dengan kos yang rendah. Isu-isu ini akan diselesaikan dalam kajian ini dengan membangunkan sistem pengesahan akses selamat berasaskan web iaitu SignSafe yang menggunakan kod respons pantas (kod QR). Kerahsiaan, pengesahan, bukan penolakan dan integriti ialah matlamat keselamatan teras sistem SignSafe. Kod QR ini boleh digunakan untuk mengesahkan integriti dokumen dan juga penandatangannya. Oleh itu, semasa pembangunan projek, model '*Waterfall'* yang merupakan salah satu daripada '*Software Development Life Cycle (SDLC)*' digunakan sebagai metodologi. PHP, HTML5 dan phpMyAdmin akan digunakan untuk membangunkan sistem SignSafe. Akibatnya, ia akan memberi kesan positif kepada masyarakat dan persekitaran korporat dengan mengurangkan penipuan dan pemalsuan serta membantu dalam kawalan proses menandatangani kontrak atau dokumen persendirian.

Kata Kunci: dokumen berasaskan kertas, pengesahan, integriti, kod QR, keselamatan.

TABLE OF CONTENT

CONTENT **PAGE**

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

SignSafe	Web-based secure access system for signature authenticity
QR Code	Quick response code
SDLC	Software Development Life Cycle
IoT	Internet of things
PHP	HyperText Preprocessor
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol
IA	Information Assurance
PC	Personal Computer
LAN	Local Area Network
PDF	Portable Document Format
DC	Document Cloud
AES	Advanced Electronic Signature
QES	Qualified Electronic Signature
SES	Simple Electronic Signature
IP	Internet Protocol
URL	Uniform Resource Locator
VCF	Virtual Contact File
CSS	Cascading Style Sheet
MP3	Moving Picture Experts Group (MPEG) Audio Layer 3
MP4	Moving Picture Expert Group (MPEG) Layer 4 Audio
PNG	Portable Network Graphics
JPEG	Joint Photographic Experts Group
Wi-Fi	Wireless Fidelity
API	Application Programming Interface
MySQL	Structured Query Language
JS	JavaScript
USIM	Universiti Sains Islam Malaysia

CHAPTER 1
INTRODUCTION

1.1 Research Background

In this digital age, the world is evolving at a breakneck speed. The majority of individuals nowadays use the Internet for various reasons and objectives, including communication, employment, leisure, entertainment, and recreation. Digital identities are increasingly important in modern life, particularly in the context of the Internet. These identities are used for various purposes, including opening a bank account, online shopping, and more. To create legally binding online signatures, reliable identification and authentication are required. Instead of using paper documents in real life, a new authentication method is used to utilize a digital signature verification system using web-based secure access.

Furthermore, since the paper produced from the plant is not being used, the term "eco-friendly" can be applied. People's acceptance of this authentication method is dependent on its interoperability and federation. From the user's perspective, using digital or online documents is more convenient than dealing with all the paper documents because various problems can be encountered. As a result, potential users show a high level of acceptance. The goal is to enable adaptive multi-factor authentication that may be used in various scenarios, ranging from commercial or Internet of things (IoT) systems to smart city environments. Different authentication entry points and a digital signature verification system are employed for easy integration and usefulness.

Creating a signature authenticity system for the confidential document using web-based secure access in this paper is to produce a list of digital files that may be used as documents with the same validity as paper documents. The fact is established by digital signature authentication, allowing the use of digital signature papers to be synced with paper-based documents in the future. The vulnerabilities in a printed confidential copy must be considered (Lax et al., 2015).

Generally, paper documents are readily displaced and damaged (Olexa & Grant, 2018). The procedures used to verify the authenticity of digital certificates appended to digital copies are known as digital signatures. The use of digital certificates is to ensure their authenticity and integrity. Indeed, a few studies have been done on digital signature authentication (Dhagat et al., 2016; Pereira et al., 2018; Adi et al., 2015). An online document accompanies the original documents. In conclusion, this method was created to demonstrate that an online document can be deemed a valid document in the future if digital signatures are used to validate it.

1.2 Problem Statement

Nowadays, many applications are now being developed to assist people in their daily routines. Authentication is necessary for gaining access to sensitive information on any application. This study proposes a signature authenticity system to validate user identity using web-based secure access. It is one of the technologies used to increase network security. It acts as a marking on data, ensuring that it is genuine.

Few individuals could have predicted that the emergence of the Internet would profoundly impact people's lives, as it has now. Transaction processing, bank account opening and even online shopping are just a few internet-based applications. As a result, all given services become more sensitive to their users' data, which is an integral component of their digital identities and must be handled securely.

Different service providers employ various techniques of user authentication to determine if the user is who he claims to be and if he is authorized to use a specific digital signature and identity. On the other hand, Figure 1.1 shows that the user is responsible for managing all of these distinct authentication systems.

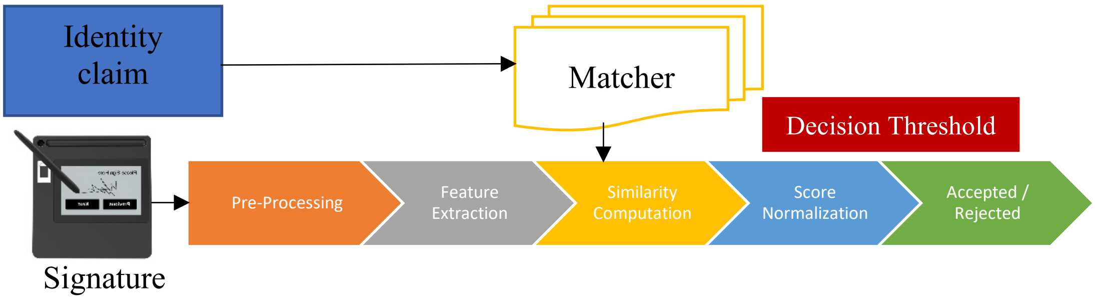


Figure 1.1: Dynamic signature authentication system

Moreover, obtaining a person's digitized signatures is no longer a difficulty. The majority of companies make collecting signatures from visitors and customers a requirement. Other sources of an ever-increasing quantity of candidate signatures include bank cheques and various application forms. However, due to the reasons stated previously, not all of them are high quality. Hence, automated authentication methods are being developed that can distinguish between the true and the fraudulent.

1.3 Research Questions

These are three research questions that should be examined in the research:

1. What is the present issue with digital signatures on confidential online documents?
2. How can web-based secure access be used to verify the signature authentication system?
3. How will the security features of the proposed web-based system be implemented?

1.4 Research Objectives

The following are the project's research objectives:

1. To examine the present issues related to the digital signatures on confidential online documents.
2. To create and develop web-based secure access which a QR code to authenticate the signature.
3. To implement authentication to protect the proposed web-based system against any violation.

1.5 Scope

The project is to develop and create a web-based system called SignSafe that can help verify and authenticate confidential documents' signatures using QR codes. The design should be able to receive, retain, keep and process the information from the user who will insert the signature into the system. In addition, the proposed system is supposed to assess the type of data submitted into the system and decide whether it can be accepted or needs to be rejected (fraudulent). The following are the project scopes:

- Implementation of a web-based user account
- Implementation of generating QR code signature
- Verification of authenticity of QR code signature
- Protection of data and information

1.6 Thesis Organization

This chapter includes background information and the description of the suggested idea, which covers the digital signature application to better understand the signature authenticity system for confidential online documents using web-based secure access. It contains detailed information about the problem statement, research questions and objectives. Lastly, this chapter also explains the project's scope of the proposed idea for the user of the system to examine.

CHAPTER 2
LITERATURE REVIEW

2.1 Overview

In the context of the secure access technique, some research has been done on signature verification systems. Here, we will go over the web-based concepts that can secure confidential documents using a signature authenticity system. Besides, we will discuss the existing concept system that is similar for maintaining the confidentiality and the quality of all the important documents. All qualifications, conceptual framework, and features proposed in this project will be based on the findings of all studies conducted throughout this literature review. Finally, we will present the current implementation of a signature authenticity system for confidential documents using a web-based secure access method which is a QR code.

2.2 Digital Signature

Traditional handwritten signatures are losing legal acceptability in favour of digital signatures nowadays. A digital signature uses public-key cryptography to ensure that a confidential document's authenticity is protected. To address the security issues of authentication, confidentiality, and integrity in the system, a digital signature has been developed. It is a pattern that is based on the message being signed and includes information that is unique to the signer (Kuacharoen, 2011). Using a digital signature for a secure authentication method will almost eliminate the possibility of some devices being hacked. The digital signature verifies that the message or command being sent originates from a legitimate source.

Digital signatures are becoming more widely utilised in e-commerce, banking, and software systems as a reliable way to ensure message validity and non-repudiation. All of these industries have a diverse set of computing equipment connected by a network, which necessitates a robust authentication mechanism to ensure the authenticity of sent data. Researchers have proposed a slew of digital signature solutions to address security flaws (Gupta et al.; Sinha et al.; Perti et al., 2020). The RSA algorithm, Digital Signature algorithm, and Elliptic Curve Digital Signature algorithm are the three approaches that make up the Digital Signature standard. Forging a digital signature is computationally impossible.

2.2.1 Authenticity

One of the five pillars of information assurance (IA) is authenticity. Integrity, availability, confidentiality, and non-repudiation are the other four principles. Authentication is a technique in digital systems that ensures and confirms a user's identity. Authentication systems are security procedures that are used to secure data and systems by requiring additional input from users. For instance, multiple-factor authentication is one of the examples that is used to describe authenticity in a system. We can increase data security and avoid potential breaches by using authentication. When a system requires multi-factor authentication to access it, it is less prone to security vulnerabilities like weak passwords or phishing threats. Authentication solutions are great for a system that needs to protect sensitive data or information that require secure user accounts.

2.2.2 Integrity

Methods of guaranteeing that data or information are true, correct, and safe from unauthorised user modification is referred to as integrity in the context of computer systems. Under various adversarial conditions, a system's integrity refers to its ability to perform accurately according to its original specification. In other words, it is the property of a system when it performs its intended purpose without being harmed, whether intentionally or accidentally.

2.3 Existing System

In this part, we will talk about the existing secure access system using signature verification over any hardware or software. We will learn about the system's history and investigate the concept's primary difficulties and previous research findings.

Due to the rapid expansion and diffusion of digital technologies and the internet in this industry, the act of gathering, analysing, storing, and altering personal data or confidential documents has never been easier. Personal data is constantly exchanged and kept in multiple databases as the use of technology has become the norm in society. "Personal information documents have become the essential fuel on which modern business and government operate (Perri,1998). This method of authentication is becoming an increasingly vital option in our networking culture. It has been a current trend to use physiological or behavioural attributes for human authentication alias biometric authentication. Nowadays, biometrics offers greater security than other authentication techniques that rely on the information that we own like a password and an ID card. The signature authentication system has been a hot topic in biometrics because of its widespread societal and legal recognition.

There are various types of signature verification systems using secure access hardware or software that have been presented to society to address this crucial issue. Figure 2.1 illustrates a variety of mediums that had been used for signature authenticity systems using secure access including Smart Card, Tablet PC and Adobe Acrobat DC.

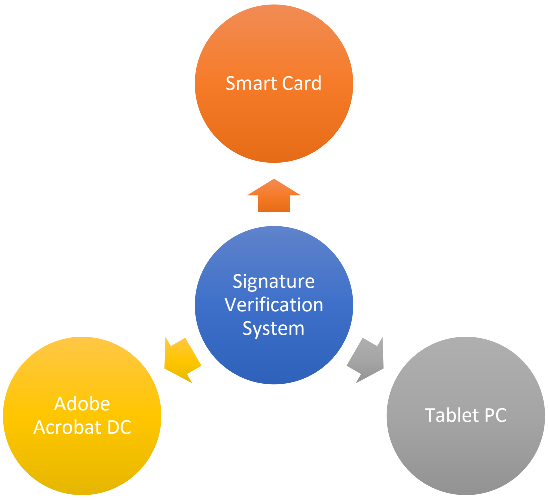


Figure 2.1: Existing signature verification system

2.3.1 Private Key on a Smart Card

The management of the signature verification system offered services that can gains sensitivity in the face of users' data, which is a part of their digital identities and thus must be kept secure. A digital identity's access and use must be limited to the user it represents only. On the other hand, Figure 2.2 indicates that the authentication method gives results in a wide range of confidence levels for the digital identities presented. As a result, the system's usability and security are constrained (Pohlmann, 2017).

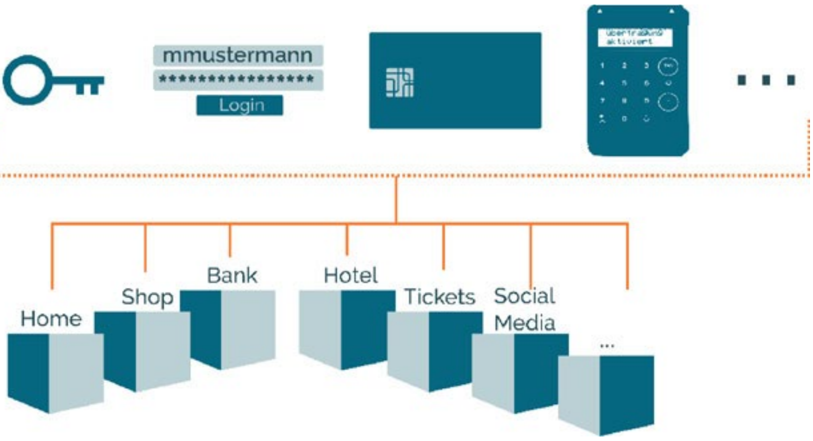


Figure 2.2: Overview of the authentication method (Manaras, 2017)

With the proliferation of commercial Internet services, a service provider must be able to trust the information provided by its users. As a result, it must be checked that the information is correct to avoid identity theft and secure from all unwanted things happening. Also, it can keep the data documents confidential. Figure 2.3 shows by using this method provide extremely reliable identifying procedures that rely on the smart card. It offers a technique in which the user is identified via a private key while showing the smart card and certain built-in security features in the application, in addition to electronically reading the information stored on the smart card. Several service providers rely on users' personal information to perform their services (Hertlein, 2017).

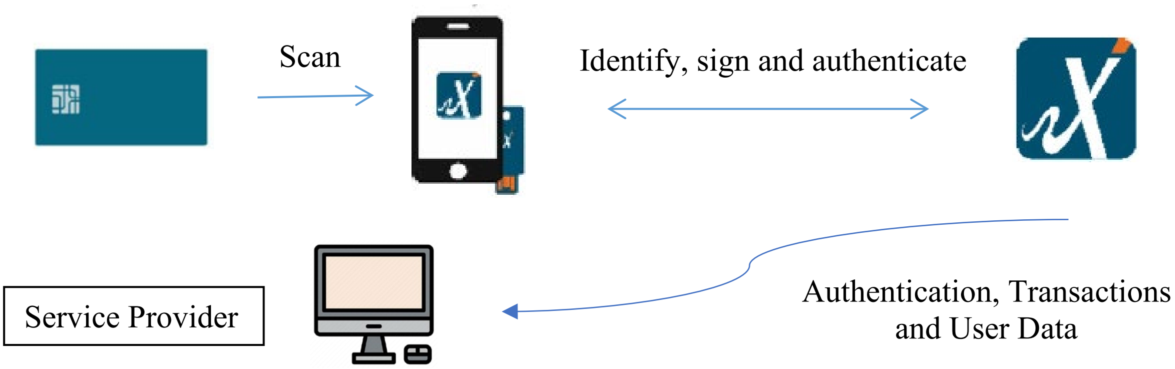

Scan
Identify, sign and authenticate
Service Provider
Authentication, Transactions and User Data

Figure 2.3: Authentication process using Smart Card

2.3.2 Signature Verification Secure Access System over Tablet PC

Tablet PC is one of the portable device examples that can capture signature signals at a low cost. This medium includes the acceptance of a written signature as proof of identity on a social and legal level that has opened up a slew of new possibilities. It is a Web-based secure access prototype with signature verification that is configurable and scalable. The architecture of this method is easily adaptable to large-scale databases and many sorts of sensors. Network-based signature verification that provides security and anonymity are also included (Alonso-Fernandez & Fierrez-Aguilar, 2015).

The increased popularity of low-cost portable devices like tablet PCs and mobile phones that are capable of accepting signature signals are driving up demand for signature-based authentication applications. This technique captures signatures using a Tablet PC, but it may simply be adapted to other signature capture devices. The verification is handled via a signature verification server. The signature verification server will communicate with the web server that uses the Hypertext Transfer Protocol (HTTP) to connect with the user terminal across the network. As shown in Figure 2.4, the user terminal is installed on a Tablet PC, while the web server and signature verification server are both on a regular PC that will connect via the Local Area Network (LAN). Any portable devices that are capable of taking online signatures can be used as a user terminal. It is said to be scalable because it can utilise strong servers that can handle several transactions simultaneously, not only HTTP transactions but any other secure or unsecured protocol as well.

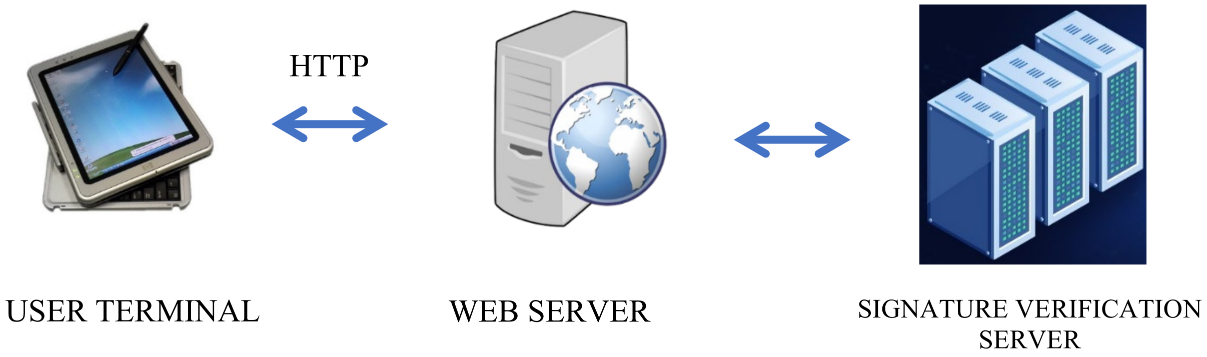


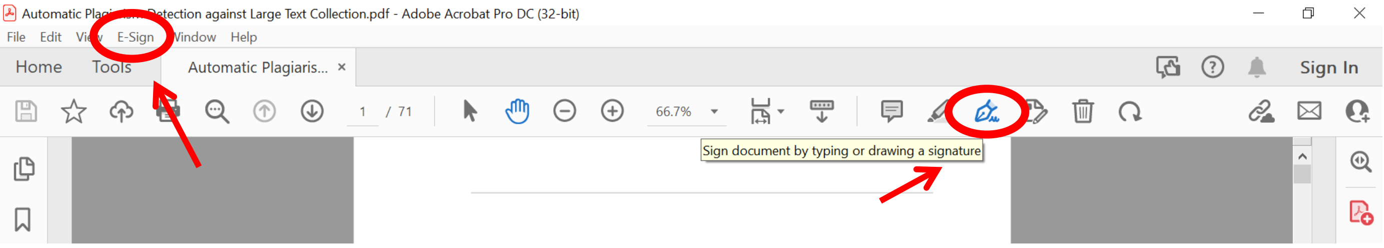
Figure 2.4: The architecture of the implemented technique

2.3.3 Digital Signatures Only with Trusted Applications

These days, electronic documents, are encouraged for many purposes, rather than paper documents, by this worldwide trend. However, while electronic documents decrease waste, they raise trust issues. It is difficult to identify changes to electronic documents. Furthermore, determining who updated the paper is challenging. To address these issues, several document processors employ digital signatures. The integrity of an electronic document can be verified, as well as the signer and time of sign. As a result, many document processors have digital signature functionality.

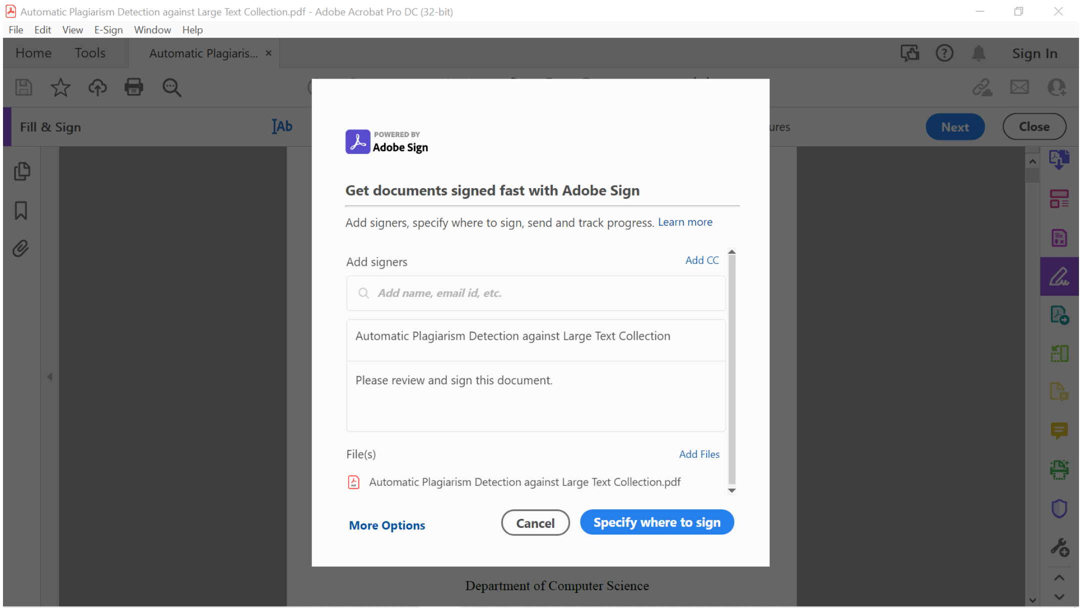
Adobe Systems created the PDF (Portable Document Format) standard in 1993 is one of the trusted applications and most widely used electronic document formats nowadays. Digital signatures for PDF documents are available in a variety of PDF software packages like Adobe Acrobat DC. However, there hasn't been much research into the security of the digital signatures that have been applied. In Adobe Acrobat DC, the signature dictionary stores information needed for digital signature services such as signatures, contents, and certificates. As a result, while creating or verifying digital signatures, PDF applications should use the signature dictionary (Nur, Adams & Brailsford, 2016).

Figure 2.5 and Figure 2.6 is the example of buttons with applied labels that can be used to add a signature. These functions will be useful to the users as they will pop up some text showing what will happen next when the user clicks the button.


Automatic Plagiarism Detection against Large Text Collection.pdf - Adobe Acrobat Pro DC (32-bit)
File Edit View E-Sign Window Help
Home Tools Automatic Plagiaris... ×
Sign In
1 / 71
66.7%

Sign document by typing or drawing a signature

Figure 2.5: Menu bar and Toolbar to add signature


Automatic Plagiarism Detection against Large Text Collection.pdf - Adobe Acrobat Pro DC (32-bit)
File Edit View E-Sign Window Help
Home Tools Automatic Plagiaris... ×
Sign In
Fill & Sign
Next
Close
POWERED BY
Adobe Sign

Get documents signed fast with Adobe Sign

Add signers, specify where to sign, send and track progress. Learn more

Add signers Add CC

Add name, email id, etc.

Automatic Plagiarism Detection against Large Text Collection

Please review and sign this document.

File(s) Add Files

Automatic Plagiarism Detection against Large Text Collection.pdf

More Options
Cancel
Specify where to sign

Department of Computer Science

Figure 2.6: Adobe Sign window to request e-signatures

2.3.4 Comparison of Digital Signatures versus Ink on Paper Signatures

Table 2.1 shows the comparison between digital and manual signatures.

Table 2.1: Comparison of Digital Signatures versus Ink on Paper Signatures

Comparison	Digital Signature	E-Signature	Ink on Paper Signature
Definition	**Public-key cryptography to verify the authenticity**	**An electronic signature, also known as an online signature, is a fast**	**Any signature is made when a person physically marks any**

	and integrity of a message. Most cryptographic protocol suites provide digital signatures as a standard feature.	**technique to acquire assent or approval for a digital document or form. It may replace a handwritten signature in almost any process because it is secure and verified.**	**hard copy or document with a pen or other writing equipment with the purpose to sign the record and also known as a wet signature.**
Identity	**The Certification Authority issues a digital certificate that connects the physical and online identities.**	**The signatory must prove that the document was signed by him or her and that it has not been tampered with in any way.**	**A signature server is used to identify the signatory because each person's signature is unique.**
Types / Examples	❖ **Advanced electronic signature (AES)** ❖ **Qualified electronic signature (QES)** ❖ **Simple electronic signature (SES)**	➢ **DocuSign** ➢ **AdobeSign** ➢ **AssureSign** ➢ **EverSign** ➢ **HelloSign** ➢ **SignEasy** ➢ **SignNow**	**A signature using pen or ink that is considered "wet".**
Security	**A strong encryption method such as multi-factor authentication.**	**Limited security features.**	**No tampering or complete security is possible.**
Tracking	✓ **IP Address** ✓ **Date & time stamps.**	**Cannot be tracked or validated the signature.**	**Cannot be tracked the location and time of the document signed.**
Evidence	• **Name** • **Date & Time** • **Location** • **IP Address**	**Difficult to prove the document's signer and must be kept securely.**	**A witness is important when signing the documents.**
Filling Time	**Directly (Instant) at anywhere and anytime.**	**Directly (Instant) at anywhere and anytime.**	**Some period of time like 2-3 weeks needed.**

Source: Lennard and Kok Leong, 2018

2.4 QR Code

The Quick Response code shortened as 'QR code,' is a sort of two-dimensional barcode. that allows to quickly access and read information. Many systematic kinds of research had been done on how information is organised and stored by arranging QR codes in a 2D matrix, as well as the columns and rows of the matrix that have been conducted. The matrix represents a storage area for data containing visible elements of QR codes in black and white as shown in Figure 2.7. QR codes are utilised in domains where text information is transferred, such as emails, phone numbers, websites, and other text files. Scanning the QR code, which is subsequently deciphered by the QR code reader is how this is done (Kr et al. & Sagar et al., 2014).

Figure 2.7: The example of a QR code

2.4.1 Type of QR Code

There are various kinds of QR codes which are:

- URL QR code – Any website or landing page can be converted (static or dynamic)
- vCard QR code – Can be applied on business cards, resumes, websites or email signatures (dynamic)
- File QR code – MP4, PDF, PNG or JPEG (dynamic)
- Social media QR code – Links to all social media platforms (dynamic)
- H5 editor QR code – A straight web page of our own (dynamic)
- Wi-Fi QR code – Connect to wi-fi without typing the password (static)
- App stores QR code – Redirect to Apple App Store, Amazon App Store or Google Play Store to install the application (dynamic)

- Multi-URL QR code – Redirects to a webpage based on location, time, number of scans and language settings (dynamic)
- MP3 QR code – Podcast, MP3 and soundtrack can be converted (dynamic)
- Individual QR code – Facebook, Pinterest, Twitter, YouTube, Instagram (static and dynamic)
- Email QR code – Leverage email marketing address, giving a sense of digitalization (dynamic)
- Text QR code – Display a combination of simple text consisting of numbers, words and special characters, does not require an internet connection (static)

2.4.2 QR Code Application

QR codes can be applied in many ways also in anywhere and anytime. There are some examples of QR code applications in our daily life. For example, in the traffic field, a QR code can be applied as passenger control such as before entering the bus, we need to scan our ticket first. So that, it will make the process smoother, passengers can easily choose where to sit on the bus and also it will not consume a lot of time to wait for one another. Other than that, it also can be applied in the medical field like scanning for the prescription.

Next, in the leisure field, admission control and mobile membership card (services) are also possible with QR code applications such as at entrance gates or the counter. Lastly, QR codes also can be applied in real-time process management like packaging, picking products and stocktaking (inventory checking). Hence, it will improve work efficiency as QR codes can prevent picking up any errors, and achieve traceability, more reliability and quicker (Vall, 2022).

2.5 Web-Based Development Tools

The development tools chosen are dictated by the needs of a web-based system. In this web-based signature authenticity system, PHP, HTML5, database, QR Code generator and QR Code Scanner will be used.

2.5.1 PHP

PHP is an open-source and strong web programming language. The purpose of PHP is to create a dynamic and appealing web-based system that meets the needs of the user. In today's business world, PHP projects are in high demand since they are more appealing, speedier, and have a better appearance and feel. In comparison to Java/.Net, PHP programmes are simple to construct and can even be modified by the user. With the smallest amount of source code, it can create the best online web-based application. PHP-based projects are very user-friendly for both programming and database processing. The web server will translate the PHP code into HTML or another viewable format.

2.5.2 HTML5

HTML5 is the web development standard that is supported by all modern browsers. A collection of linked technologies using HTML, JavaScript, and CSS to construct a high-performance web-based system without the use of plugins and with fewer service calls. With good reason, HTML5 is one of the trendiest topics in web development. It is not only the most recent version of the web's markup language, but it also establishes a new standard for constructing online web-based applications. HTML5 introduces several new components that can be used to create sophisticated internet applications, as well as a set of JavaScript APIs that browsers must support. A web page's content and layout are organised using HTML5 (Wright, 2020).

2.5.3 Database

The chosen database of signature authenticity system for confidential documents using web-based secure access is phpMyAdmin. phpMyAdmin is a free PHP-based software tool for remotely managing MySQL databases. It is an open-source web-based database client that makes working with MySQL and application databases much easier. phpMyAdmin is also a MySQL and MariaDB administration tool that can handle a wide range of tasks. The user interface can be used to manage common operations including databases, tables, columns, relations, indexes, users, and permissions while also running SQL commands directly.

2.5.4 QR Code Generator

QR codes may hold a variety of data types and have a large storage capacity (Furht, 2011). The QR code's main structure is made up of a three-squares finder pattern that represents the timing pattern. This square is made up of horizontal and vertical lines of black and white cells. It can be used to determine a symbol's coordinates as well as to ensure that a symbol is stable and capable of delivering information without any alterations. While the quiet zone is the space surrounding the QR code's structure for reading the QR code. It has four or more cells in most cases as shown in Figure 2.8 (Ammar & Alaa, 2020).

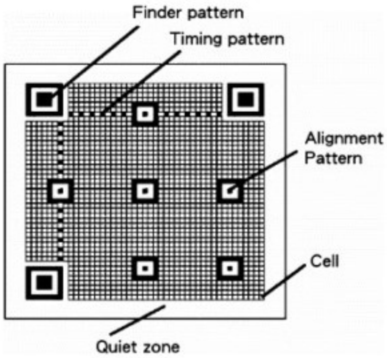


Figure 2.8: The components of a QR code's structure (Ammar & Alaa, 2020)

2.5.5 QR Code Scanner

A QR code scanner, also known as a QR code reader, is a scanning device that can read QR codes. QR code scanners are incorporated into the cameras of most smartphones and tablets. However, a webcam is required to read the QR code from a computer. It has to point the camera at a QR code and scan to read it. When scanning a QR code, we will immediately gain access to the information it contains. Besides, the QR code reader can do things like open the website URL in the browser. Other options include adding the business card to the smartphone's contact list, connecting to wireless, or doing any other activity associated with the QR code.

2.6 Summary

This chapter outlines the proposed system's overview and web-based development tools. Furthermore, this chapter also evaluates numerous existing systems and a comparison table between a digital signature and a paper signature.

CHAPTER 3
METHODOLOGIES

3.1 Overview

This chapter explains the method employed in this thesis. To build a system, we need a good method. To fulfil the goals, this proposal employs a Waterfall methodology. The development of a web-based signature authenticity system for confidential documents using QR codes can be divided into 5 phases that are depicted on a Waterfall Life Cycle diagram which are analysis, design, implementation, testing and maintenance. This methodology must follow each step accordingly. The reasoning for the technique, as well as the research methods that were chosen, are presented in this chapter. Thus, the developer will then be able to meet all of the requirements and provide a high-quality system.

3.2 Research Methodology

One of the most important aspects of creating a system is the methodologies. Another word for software development technique is software development life cycle (SDLC). It is a series of processes in the development process for software development and lifecycle control. This SDLC method will make the process of developing an efficient, cost-effective, and high-quality system much easier. SDLCs come in a variety of types, including waterfall, agile, and more (Aroral, 2021). The proposed web-based signature authentication system will be developed using the waterfall methodology as a Software Development Life Cycle (SDLC). It is one of the most straightforward and manageable approaches. It's also a project management technique that adheres to a sequential design approach like before moving on to the next level, one must complete the previous one as illustrated in Figure 3.1. It will repeat each phase until a perfect cycle is achieved. Small projects with precisely specified requirements benefit from the waterfall paradigm (Aroral, 2021).

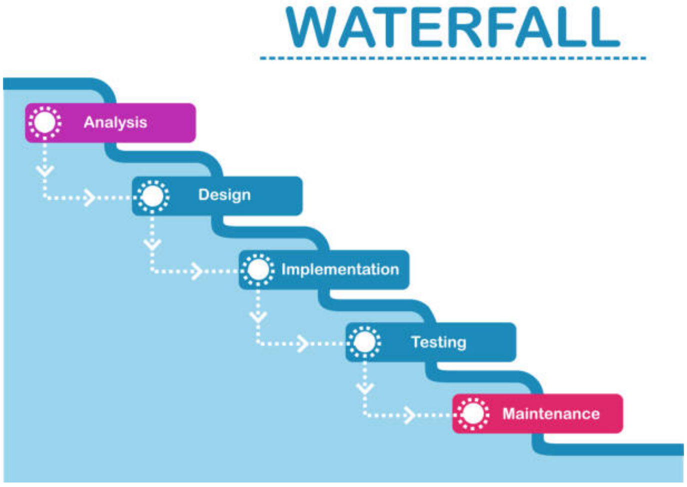


Figure 3.1: Phases of Waterfall model (nTask, 2021)

3.2.1 Requirement Analysis

The waterfall model attempts to evaluate needs from the start and did not allow the implementation to begin until all requirements have been fully understood, documented, and substantially fixed (Demirel & Das, 2018). This is when the clients and developers agree on product needs and features, according to Modi et al; 2017. In addition, some web research was carried out to acquire information about the suggested system.

Figure 3.2 indicates the signature authenticity system environment that will be applied along with the development of the proposed project.

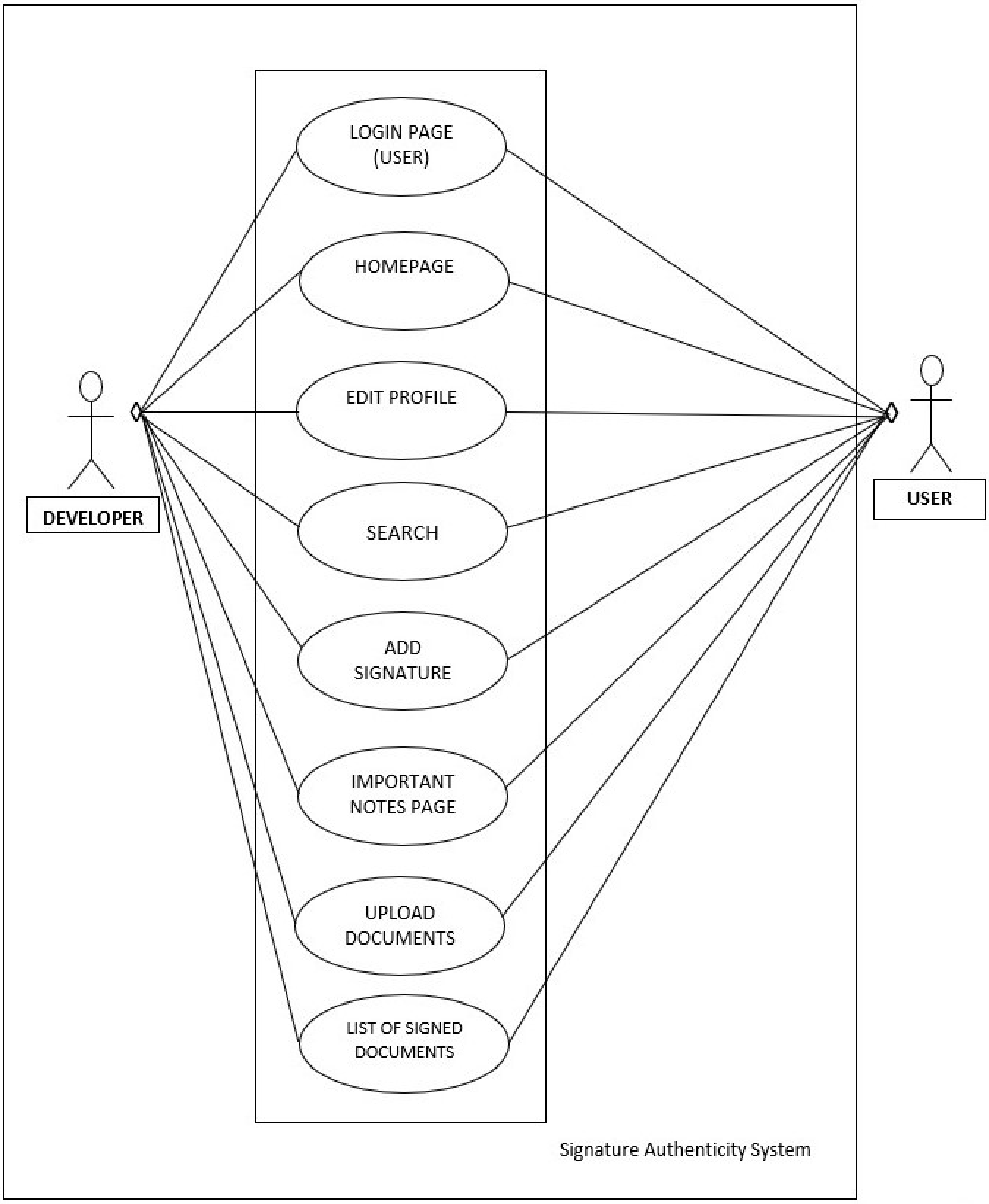


Figure 3.2: Signature authenticity system environment

Table 3.1 indicates use cases of project development for the SignSafe system.

Table 3.1: Use case table

Use Case	**1. Use Case: User Login System** The developer builds and manages the Signature Authenticity System for the user. The users of the system will access the system through browsers because it is a web-based secure access system. Users need to sign up for new users and login into the application. **2. Use Case: Homepage** The developer will build a user-friendly interface for the homepage to let the user experience a much easier system for doing their tasks. **3. Use Case: Edit Profile (User)** The user of the system will access the web-based system, log in to the user interface and edit the profile. **4. Use Case: Search Function** The developer will build a search bar to make the process of searching documents that have been signed or not more easily for the user. The categorized section will be built based on the type of item. **5. Use Case: Add Signature Function** The developer will build an ‘add signature’ website to make the process of adding the sign more arranged, need and easy for the user to use. **6. Use Case: Important Notes** The developer will prepare a section for the user to list out any important contact or notes to have more detailed information about the confidential documents. A secured function will be applied in this section to protect the confidentiality of the data and documents. **7. Use Case: Uploaded Documents Function** The user can upload the documents that need to be signed and save them there for personal use. **8. Use Case: List of Signed Documents** The developer will manage an interface to list out and show all the signed or unsigned documents to ease the user.
Actor	1. Developer 2. User

3.2.2 System Design

In system design, the selection of the database conceptual schema, software architecture design, and logical diagram design will all take place. This phase concludes with a description of how the system should be built and implemented (Kramer, 2018). The system's requirements will be converted into a detailed design. To give the system a clean appearance, they have all been developed in a straightforward and efficient design style. When it comes to system design, it is preferable to display only the information that is required on each page and keep the pages simple, rather than cluttering the interface with complex labelling and buttons (Lupanda & Van-Rensburg, 2021).

Figure 3.3 illustrates the signature authenticity system flowchart that will be applied throughout the development process of the proposed project.

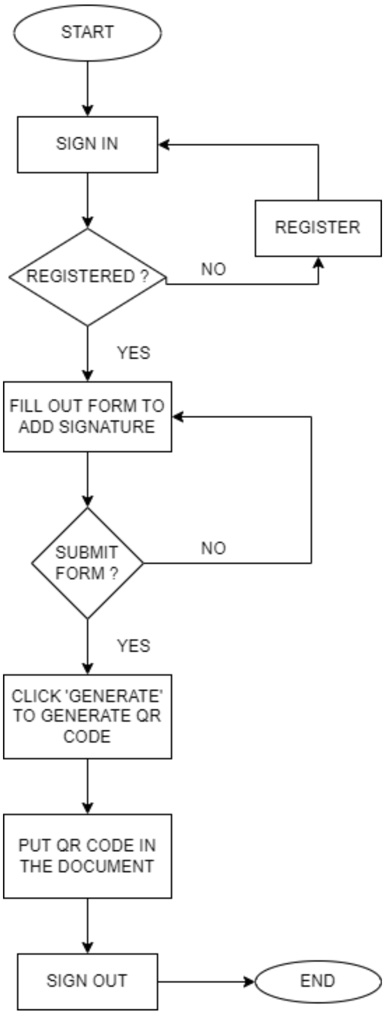

START
SIGN IN
REGISTER
REGISTERED ?
NO
YES
FILL OUT FORM TO ADD SIGNATURE
SUBMIT FORM ?
NO
YES
CLICK 'GENERATE' TO GENERATE QR CODE
PUT QR CODE IN THE DOCUMENT
SIGN OUT
END

Figure 3.3: Flowchart of signature authenticity system

3.2.3 System Implementation

This system implementation stage entails turning all of the designs into machine-readable code. Future improvements, as well as system dependability, were considered during the coding phase. A rudimentary prototype was created during this phase to offer a general idea of how the system worked. Any button or function configuration is decentralised and continually examined to ensure that the purpose is met. This is the most time-consuming step of the Waterfall life cycle process (Kramer, 2018). The programming language chosen is based on the needs of a web-based application.

3.2.4 System Testing

The system testing step necessitates the real testing and assessment of the software solutions created to meet the original specifications. This testing will cover the entire system and ensure that it meets the standards. A usability test will be conducted to determine whether the generated project is usable. During this phase, bugs and device vulnerabilities are found, fixed, and improved. Functional testing, sometimes known as black-box testing, was utilized as the testing approach. The system will also be examined and tested against the required standards, which were established early on. The goal of validation is to ensure that the system meets its objectives by performing as expected in terms of performance and functionality.

3.3 Summary

To sum up, the process for gathering data for this thesis has been explained in this chapter. It also discusses the technique's justification and research methodologies. This chapter explains why the Waterfall technique was chosen for the proposed system's development. Requirements analysis, system design, system implementation and system testing are the four phases that must be followed. Its goal is to illustrate the research process and phases, as well as the security implementation and methodology used.

CHAPTER 4
EXPECTED RESULT

4.1 Overview

This chapter delves deeper into the overall system. This chapter creates numerous information linked to the design of a web-based signature authenticity system to discuss the predicted outcomes of the proposed system. In this chapter, we'll go through the overall system architecture. The results of the testing will also be supplied, as well as a table comparing the expected and actual results.

4.2 Testing Result

The signature authentication website's results and implementation will be displayed in this chapter. Register, log in, create a user profile, add signatures, and upload documents will all be part of the process. The proposed approaches from Chapter 3 will be implemented for this project. The output of the development process on the web application 'SignSafe' will be shown at the end of this chapter.

4.2.1 Test Case Expected versus Actual Result

Table 4.1 shows the list of activities that are expected to be done and the actual result of the project development.

Table 4.1: Test case table

Test Case	Step No	Step Description	Expected Results (Results supposed to be)	Actual Results (Results shown during testing)	Status (Pass/Fail)
1	1	Empty Username	User unable to login		
	2	Empty Password			
	3	Click Login			
2	1	Wrong Username	User unable to login		
	2	Empty Password			
	3	Click Login			
3	1	Empty Username	User unable to login		
	2	Wrong Password			
	3	Click Login			
4	1	Correct Username	User unable to login		
	2	Empty Password			
	3	Click Login			
5	1	Correct Username	User unable to login		
	2	Wrong Password			
	3	Click Login			
6	1	Empty Username	User unable to login		
	2	Correct Password			
	3	Click Login			
7	1	Correct Username	Users able to log in and allowed to dashboard		
	2	Correct Password			
	3	Click Login			

4.3 Analysis and Conclusion

To summarise, all of the project's research objectives and scope of the study were met. However, several shortcomings could be addressed in the future to improve system compatibility. This chapter summarises how the functional testing of the web-based signature authenticity system is carried out. It was done to uncover and fix flaws or errors in the software system to improve its quality. Following that, test cases were built to ensure that the actual testing result matched the projected outcome. Following the testing, it is feasible to conclude that all of the test cases were completed, implying that the system's functions are functional and meet the system's criteria.

CHAPTER 5
MILESTONES AND TIME PLANS

5.1 Overview

The milestones, project planning, and timelines are all measured and recorded in this chapter using a Gantt Chart.

5.2 Gantt Chart

Table 5.1 and Table 5.2 indicate the list of phases and tasks (milestones) that are planned to be done and also the timelines throughout the project development.

Table 5.1: Gantt Chart 1 (21/3 – 15/5)

SIGNSAFE: SIGNATURE AUTHENTICITY SYSTEM FOR CONFIDENTIAL DOCUMENTS USING WEB-BASED SECURE ACCESS

NUR AZILA BINTI MUHAMMAD
GANTT CHART

Wed, 3/23/2022

1

TASK	PROGRESS	START	END
Phase 1: Requirement Analysis			
Task 1: Identifying Problem Statement, Objectives and Project Scope	100%	3/23/22	4/1/22
Task 2: Comparing Existing System	100%	4/11/22	4/15/22
Task 3: Comparing Between Types of System	100%	4/16/22	4/20/22
Task 4: Observation	100%	4/25/22	5/8/22
Task 5: Use Case Diagram	100%	5/9/22	5/15/22
Phase 2: System Design			
Task 1: Identifying SDLC Model	100%	5/23/22	5/29/22
Task 2: Designing User Interface	10%	10/10/22	10/24/22
Task 3: Designing Flowchart	30%	10/24/22	10/31/22
Phase 3: System Implementation			
Task 1: Development	5%	11/1/22	11/21/22
Task 2: Coding	1%	11/21/22	12/18/22
Phase 4: System Testing			
Task 1: Test Case	20%	12/18/22	1/8/23
Deployment			
Task 1: Choose Thesis Topic	100%	3/23/22	4/1/22
Task 2: Introduction	100%	4/1/22	4/15/22
Task 3: Literature Review	100%	4/15/22	4/29/22
Task 4: Research Methodology	100%	4/29/22	5/20/22
Task 5: Milestones and Planning	100%	5/20/22	6/10/22
Task 6: Thesis Submission	100%	6/10/22	6/19/22
Task 7: Thesis Presentation	30%	6/19/22	7/3/22

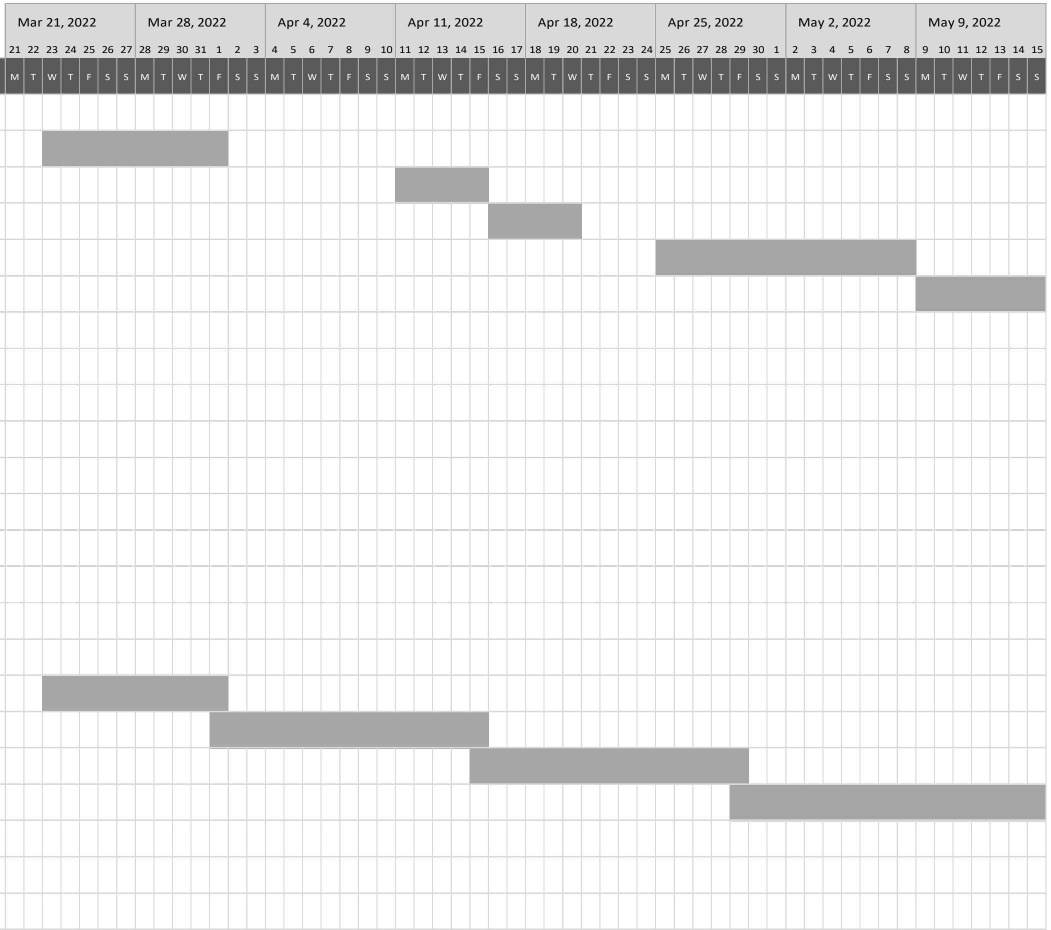


Table 5.2: Gantt Chart 2 (16/5 – 10/7)

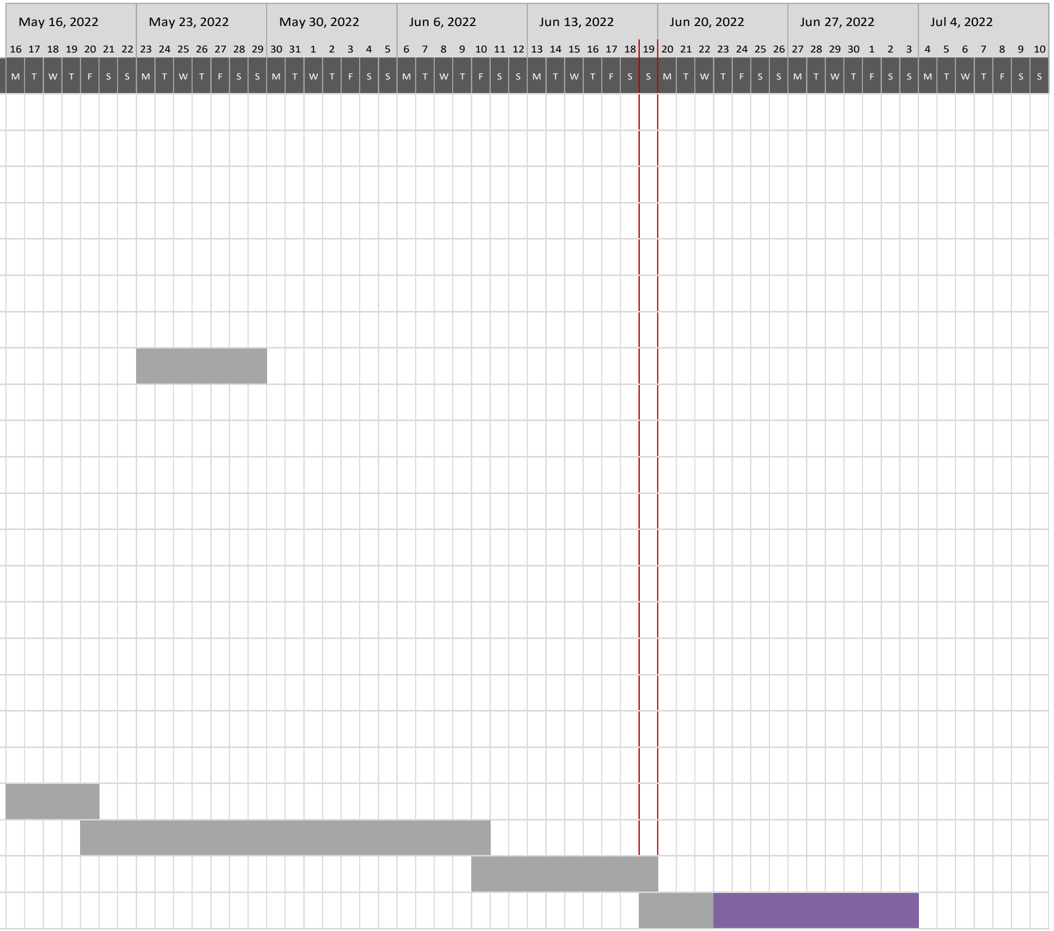
SIGNSAFE: SIGNATURE AUTHENTICITY SYSTEM FOR CONFIDENTIAL DOCUMENTS USING WEB-BASED SECURE ACCESS

NUR AZILA BINTI MUHAMMAD
GANTT CHART

Wed, 3/23/2022

9

TASK	PROGRESS	START	END
Phase 1: Requirement Analysis			
Task 1: Identifying Problem Statement, Objectives and Project Scope	100%	3/23/22	4/1/22
Task 2: Comparing Existing System	100%	4/11/22	4/15/22
Task 3: Comparing Between Types of System	100%	4/16/22	4/20/22
Task 4: Observation	100%	4/25/22	5/8/22
Task 5: Use Case Diagram	100%	5/9/22	5/15/22
Phase 2: System Design			
Task 1: Identifying SDLC Model	100%	5/23/22	5/29/22
Task 2: Designing User Interface	10%	10/10/22	10/24/22
Task 3: Designing Flowchart	30%	10/24/22	10/31/22
Phase 3: System Implementation			
Task 1: Development	5%	11/1/22	11/21/22
Task 2: Coding	1%	11/21/22	12/18/22
Phase 4: System Testing			
Task 1: Test Case	20%	12/18/22	1/8/23
Deployment			
Task 1: Choose Thesis Topic	100%	3/23/22	4/1/22
Task 2: Introduction	100%	4/1/22	4/15/22
Task 3: Literature Review	100%	4/15/22	4/29/22
Task 4: Research Methodology	100%	4/29/22	5/20/22
Task 5: Milestones and Planning	100%	5/20/22	6/10/22
Task 6: Thesis Submission	100%	6/10/22	6/19/22
Task 7: Thesis Presentation	30%	6/19/22	7/3/22



5.3 Summary

To summarize, Gantt Chart can make the process of understanding the project’s objectives, gathering data, implementing methodologies, developing the system and conducting the testing easier and much smoother. As a consequence, the project’s development will allow more detailed progress with all of the listed milestones provided. Hence, this will help to ensure that the developed system is beneficial to others, meet the objectives and solve all of the problems stated.

REFERENCES

After the Disaster: Replacing Lost or Damaged Documents. 2015. *FEMA.gov* [Internet]. Accessed April 10, 2022, from https://www.fema.gov/newsrelease/2015/06/19/after-disaster-replacing-lost-or-damaged-documents

Al, A., Alzahrani, M., Alfosail, M., Aldossary, M., Almuhaidib, S., Alqahtani, N., Saqib, K., Alissa, N., & Almubairik. (n.d.). *Secure Sign: Signing Document Online*.

Alonso-Fernandez, F., & Fierrez, J. 2015. Secure access system using signature verification over tablet PC Fusion of Spatio-Temporal Information for Footstep Recognition. View project ICCST-2017: 51st International Carnahan Conference on Security Technology View project. *Secure Access System Using Signature Verification over Tablet PC*. https://doi.org/10.1109/MAES.2007.351725

Aroral, H. K. 2021. Waterfall Process Operations in the Fast-paced World: Project Management Exploratory Analysis. *International Journal of Applied Business and Management Studies*, 6(1), 91–99.

Demirel, S. T., & Das, R. 2018. Software requirement analysis: Research challenges and technical approaches. *6th International Symposium on Digital Forensic and Security, ISDFS 2018 - Proceeding, 2018-Janua*, 1–6. https://doi.org/10.1109/ISDFS.2018.8355322

Desarkar, A., Sanyal, S., Baidya, A., Das, A., & Chaudhuri, C. 2019. Innovative Outlier Removal Techniques to Enhance Signature Authentication Accuracy for Smart Society. *International Journal of Distributed Systems and Technologies*, 10(2), 64–83. https://doi.org/10.4018/ijdst.2019040104

Dhagat, R., Joshi, P. 2016. New approach of user authentication using a digital signature. *Symposium on Colossal Data Analysis and Networking (CDAN)*.

Examples of QR code application | Technical Information | automatic data capture | DENSO WAVE. (n.d.). Www.denso-Wave.com [Internet]. Accessed May 18, 2022, from https://www.denso-wave.com/en/adcd/fundamental/2dcode/case/index.html

Ferng, H.-W., & Khoa, N. M. 2016. On security of wireless sensor networks: a data authentication protocol using digital signature. *Wireless Networks*, 23(4), 1113–1131. https://doi.org/10.1007/s11276-016-1208-0

Finandhita, A., & Afrianto, I. 2018. Development of E-Diploma System Model with Digital Signature Authentication. IOP *Conference Series*: *Materials Science and Engineering*, 407, 012109. https://doi.org/10.1088/1757-899x/407/1/012109

Gupta, P., Sinha, A., Kr. Srivastava, P., Perti, A., & Singh, A. K. 2020. Security Implementations in IoT Using Digital Signature. *Lecture Notes in Electrical Engineering*, 523–535. https://doi.org/10.1007/978-981-15-4692-1_40

Harder, J. 2017. Buttons, Navigation, Form and Non-Form Actions. *Enhancing Adobe Acrobat DC Forms with JavaScript*, 55–90. https://doi.org/10.1007/978-1-4842-2893-7_4

HEILMANN, C. June 2011. *Chapter 1. HTML5: from documents to applications · HTML5 in Action*. Livebook.manning.com. https://livebook.manning.com/book/html5-in-action/chapter-1/

Hertlein, M., Manaras, P., & Pohlmann, N. (2017). Smart Authentication, Identification and Digital Signatures as Foundation for the Next Generation of Eco Systems. *Digital Marketplaces Unleashed*, 905–919. https://doi.org/10.1007/978-3-662-49275-8_80

Huh, J.-H. 2020. Surgery Agreement Signature Authentication System for Mobile Health Care. *Electronics*, 9(6), 890. https://doi.org/10.3390/electronics9060890

info@qrtiger.com, B. C. 2022, June 14. *QR code types: 15 primary QR solutions and their functions*. Qrcode-Tiger.com [Internet]. https://www.qrcode-tiger.com/qr-code-types

Kaspersky. 2020, September 10. *What is a QR Code and how do I scan one?* Www.kaspersky.com [Internet]. https://www.kaspersky.com/resource-center/definitions/what-is-a-qr-code-how-to-scan

Kramer, M. 2018. BEST PRACTICES IN SYSTEMS DEVELOPMENT LIFECYCLE: AN ANALYSES BASED ON THE WATERFALL MODEL. *Review of Business & Finance Studies, 9(1),* 77–84. https://ssrn.com/abstract=3131958www.theIBFR.com

Lax, G., Buccafurri, F., Caminiti, G. 2015. Digital Document Signing: Vulnerabilities and Solutions. *Information Security Journal: A Global Perspective,* pp **24** (1-3) 1-14.

Lupanda, I. S., & van Rensburg, J. T. J. (2021). Design guidelines for mobile applications. *15th International Conference on Interfaces and Human Computer Interaction, IHCI 2021 and 14th International Conference on Game and Entertainment Technologies, GET 2021 - Held at the 15th Multi-Conference on Computer Science and Information Systems, MCCSI, 92–99.*

Modern Applications of QR Codes | QR Code Generator. (n.d.). Www.binarytranslator.com [Internet]. Accessed June 18, 2022, from https://www.binarytranslator.com/modern-applications-of-qr-codes

Mohammed Ali, A., & Farhan, A. K. 2020. Enhancement of QR Code Capacity by Encrypted Lossless Compression Technology for Verification of Secure E-Document. *IEEE Access*, 8, 27448–27458. https://doi.org/10.1109/access.2020.2971779

Nur, S., Adams, C. E., & Brailsford, D. F. 2016. Using built-in functions of Adobe Acrobat Pro DC to help the selection process in systematic reviews of randomised trials. *Systematic Reviews*, 5(1). https://doi.org/10.1186/s13643-016-0207-7

Olexa, M., Grant, L. 2016. Replacing Lost or Damaged Documents. *IFAS* [Internet]. Florida: Extension University of Florida. Accessed April 11, 2018, from: http://edis.ifas.ufl.edu/pdffiles/DH/DH21500.pdf

Patel, U., Patel, A., & Suthar, F. 2019. *THE STUDY OF DIGITAL SIGNATURE AUTHENTICATION PROCESS.*

Patil, P. R., & Patil, B. V. 2021. A Review - Signature Verification System Using Deep Learning: A Challenging Problem. *International Journal of Scientific Research in Science and Technology*, 295–298. https://doi.org/10.32628/ijsrset207632

Pereira, C., Barbosa, L., Martins, J., Borges, J. 2018. Digital Signature Solution for Document Management Systems. *Advances in Intelligent Systems and Computing.* The University of Trás-os-Montes and Alto Douro, pp **12** 16-25.

phpMyAdmin contributors. 2019. *phpMyAdmin*. PhpMyAdmin [Internet]. https://www.phpmyadmin.net/

Prasetyo, A., Adi, W.P. 2015. Design Validation System and Legalized Document Using E-Certificate Application. *Information Systems International Conference (ISICO),* pp **12** 12-14.

Sayers, A. (n.d.). *Signatures: Digital vs. Paper*. Blog.clinked.com [Internet]. https://blog.clinked.com/signatures-digital-vs.-paper

Schurman, E. M., & Pardi, W. J. 1999. *Dynamic HTML in action*. Microsoft Press. *StackPath*. 2019, August 8. Www.ntaskmanager.com [Internet]. https://www.ntaskmanager.com/blog/how-to-use-ntask-for-waterfall-project-management-a-practical-guide-for-first-timers/

Thoopsamut, P., & Limthanmaphon, B. 2019. Handwritten Signature Authentication using Color Coherence Vector and Signing Behavior. *Proceedings of the 2019 2nd International Conference on Information Science and Systems*. https://doi.org/10.1145/3322645.3322682

trilabwpadmin. (n.d.). *The Differences between Digital, Electronic and Wet-Ink Signatures*. Tricor Labuan [Internet]. Accessed June 18, 2022, from https://tricorlabuan.com/highlights/featured-articles/the-differences-between-digital-electronic-and-wet-ink-signatures/#

Vorugunti, C. S., Guru, D. S., & Pulabaigari, V. 2019. A Secure and Light Weight User Authentication System Based on Online Signature Verification for Resource Constrained Mobile Networks. *Communications in Computer and Information Science*, 133–140. https://doi.org/10.1007/978-981-13-9361-7_12

Warasart, M., & Kuacharoen, P. 2012. Paper-based Document Authentication using Digital Signature and QR Code. *4TH International Conference on Computer Engineering and Technology, 40(January), 94-98.*

Wu, Z., Guo, A., Yue, M., & Liu, L. 2020. An ADS-B Message Authentication Method Based on Certificateless Short Signature. *IEEE Transactions on Aerospace and Electronic Systems,* 56(3), 1742–1753. https://doi.org/10.1109/taes.2019.2933957