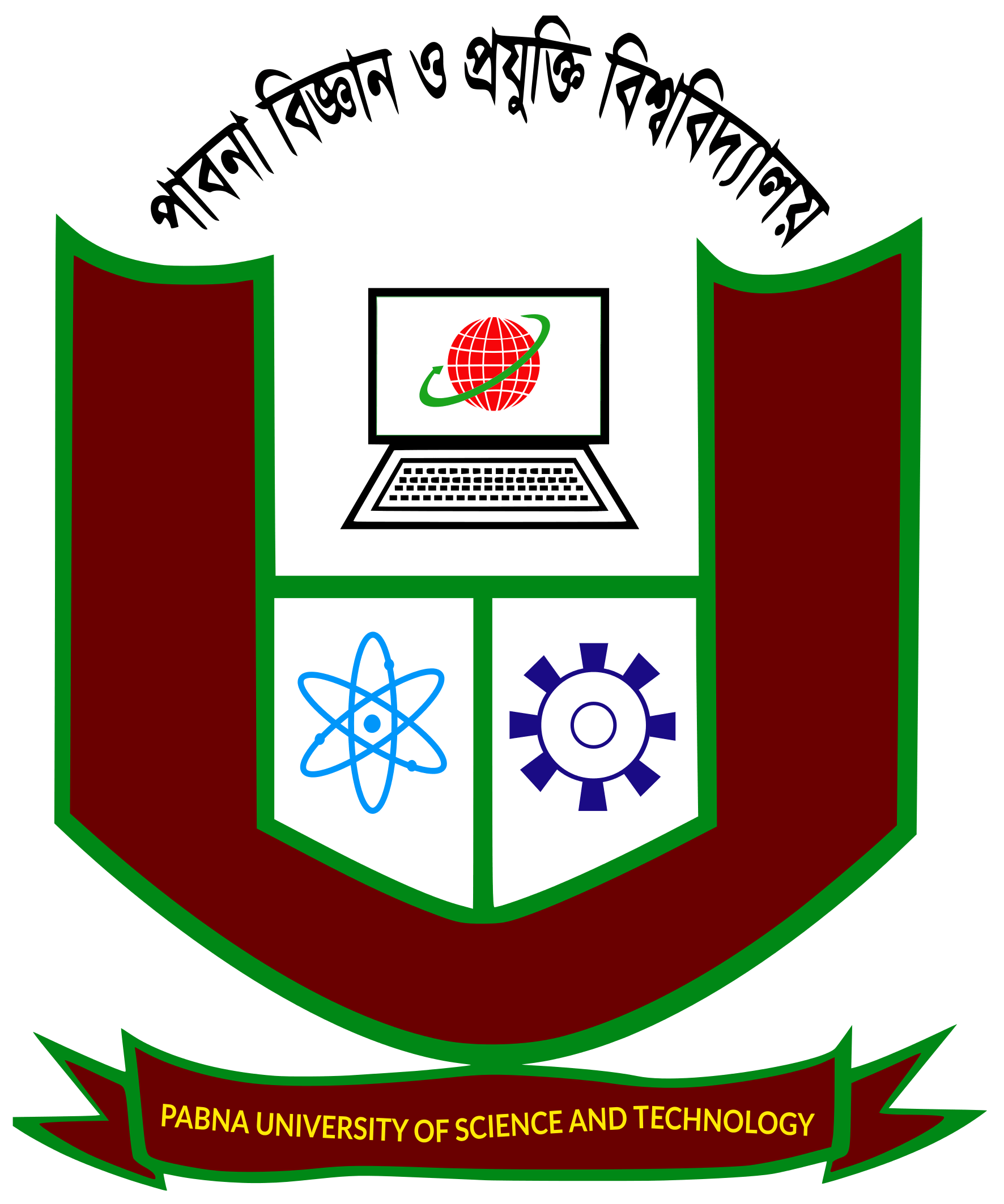
**Web-based Certificate Verification**

****

**B.Sc. (Engineering) 3rd Year 2nd Semester Examination 2021**

**Course Title: Project Design and Development**

**Course Code: ICE-3211**

**B.Sc. (Engineering) Project**

A project paper submitted to the Department of Information and Communication Engineering, Pabna University of Science and Technology (PUST) in partial fulfillments of the requirements for the B.Sc. (Engineering) 3rd Year 2nd Semester Examination 2021

**Supervised By:**

**Taskin Noor Turna**

Assistant Professor

Department of Information and Communication Engineering,

Pabna University of Science and Technology

**Submitted By:**

**Md. Omar Faruk**

Roll No: 190605

Registration No. 1065330

Session: 2018-19

3rd Year 2nd Semester

**Department of Information and Communication Engineering,**

**Pabna University of Science and Technology**

**Pabna-6600, Bangladesh**

**ACKNOWLEDGEMENT**

First and foremost, I would like to express my sincere gratitude to Almighty Allah for bestowing upon me the strength and perseverance to complete this project.

I am deeply indebted to my university, Pabna University of Science and Technology, for providing me with a conducive and stimulating environment to pursue my academic excellence. I am honored and privileged to have had the opportunity to undertake this project as part of the Bachelor's Program in the Department of Information and Communication Engineering, Faculty of Engineering and Technology.

I would like to extend my special thanks and appreciation to my project supervisor, Taskin Noor Turna (Assistant Professor, Dept. of ICE, PUST), for her invaluable guidance, support, and encouragement throughout this project. Her dynamism, vision, and dedication have inspired me greatly. I am also grateful for her friendship, empathy, and sense of humor.

**ABSTRACT**

This project aims to develop a web-based certificate verification system tailored to the Bangladesh context. The system leverages web technology to enhance the process of verifying educational certificates, addressing the need for authenticity and transparency. By utilizing real-time verification, advanced security measures, and streamlined processes, the system offers accessibility, accuracy, and reduced administrative burden. While challenges such as technical dependencies and cybersecurity risks exist, the benefits of web-based verification, including scalability and cost-effectiveness, outweigh these concerns. The project seeks to contribute to the integrity of the education system in Bangladesh, promote fair employment practices, and establish a trusted ecosystem for certificate verification.

**Keywords:** Blockchain, Digital Certificate, Hashing, Validation.

**TABLE OF CONTENTS**

Acknowledgement …………………………………………………………………………..…..... i

Abstract …………………………………………………………………………………….……. ii

Table of Contents …………………………………………………………………………....... iii-v

**1. INTRODUCTION 1-7**

1.1 Background of the study ……..…..………………………………….….…………..1-3

* 1. Website Development Process ...…..……………….…………………….…………4-7

1.2.1 Types of Website Development …….…………….…………….…………..6-7

**2. SYSTEM ENVIRONMENT 8-9**

2.1 Hardware Configuration ……..…………….…………………………….…………… 8

2.2 Software Configuration …………....……..….……….………………………..….…8-9

2.2.1 OS: Microsoft Windows 10/11 …….…...……………….……………….…..8-9

2.2.2 Visual Studio Code …..…………………………………………………...……9

**3. USED LANGUAGES 10-19**

3.1 HTML (Hypertext Markup Language) ……….……….….………………………10-11

3.2 CSS (Cascading Style Sheets) ………….………………..……………………….11-12

3.3 Bootstrap ………………………………….…………………..…………………..….13

3.4 JavaScript …………………………..………………………………………...…..14-16

3.4.1 Client-Side JavaScript…………………………..………......…...………….14-15

3.4.2 Advantages of JavaScript……………………..………............……………….15

3.4.3 Limitations of JavaScript……………………..….…....……....……………….15

3.4.4 JavaScript Development Tools…….……………..……..……....………….15-16

3.4.4 JavaScript – Syntax……………………..…....……....………………………..,16

3.6 PHP (Hypertext Preprocessor) ………………………….…………..…………… 16-18

3.5.1 Characteristics of PHP………………………….…….…..…..….………… 16-17

3.5. 2 Why to Learn PHP? ……...…………………….………..…..….………….….17

3.5. 3 Applications of PHP……..………...…………….…...…..…..….………….….17

3.5. 3 Basic PHP Syntax ……..………...…………….…..........…..…..….………….….18

3.7 MySQL …………………………………………………………………………...18-19

**4. COMPUTATIONAL METHOD 20-22**

4. 1 Overview……………………………………………………………………………… 20

4.2 Hash Function................................................................................................................20

4.3 SHA-256 …………………………………………………………………………. 21-22

4.4 Flow Chart ……………………………………………………………….….….…… 22

**5. PROJECT OVERVIEW 23-24**

5.1 Certificate Uploading...…………………………………………….…….……………. .2

5.1.1 Uploading Certificate……………….….….…………….…….……….…….……23

5.1.2 Uploading Message ….……………………………………………………....……23

5.2 Certificate Verification….………………………………….……....…………...……24

5.2.1 If certificate match ….…………………………………………...…….…….……24

5.2.2 If certificate does not match ….…………………………………………..….……24

**6. CONCLUSION AND FUTURE PLAN**….………………………….…………….….25-26

6.1 Conclusion…………….……………………………………………………………….25

6.2 Future plan……………………………………………………………………………..26

**REFERENCES ………………………………………………………………………………...27**

**LIST OF FIGURES:**

1. Example Of Certificate Management System …………………….………………………..2

2. Development Process…………………………………………………………………..........4

3. HTML5……………….……...………………………………….……..................................10

4. CSS3……………….....……………………………...……………………………………..12

5. Syntax of CSS …………….………………………...……………………………………...12

6. Bootstrap ….…………………………………...……………………………….…….…….13

7. JavaScript ……………………………………...…….……………………………………..14

8. PHP ……………………………...……………………………………..…………………..16

10. MySQL …….…………………….……...……………………………….……………….. 20

11. Examples of Hash Function…….…………………….……...………………………………21

12. Flow chart of hash function………………………………………………………………….22

13. Upload Certificate……………………………………………………………………………23

13. Upload Message…………………………………………………...…………………………23

14. Verification Message (Figure 5.3) ….……………………………………………….………24

14. Verification Message (Figure 5.4) ….……………………………………………….………24

**CHAPTER 1**

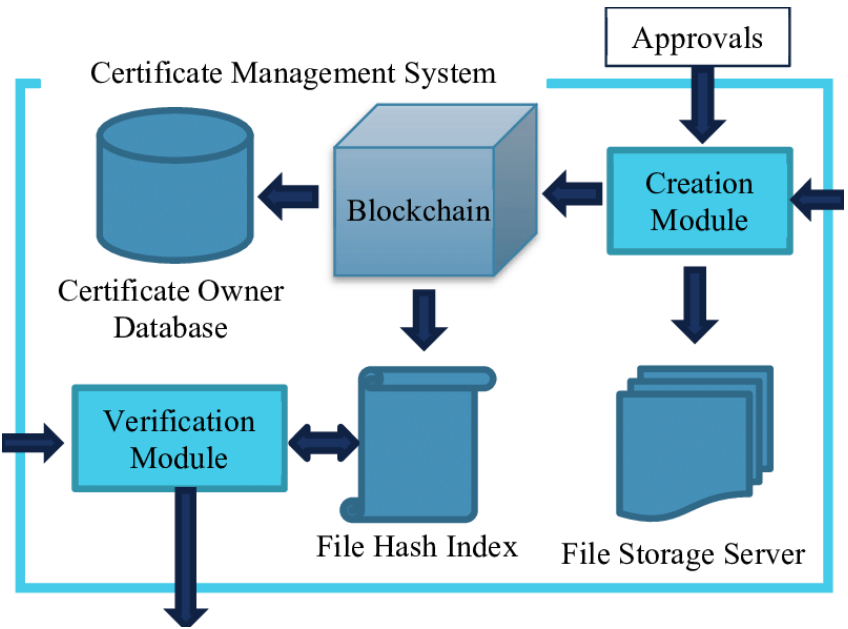
**INTRODUCTION**

* 1. **Background of the Study**

Digital transformation refers to the incorporation of computer technologies into different aspects of business operations, playing a crucial role in enhancing overall efficiency for organizations. Nevertheless, academic certificates, which are currently issued in physical form or scanned copies, are slow to adapt to this transformative trend.

The process of recruiting personnel for an organization can be time-consuming, especially when it involves analyzing a large volume of candidate resumes. Additionally, verifying paper or digitized certificates can be a lengthy task that requires manual contact with the academic institutions that issued them, resulting in significant time and resource consumption. However, this verification is crucial due to the presence of counterfeit academic diplomas and certificates in the market. Recent surveys indicate that a substantial number of employers (58%) have encountered instances of false information in resumes, with a notable increase (33%) in embellished or fabricated credentials [Car]. Another survey corroborates these findings, revealing that more than half of the resumes and job applications (53%) contain falsifications, and a significant majority (78%) are misleading [Sta]. Even public figures, including politicians, frequently find themselves embroiled in controversies regarding their education and certificates.

Web technology offers solutions to these challenges by storing data on servers. Moreover, it enables organizations to eliminate intermediaries, resulting in reduced processing time by avoiding the involvement of third parties. Additionally, it helps in lowering transaction costs.

In 2008, blockchain was first referenced by Satoshi Nakamoto. Blockchain is a web-based record that makes it conceivable to trade information in a straightforward and decentralized way. An Android application that can be utilized to empower secure authentication confirmation will be created as a feature of this task. As of now, all recognitions and records contain data that can be effectively changed in an unlawful way by people and ought not be effectively open to different associations. As an outcome of this, there is a squeezing need for a rapid system that is fit for guaranteeing that the data contained in such certificates is veritable. This shows that the record was gotten from a solid and endorsed source and isn't messed with. For instructive foundations, various advances have been created to safely store and safeguard e-testaments in cloud-based frameworks.

**Figure 1.1.: Example Figure**

Blockchain is the essential instrument for satisfying this need, and when joined with other hashing calculations, it makes a strong information security system. It likewise disposes of the need to regularly confirm endorsements. Blockchain innovation is being utilized to lessen the quantity of phony graduation authentications and work on their security, realness, and mystery. To ensure the validness, trustworthiness, and non-renouncement of computerized records, computerized marks are a sort of safety innovation. Furthermore, endorsement capacity is safer when blockchain is being used. An application that works with the solid approval of computerized testaments was created by utilizing these advances.

Fabrication of scholarly certifications has for some time been an issue in scholarly world. The Massachusetts Establishment of Innovation Media Lab's Block-certs project, a technique principally executed by joining the hash worth of neighborhood records with the blockchain yet with various issues, was the primary compelling mechanical way to deal with safeguard bona fide qualification confirmation and notoriety. Various cryptographic arrangements are proposed to address the previously mentioned issues in light of Blockcerts, for example, carrying out a multi-signature plan to improve certificate confirmation; setting up a protected disavowal component to build the unwavering quality of testament repudiation; and making a safe unified distinguishing proof to check the organization giving the card.

Establishments grant confirmations to graduates who have met all graduation necessities. A graduation testament is for the most part a paper-based report in light of the fact that an electronic record can't really supplant an actual declaration [1]. Be that as it may, testament misrepresentation has expanded because of the accessibility of front line and modest examining and printing innovation. This puts the authenticity of the declaration holder and the association that gave the certificate in peril [2]. Thus, archive approval and check have advanced into fundamental errands. It is important to confirm that the holder is the legitimate proprietor of the alumni's graduation certificate. A graduation certificate must also be checked to make sure the information on it is correct and comes from a legitimate source [3]. Educational establishments employ a variety of strategies to combat forgery and fraud. Nevertheless, the majority of the procedures take time due to their manual nature and human involvement [4]. In the meantime, a lot of time will be spent either reaching the establishment to approve a certificate or sitting tight for a reaction from the college to affirm that the data on the endorsement is precise. To survey the affirmations of many up-and-comers, this technique might be incredibly tedious and exorbitant. As a result, the research in this study aims to develop a theoretical model for a possible blockchain-based method of verifying academic degrees.

* 1. **Website Development Process**

Website development is the process of creating a website. It involves a number of steps, including planning, design, development, testing, and launch**.**

Here is a general overview of the website development process:



**Figure 1.2: Development Process**

**Step 1. Information gathering**

Before you can actually build a website, you need to gather information. This will include your purpose, main goals, and target audience.

Your purpose is essentially the reason behind creating this website. Is it for self-promotion or to provide information about a certain topic? Your goals are what you want to accomplish with this website. Having goals will give you a better idea of how to go about creating the website and what content to include. Your target audience is who your website is going to appeal to. Every business has a target audience, so make sure you figure out who yours is before actually creating the website. Imagine your ideal customer, including their age, gender, and interests.

**Step 2. Planning**

This step involves defining the purpose of the website, identifying the target audience, and creating a sitemap. The sitemap is a blueprint of the website that shows how the different pages will be linked together.

**Step 3. Design**

This step involves creating the visual appearance of the website. This includes designing the layout, choosing the colors and fonts, and creating the overall look and feel of the site.

**Step 4: Content**

The content that you have on your website is one of the most important aspects of a website. Your content will convey your message to your audience and encourage them to use your website. But before you can write your content, you need to figure out your goals and purpose, which is why step 2 is so important. Your content should be relevant and interesting enough that your users keep coming back.

**Step 5: Functionality**

At this step is when you’ll actually start to build your website. This is also when all the above steps will come together to create the look and functionality of the website. You want your website to be user-friendly and easy to get around. The homepage will usually be created first, and then all the sub-pages will come after. You also need to make sure the website can be accessible from both a desktop and mobile phone.

**Step 6: Testing**

Once the website has been successfully created, it’s not quite ready to be launched just yet. It needs to be tested first. Testing the website can be a tedious process, but it’s necessary to make sure the website is running properly. During this step, you’ll test all the links and buttons on the website, check the spelling of everything, and make sure the website looks the same on a phone than it does on a computer.

**Step 7: Launch**

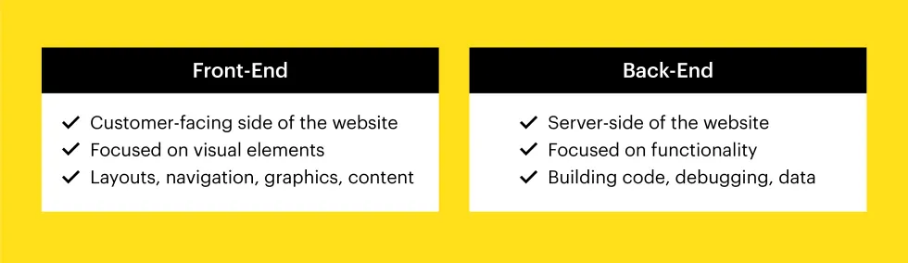
After you’ve thoroughly checked the website and tested it a few times, now comes the exciting part: actually launching it. To launch your website, you need to upload it to a server. Once it’s uploaded, you’ll want to quickly run one last test just to double check that everything is correct. The website will now be viewable to the public.

**Step 8: Monitoring and updates**

Even after you successfully launch your website, it’s still crucial to go back and check it from time to time. Mistakes can happen, and it’s important to stay on top of the website to make sure it remains in good shape. You want to fix any problems as quickly as possible and always keep your website up to date.

**1.2.1 Types of Website Development**

There are a few different types of website development, but the most common types are front-end development and back-end development. This refers to what a user sees on the website, and what a user doesn’t see.



**Figure 1.3: Types of website development**

**Front-end development**

Front-end development is what the user will see and interact with on the website. This typically involves website design and includes the website’s colors, layout, fonts, and images. If you’re a front-end developer, that means you're responsible for having a website look and feel a certain way.

Front-end development involves using tools like Photoshop and Illustrator to create the website design. A front-end developer will also need to understand various programming languages, or coding languages, like [HTML](https://templates.mailchimp.com/), CSS, and JavaScript. Understanding these programming languages is crucial so that a user can actually interact with the website with buttons and navigation menus.

**Back-end development**

Back-end development is what the user doesn’t see with the website. Back-end development is focused more on how the website works, rather than how it looks. This can include user authentication, network and hosting configuration, database interaction, and anything else that goes on behind the scenes of a website.

A back-end developer is responsible for making sure everything is running smoothly within the website. For example, if people upload their information onto a website, a back-end developer is responsible for compiling and analyzing that data. A back-end developer needs to be familiar with server-side languages, like Ruby, .Net, and Python.

Another type of website development is full-stack development. Full-stack developers can do both front-end and back-end development. A full-stack developer must be knowledgeable of both programming languages and server-side languages and needs to be able to handle all aspects of website development.

Because hiring one person to the job is obviously much easier than hiring two people, many businesses prefer to hire full-stack developers. However, it’s a very in-demand job in the tech industry.

**CHAPTER 2**

**SYSTEM ENVIROMENT**

**2.1 Hardware Configuration**

Laptop

* AMD As-7410 APU
* 4 GB RAM
* 500/1000 GB HDD

**2.2 Software Configuration**

* OS: Microsoft Windows 10
* Visual Studio Code

**2.2.1 OS: Microsoft Windows 10/11**

Windows is a family of graphical operating systems developed by Microsoft. It is the most popular operating system in the world, with over 1.5 billion active users.

Windows is a graphical user interface (GUI) operating system, meaning that users interact with the computer using icons, windows, and menus. Windows also uses a mouse or other pointing device to allow users to select and manipulate objects on the screen.

Windows is a multitasking operating system, meaning that it can run multiple programs at the same time. Windows also has a built-in memory management system that allocates memory to programs as needed.

**Classification of Windows**

Windows operating systems can be classified into two main types:

1. Client operating systems and
2. Server operating systems.

Client operating systems are designed for use on desktop computers and laptops. They are focused on providing a user-friendly interface and a variety of features for productivity and entertainment. Some examples of client Windows operating systems include:

* Windows 11
* Windows 10
* Windows 8.1
* Windows 7

Server operating systems are designed for use on servers. They are focused on providing reliability, security, and performance for hosting and managing applications and data. Some examples of server Windows operating systems include:

* Windows Server 2022
* Windows Server 2019
* Windows Server 2016
* Windows Server 2012 R2

Windows operating systems can also be classified by their target audience. For example, there are versions of Windows designed for businesses, schools, and students. There are also versions of Windows designed for specific types of devices, such as tablets and mobile phones.

**2.2.2 Visual Studio Code**

Visual Studio Code (VS Code) is a lightweight but powerful source code editor developed by Microsoft for Windows, Linux, and macOS. It comes with built-in support for JavaScript, TypeScript, and Node.js, and has a rich ecosystem of extensions for other languages and runtimes (such as C++, C#, Java, Python, PHP, Go, .NET).

VS Code is known for its many features, including:

* Intelligent code completion: VS Code provides intelligent code completion for functions, variables, and other symbols, which can help you write code faster and more accurately.
* Syntax highlighting: VS Code highlights the syntax of your code in different colors, which can make it easier to read and understand.
* Linting: VS Code can detect and warn you about potential errors and stylistic problems in your code.
* Debugging: VS Code has a built-in debugger that allows you to step through your code line by line, set breakpoints, and inspect variables.
* Git integration: VS Code has built-in Git integration, which allows you to track changes to your code, commit changes to a repository, and push and pull changes from a remote repository.
* VS Code is also highly customizable. You can change the theme, font size, and other settings to suit your preferences. You can also install extensions to add new features and functionality to VS Code.

**CHAPTER 3**

**USED LANGUAGES**

In this project I have used PHP and MySQL in backend and for the frontend coding I have used HTML5, CSS, Bootstrap, JavaScript

**3.1 HTML (Hypertext Markup Language)**



**Figure 3.1: HTML5**

HTML, or HyperText Markup Language, is the standard markup language used to create and design documents on the World Wide Web. It is a key building block of web development and is used to structure content on the internet. HTML uses a system of tags and attributes to define the structure and presentation of content on a web page.

Here are some key points about HTML:

* **Markup Language:** HTML is a markup language, not a programming language. It is used to structure content and provide a framework for web browsers to interpret and display that content.
* **Tags and Elements:** HTML documents consist of HTML tags, which are used to define elements on a page. Tags are enclosed in angle brackets (< >) and usually come in pairs, with an opening tag and a closing tag. The content is placed between these tags. Example

<p>This is a paragraph.</p>

* **Document Structure:** HTML documents typically have a specific structure, including a head and a body. The head contains meta-information about the document, such as the title,
* **Attributes:** HTML tags can have attributes that provide additional information about the element. Attributes are included within the opening tag and are usually name-value pairs. Example:

<a href="https://www.example.com" target="\_blank">Visit Example.com</a>

* **Versioning:** HTML has evolved over time, and different versions exist. The latest version is HTML5, which introduced new features and enhancements for multimedia, graphics, and improved semantics

**A Simple HTML Syntax:**

|  |
| --- |
| <!DOCTYPE html>  <html>  <head>  <title> Type here the title </title>  </head>  <body>  <h1> Basic Example of HTML </h1>  <p> Hello HTML! </p>  </body>  </html> |

Explanation of some HTML tags:

* The <!DOCTYPE html> declaration defines this document to be HTML5
* The <html> element is the root element of an HTML page
* The <head> element contains meta information about the document
* The <title> element specifies a title for the document
* The <body> element contains the visible page content
* The <h1> element defines a large heading
* The <p> element defines a paragraph
* character set, and links to external resources. The body contains the actual content of the document. Example:

<!DOCTYPE html>

<html>

<head>

<title>My Web Page</title>

</head>

<body>

<h1>Hello, World!</h1>

<p>This is my first web page.</p>

</body>

</html>

**3.2 CSS (Cascading Style Sheets)**



**Figure 3.2: CSS3**

Cascading Style Sheets is a simple mechanism for adding styles (e.g., fonts, colors, spacing) to Web documents. CSS defines how HTML elements are to be presented on screen, paper, or in other media. CSS saves a lot of work. It can control the layout of multiple web pages all at once.

CSS is designed to enable the separation of presentation and content, including layout, colors, and fonts. This separation can improve content accessibility, provide more flexibility and control in the specification of presentation characteristics, enable multiple web pages to share formatting by specifying the relevant CSS in a separate .css file, and reduce complexity and repetition in the structural content.

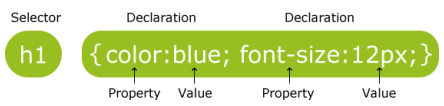
**CSS Syntax**:

A CSS rule set consists of a selector and a declaration block:

The selector points to the HTML element you want to style.

The declaration block contains one or more declarations separated by semicolons.

Each declaration includes a property name and a value, separated by a colon.



**Figure 3.3: Syntax of CSS**

**3.3 Bootstrap**



**Figure 3.4: Bootstrap**

* Bootstrap is the most popular HTML, CSS and JavaScript framework for developing a responsive and mobile friendly website.
* It is absolutely free to download and use.
* It is a front-end framework used for easier and faster web development.
* It includes HTML and CSS based design templates for typography, forms, buttons, tables, navigation, modals, image carousels and many others.
* It can also use JavaScript plug-ins.
* It facilitates you to create responsive designs.

**Why use Bootstrap?**

**Here are some of the reasons why we use Bootstrap:**

* **Responsiveness:** Bootstrap makes it easy to create websites that look good on all devices, from desktop computers to smartphones.
* **Mobile-first:** Bootstrap is designed with a mobile-first approach, meaning that it prioritizes the mobile experience. This is important because more and more people are using their smartphones to browse the web.
* **Pre-built components**: Bootstrap comes with a variety of pre-built components, such as buttons, forms, navigation bars, and modals. This can save you a lot of time and effort, as you don't have to create these components from scratch.
* **Grid system:** Bootstrap's grid system makes it easy to layout your website's content. The grid system consists of a series of rows and columns, which you can use to position your elements.
* **Customizable:** Bootstrap is highly customizable, so you can easily modify its styles to match your brand or project.
* **Open source:** Bootstrap is an open-source project, which means that it is free to use and modify. This makes it a great option for businesses and individuals on a budget.

**3.4 JavaScript**

****

**Figure 3.5: JavaScript**

JavaScript is a dynamic computer programming language. It is lightweight and most commonly used as a part of web pages, whose implementations allow client-side script to interact with the user and make dynamic pages. It is an interpreted programming language with object-oriented capabilities.

JavaScript was first known as LiveScript, but Netscape changed its name to JavaScript, possibly because of the excitement being generated by Java. JavaScript made its first appearance in Netscape 2.0 in 1995 with the name LiveScript. The general-purpose core of the language has been embedded in Netscape, Internet Explorer, and other web browsers.

The ECMA-262 Specification defined a standard version of the core JavaScript language.

* JavaScript is a lightweight, interpreted programming language.
* Designed for creating network-centric applications.
* Complementary to and integrated with Java.
* Complementary to and integrated with HTML.
* Open and cross-platform

**3.4.1 Client-Side JavaScript**

Client-side JavaScript is the most common form of the language. The script should be included in or referenced by an HTML document for the code to be interpreted by the browser.

It means that a web page need not be a static HTML, but can include programs that interact with the user, control the browser, and dynamically create HTML content.

The JavaScript client-side mechanism provides many advantages over traditional CGI server-side scripts. For example, you might use JavaScript to check if the user has entered a valid e-mail address in a form field.

The JavaScript code is executed when the user submits the form, and only if all the entries are valid, they would be submitted to the Web Server.

JavaScript can be used to trap user-initiated events such as button clicks, link navigation, and other actions that the user initiates explicitly or implicitly.

**3.4.2 Advantages of JavaScript**

The merits of using JavaScript are −

* **Less server interaction** − You can validate user input before sending the page off to the server. This saves server traffic, which means less load on your server.
* **Immediate feedback to the visitors** − They don't have to wait for a page reload to see if they have forgotten to enter something.
* **Increased interactivity** − You can create interfaces that react when the user hovers over them with a mouse or activates them via the keyboard.
* **Richer interfaces** − You can use JavaScript to include such items as drag-and-drop components and sliders to give a Rich Interface to your site visitors.

**3.4.3 Limitations of JavaScript**

* We cannot treat JavaScript as a full-fledged programming language. It lacks the following important features −
* Client-side JavaScript does not allow the reading or writing of files. This has been kept for security reason.
* JavaScript cannot be used for networking applications because there is no such support available.
* JavaScript doesn't have any multi-threading or multiprocessor capabilities.

Once again, JavaScript is a lightweight, interpreted programming language that allows you to build interactivity into otherwise static HTML pages.

**3.4.4 JavaScript Development Tools**

One of major strengths of JavaScript is that it does not require expensive development tools. You can start with a simple text editor such as Notepad. Since it is an interpreted language inside the context of a web browser, you don't even need to buy a compiler.

To make our life simpler, various vendors have come up with very nice JavaScript editing tools. Some of them are listed here –

* Microsoft FrontPage − Microsoft has developed a popular HTML editor called FrontPage. FrontPage also provides web developers with a number of JavaScript tools to assist in the creation of interactive websites.
* Macromedia Dreamweaver MX − Macromedia Dreamweaver MX is a very popular HTML and JavaScript editor in the professional web development crowd. It provides several handy prebuilt JavaScript components, integrates well with databases, and conforms to new standards such as XHTML and XML.
* Macromedia HomeSite 5 − HomeSite 5 is a well-liked HTML and JavaScript editor from Macromedia that can be used to manage personal websites effectively.

**3.4.5 JavaScript – Syntax**

JavaScript can be implemented using JavaScript statements that are placed within the <script>... </script> HTML tags in a web page. You can place the <script> tags, containing your JavaScript, anywhere within your web page, but it is normally recommended that you should keep it within the <head> tags. The <script> tag alerts the browser program to start interpreting all the text between these tags as a script. A simple syntax of your JavaScript will appear as follows.

<script ...>

JavaScript code

</script>

**3.5 PHP (Hypertext Preprocessor)**



**Figure 3.6: PHP**

The term PHP is an acronym for PHP: Hypertext Preprocessor. PHP is a server-side scripting language designed specifically for web development. It is open-source which means it is free to download and use. It is very simple to learn and use. The files have the extension “.php”.

Rasmus Lerdorf inspired the first version of PHP and participated in the later versions. It is an interpreted language and it does not require a compiler.

**3.5.1 Characteristics of PHP**

* PHP code is executed in the server.
* It can be integrated with many databases such as Oracle, Microsoft SQL Server, MySQL, PostgreSQL, Sybase, and Informix.
* It is powerful to hold a content management system like WordPress and can be used to control user access.
* It supports main protocols like HTTP Basic, HTTP Digest, IMAP, FTP, and others.
* Websites like www.facebook.com and www.yahoo.com are also built on PHP.
* One of the main reasons behind this is that PHP can be easily embedded in HTML files and HTML codes can also be written in a PHP file.
* The thing that differentiates PHP from the client-side language like HTML is, that PHP codes are executed on the server whereas HTML codes are directly rendered on the browser. PHP codes are first executed on the server and then the result is returned to the browser.

**3.5.2 Why to Learn PHP?**

PHP started out as a small opensource project that evolved as more and more people found out how useful it was. Rasmus Lerdorf unleashed the first version of PHP way back in 1994.

PHP is a MUST for students and working professionals to become a great Software Engineer specially when they are working in Web Development Domain. I will list down some of the key advantages of learning PHP:

* PHP is a recursive acronym for "PHP: Hypertext Preprocessor".
* PHP is a server side scripting language that is embedded in HTML. It is used to manage dynamic content, databases, session tracking, even build entire e-commerce sites.
* It is integrated with a number of popular databases, including MySQL, PostgreSQL, Oracle, Sybase, Informix, and Microsoft SQL Server.
* PHP is pleasingly zippy in its execution, especially when compiled as an Apache module on the Unix side. The MySQL server, once started, executes even very complex queries with huge result sets in record-setting time.
* PHP supports a large number of major protocols such as POP3, IMAP, and LDAP. PHP4 added support for Java and distributed object architectures (COM and CORBA), making n-tier development a possibility for the first time.
* PHP is forgiving: PHP language tries to be as forgiving as possible.
* PHP Syntax is C-Like.

**3.5.3 Applications of PHP**

As mentioned before, PHP is one of the most widely used language over the web. I'm going to list few of them here:

* PHP performs system functions, i.e. from files on a system it can create, open, read, write, and close them.
* PHP can handle forms, i.e. gather data from files, save data to a file, through email you can send data, return data to the user.
* You add, delete, modify elements within your database through PHP.
* Access cookies variables and set cookies.
* Using PHP, you can restrict users to access some pages of your website.
* It can encrypt data.

**3.5.4 Basic PHP Syntax**

<?php

// PHP code goes here

?>

**Example**

<html>

<head>

<title>Hello World</title>

</head>

<body>

<?php echo "Hello, World!";?>

</body>

</html>

**3.6 MySQL**

****

**Figure 3.7: MySQL**

MySQL is the world’s most popular opensource database. According to DB-Engines, MySQL ranks as the second-most-popular database, behind Oracle Database. MySQL powers many of the most accessed applications, including Facebook, Twitter, Netflix, Uber, Airbnb, Shopify, and Booking.com.

Since MySQL is open source, it includes numerous features developed in close cooperation with users over more than 25 years. So it’s very likely that your favorite application or programming language is supported by MySQL Database.

MySQL is a relational database management system:

Databases are the essential data repository for all software applications. For example, whenever someone conducts a web search, logs in to an account, or completes a transaction, a database system is storing the information so it can be accessed in the future.

A relational database stores data in separate tables rather than putting all the data in one big storeroom. The database structure is organized into physical files optimized for speed. The logical data model, with objects such as data tables, views, rows, and columns, offers a flexible programming environment. You set up rules governing the relationships between different data fields, such as one to one, one to many, unique, required, or optional, and “pointers” between different tables. The database enforces these rules so that with a well-designed database your application never sees data that’s inconsistent, duplicated, orphaned, out of date, or missing.

The “SQL” part of “MySQL” stands for “Structured Query Language.” SQL is the most common standardized language used to access databases. Depending on your programming environment, you might enter SQL directly (for example, to generate reports), embed SQL statements into code written in another language, or use a language-specific API that hides the SQL syntax.

MySQL is open source:

Open source means it’s possible for anyone to use and modify the software. Anybody can download MySQL software from the internet and use it without paying for it. You can also change its source code to suit your needs. MySQL software uses the GNU General Public License (GPL) to define what you may and may not do with the software in different situations.

If you feel uncomfortable with the GNU GPL or need to embed MySQL code into a commercial application, you can buy a commercially licensed version from Oracle. See the MySQL Licensing Information section for more information.

**CHAPTER 4**

**COMPUTATIONAL METHOD**

**4.1 Overview**

In this verification system, a certificate is initially created and uploaded to the system. Upon upload, the certificate is converted into a specific hash value using a hash function. This hash value is then stored in a central authority's server. To verify a certificate, it is uploaded again, and its hash value is compared to the stored hash value in the server. If the hash values match, the certificate is considered valid and verified. This process helps maintain the integrity and authenticity of the certificates.

**4.2 Hash Function**

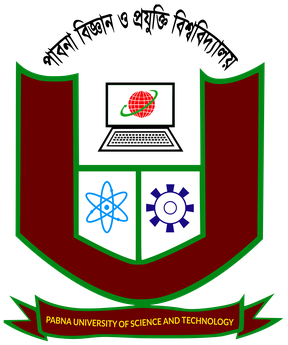
The working principle of a hash function involves the following key aspects:

* **Input Data:** A hash function takes an input, which can be any data of arbitrary size, such as a file, text, or binary data.
* **Fixed Output Size:** A hash function produces a fixed-size output, regardless of the size of the input. For example, the SHA-256 hash function always produces a 256-bit (32-byte) output.
* **Deterministic**: Given the same input, a hash function will always produce the same output. This property ensures consistency and predictability.
* **One-Way Function:** A hash function is designed to be computationally easy to compute in one direction but computationally difficult to reverse. It means that given the hash value, it is computationally infeasible to retrieve the original input data.
* **Collision Resistance:** A good hash function aims to minimize the likelihood of two different inputs producing the same output, known as a collision. Collision resistance helps ensure the uniqueness of hash values and the integrity of data.
* **Uniform Distribution:** A hash function should distribute its output uniformly across the entire range of possible hash values. This property ensures that small changes in the input produce significant changes in the resulting hash value.
* **Efficiency:** Hash functions are designed to be efficient, with fast computation times, regardless of the input size.

Hash functions find applications in various areas, including data integrity verification, password storage, digital signatures, and data retrieval structures like hash tables. By converting arbitrary data into fixed-size hash values, hash functions provide a way to summarize and verify the integrity of data efficiently.

**4.3 SHA-256**

Encryption and hashing have become fundamental principles in enhancing network security. One prominent hash algorithm is SHA-256, which employs a 256-bit digest size. This algorithm has gained significant popularity and is widely utilized due to its robustness and applicability in various real-world scenarios. Despite the existence of other variations, SHA-256 remains at the forefront of practical implementations, contributing to the advancement of network security.SHA-256 is indeed a member of the SHA-2 family of hash algorithms. The acronym "SHA" stands for Secure Hash Algorithm. Developed collaboratively by the National Security Agency (NSA) and the National Institute of Standards and Technology (NIST), SHA-256 was introduced in 2001 as a replacement for the SHA-1 family of algorithms. The need for a successor arose as SHA-1 was becoming vulnerable to brute force attacks, prompting the development of stronger and more secure hash functions within the SHA-2 family, with SHA-256 being one of the prominent members



a011733cfb7A591a6d40bf420404 A591a6d40bf420404

b190d62c65b

hello world

a91as56d40404a011733cfb70bf42 b190d62c65c

b190d62c65b

A591a6d40bf420404a011733cfb7

b190d62c65b

Hello World

SHA256

SHA256

SHA256

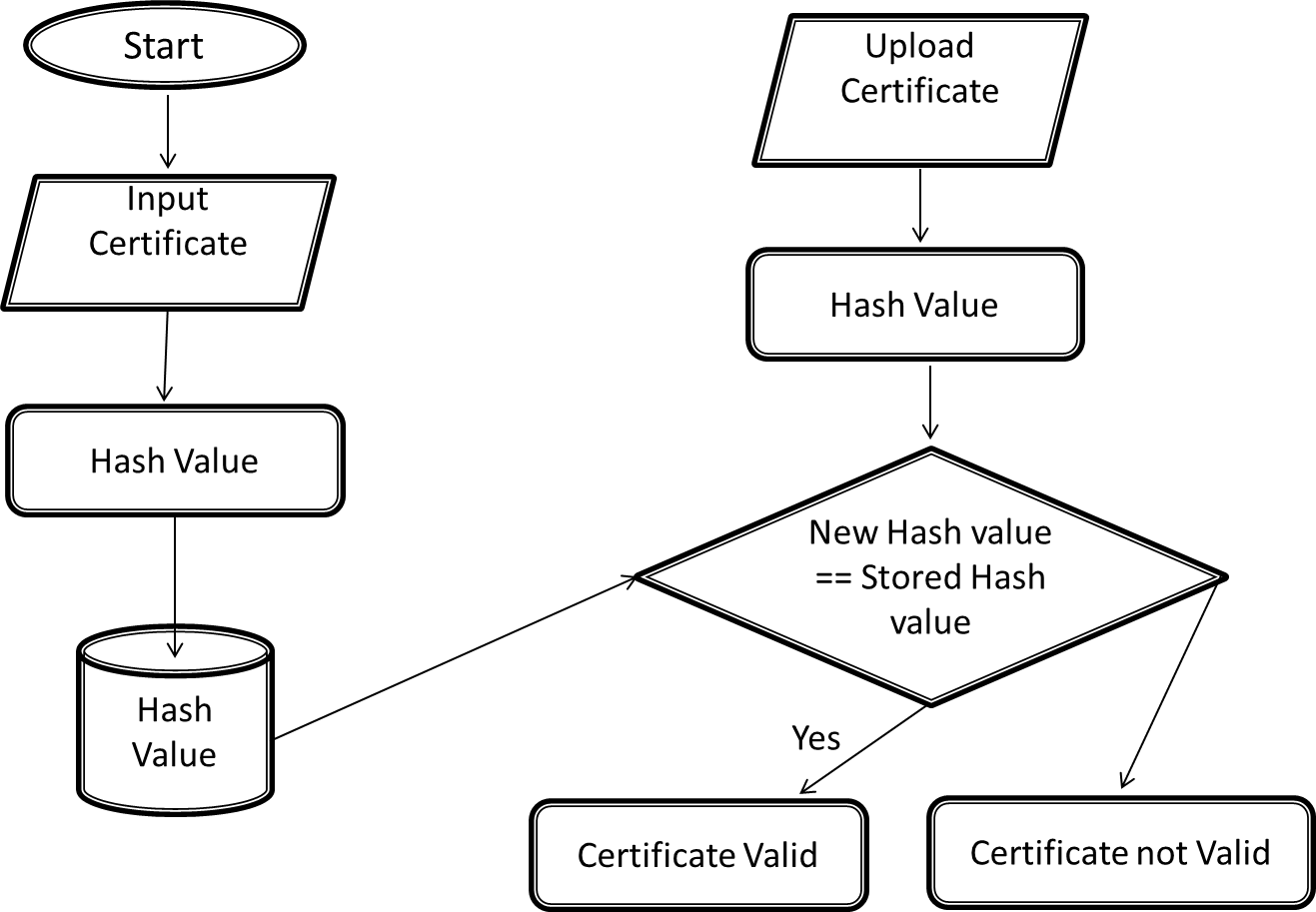
**Figure 4.1: Examples of Hash Function**

The SHA algorithm possesses several notable features, which include:

* Message Length: The SHA algorithm places a limit on the length of the input message to ensure the resulting hash digest remains sufficiently random. For SHA-256, the cleartext length should be less than 2^64 bits.
* Digest Length: Each variant of the SHA algorithm has a specific digest length. In the case of SHA-256, the hash digest is 256 bits, while SHA-512 has a digest length of 512 bits. Larger digest lengths generally indicate stronger security, but at the expense of increased computational complexity, speed, and storage requirements.
* Irreversibility: Hash functions like SHA-256 are intentionally designed to be irreversible. It means that it is computationally infeasible to retrieve the original plaintext message from the hash digest, and the digest itself cannot be used to reconstruct the original input. This property ensures the integrity and security of the hash function.

These features collectively contribute to the strength and security of the SHA algorithm family, including SHA-256, making them suitable for various cryptographic applications where data integrity, non-repudiation, and confidentiality are critical requirements.

**4.4 Flow Chart**



**Figure 4.2: Flow chart of hash function**

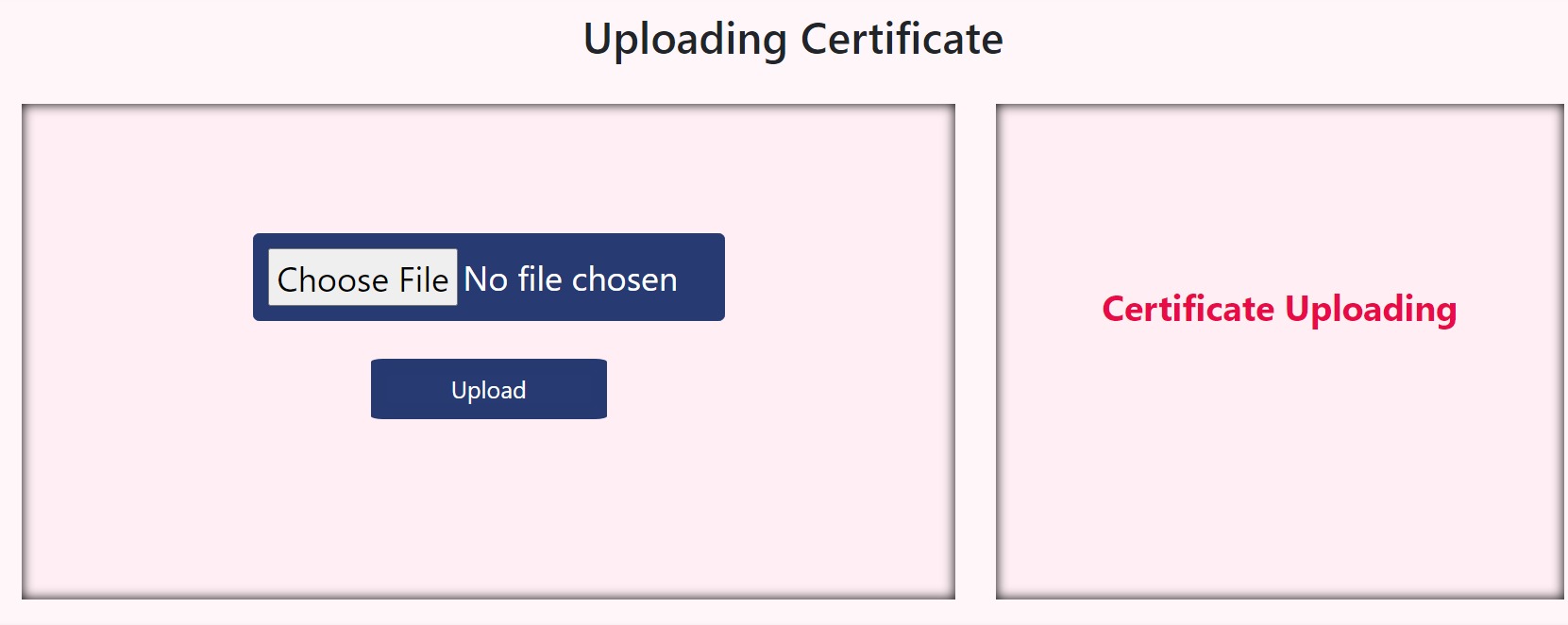
**CHAPTER 5**

**PROJECT OVERVIEW**

**5.1 Certificate uploading**

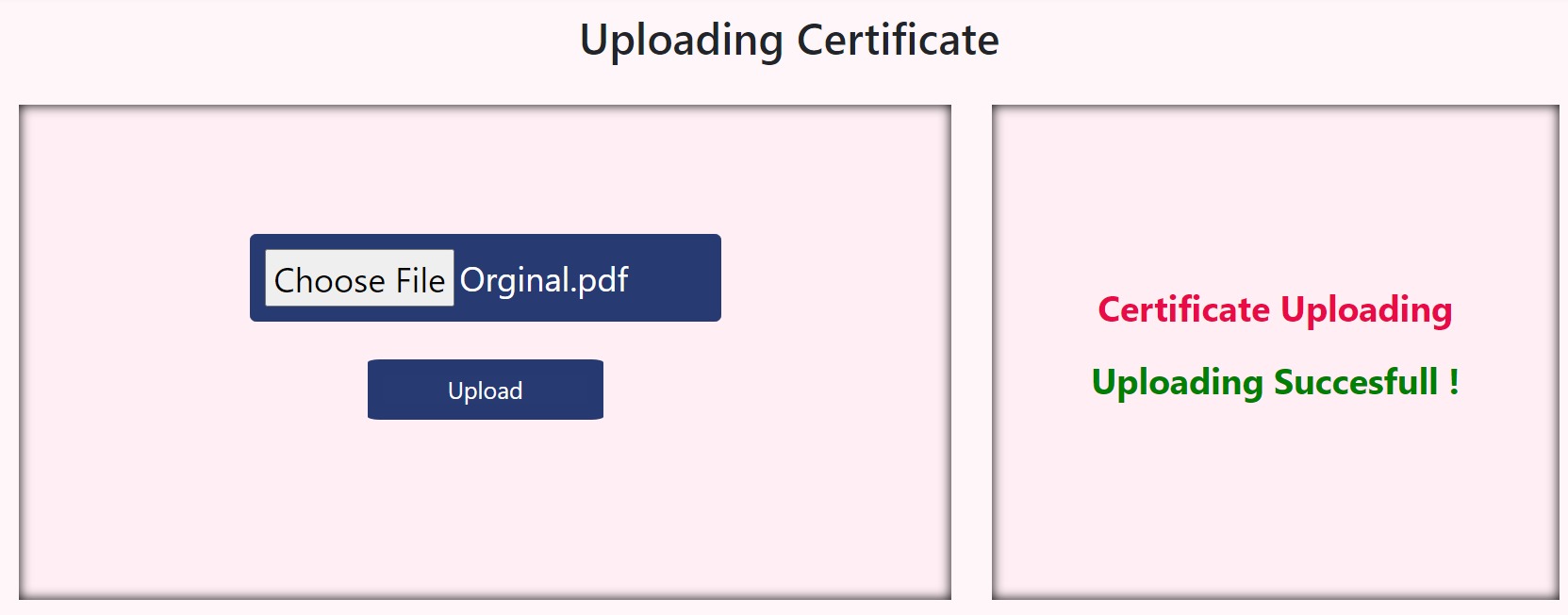
Upload the certificate, convert it using a hash function, store it in the database, and then display the message 'Certificate uploaded successfully

**5.1.1 Uploading Certificate**



**Figure 5.1: Upload Certificate**

**5.1.2 Uploading message**

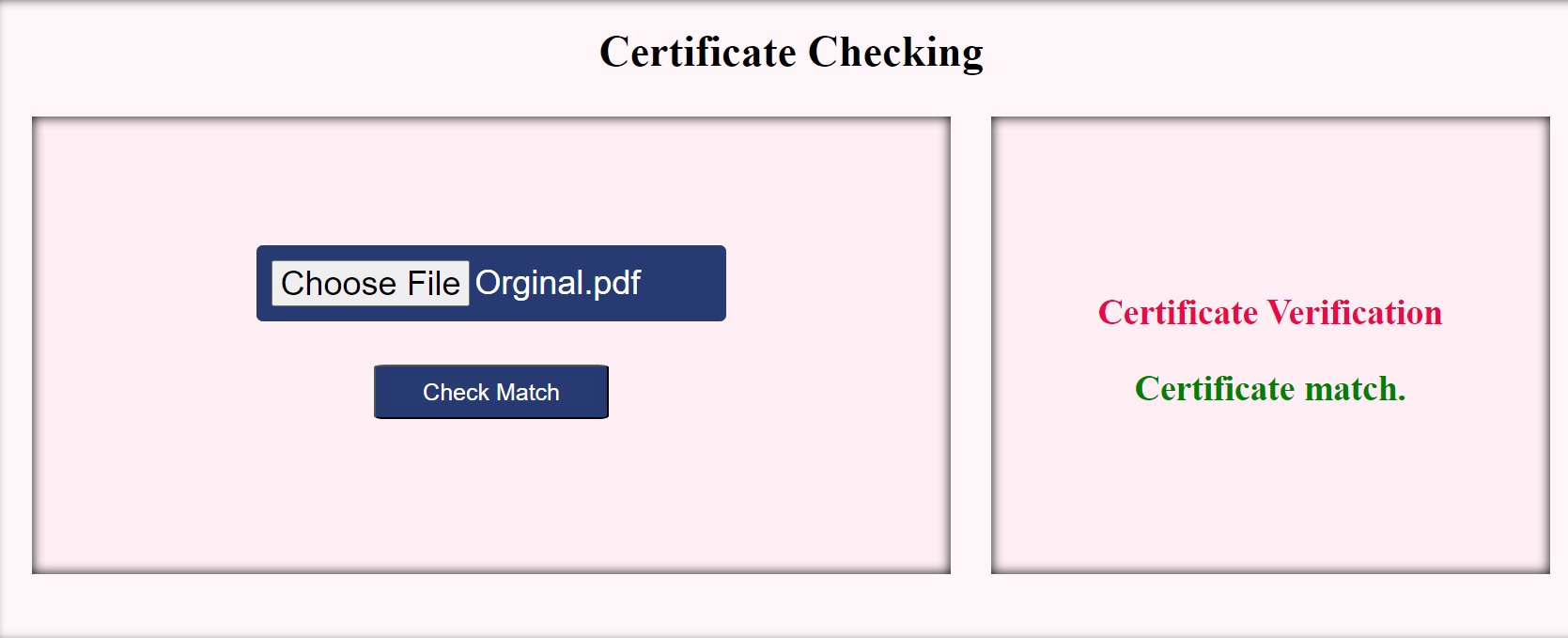


**Figure 5.2: Uploading message**

**5.2 Certificate Verification**

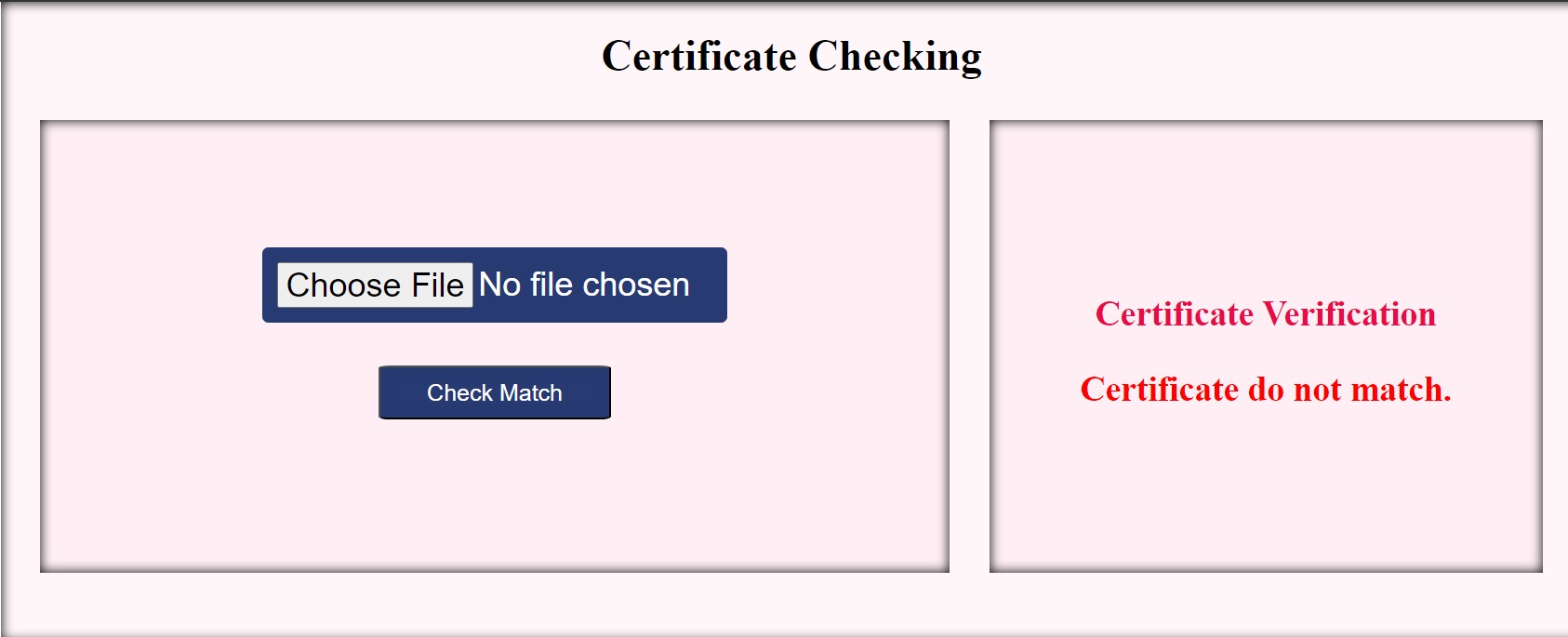
To verify a certificate, upload the certificate and convert it using a hash function. Then, compare the resulting hash value to the hash value stored in the database. If the hash values match, display a message indicating that the certificate matches. Otherwise, display a message indicating that the certificate does not match.

**5.2.1 If certificate match**

****

**Figure 5.3: Verification Message**

**5.2.2 If certificate does not match**

****

**Figure 5.4: Verification Message**

**CHAPTER 6**

**CONCLUSION AND FUTURE PLAN**

**6.1 Conclusion**

Certificate verification using hash functions plays a crucial role in ensuring the integrity and authenticity of digital certificates, which are essential for secure communication across the internet. Hash functions provide a unique and irreversible fingerprint for each certificate, allowing for reliable identification and verification. This mechanism protects against unauthorized modifications or tampering with certificates, preventing attackers from impersonating legitimate entities and compromising the security of online transactions.

**The use of hash functions in certificate verification offers several advantages:**

* **Integrity Assurance:** Hash values guarantee the unchanged nature of certificate content, ensuring that the information contained within the certificate remains unaltered.
* **Authenticity Verification:** Hash values enable the validation of a certificate's origin and issuer, preventing the issuance of fraudulent certificates by unauthorized parties.
* **Tamper Detection:** Any alterations to the certificate's content will result in a different hash value, immediately alerting the system to potential tampering.
* **Efficient Verification:** Hash functions provide a quick and efficient method for verifying the authenticity of certificates without the need to examine the entire certificate content.
* **Algorithmic Security:** Cryptographic hash functions are designed to be resistant to collision attacks, making it extremely difficult for attackers to create two different certificates with the same hash value.

The combination of hash functions with digital signatures further strengthens the security of certificate verification. Digital signatures allow the certificate issuer to cryptographically bind their identity to the certificate content, ensuring that the certificate originates from a trusted source. The hash value is then included in the signature, allowing the verifier to confirm that the certificate has not been tampered with since it was signed.

In conclusion, certificate verification using hash functions is a fundamental security measure in the realm of digital communications. It safeguards against unauthorized modifications, ensures the authenticity of certificates, and provides a reliable means of verifying the integrity of information exchanged across the internet.

**6.2 Future plan**

Certificate verification using hash functions is a critical component of digital security, ensuring the integrity and authenticity of digital certificates. As technology advances and security threats evolve, it is essential to continually enhance certificate verification mechanisms to maintain a robust and resilient digital infrastructure.

* **Post-Quantum Cryptography:** Quantum computers pose a significant challenge to traditional cryptography, including the hash functions currently used for certificate verification. To address this threat, research is underway to develop post-quantum cryptographic hash functions that are resistant to quantum attacks. These new hash functions will need to be standardized and integrated into existing certificate verification protocols.
* **Enhanced Hash Function Security:** Even with the development of post-quantum cryptography, it is crucial to continuously improve the security of hash functions. This includes exploring new algorithms, increasing hash function lengths, and developing techniques to mitigate potential vulnerabilities.
* **Transparency and Auditability:** Certificate verification processes should be transparent and auditable to ensure accountability and trust. This involves maintaining detailed logs of certificate issuance, revocation, and verification activities. These logs should be accessible to authorized parties for auditing purposes.
* **Automated Certificate Management:** Manual handling of certificates can be error-prone and time-consuming, making it vulnerable to human error and security lapses. Automated certificate management systems can streamline the issuance, revocation, and verification of certificates, reducing the risk of errors and improving overall security.
* **Integration with Emerging Technologies:** Certificate verification should be seamlessly integrated with emerging technologies, such as blockchain and the Internet of Things (IoT). This will require developing new protocols and standards that leverage the unique capabilities of these technologies to enhance certificate verification.

**REFERENCES**

1. Pathak, S., Gupta, V., Malsa, N., Ghosh, A. and Shaw, R.N., 2022. Blockchain-based academic certificate verification system—a review. Advanced Computing and Intelligent Technologies: Proceedings of ICACIT 2022, pp.527-539.
2. Rao, L.J., Rao, M.V. and Saradhi, T.V., 2016. How the smrtcard makes the certification verification easy. Journal of Theoretical and Applied Information Technology, 83(2), p.180.
3. Han, M., Li, Z., He, J., Wu, D., Xie, Y. and Baba, A., 2018, September. A novel blockchain-based education records verification solution. In Proceedings of the 19th annual SIG conference on information technology education (pp. 178-183).
4. Gresch, J., Rodrigues, B., Scheid, E., Kanhere, S.S. and Stiller, B., 2019. The proposal of a blockchain-based architecture for transparent certificate handling. In Business Information Systems Workshops: BIS 2018 International Workshops, Berlin, Germany, July 18–20, 2018, Revised Papers 21 (pp. 185-196). Springer International Publishing.
5. Gadelrab, M.S. and Abouhogail, R.A., 2021. Towards a new generation of digital calibration certificate: Analysis and survey. Measurement, 181, p.109611.
6. Hameed, B., Khan, M.M., Noman, A., Ahmad, M.J., Talib, M.R., Ashfaq, F., Usman, H. and Yousaf, M., 2019. A review of Blockchain based educational projects. International Journal of Advanced Computer Science and Applications, 10(10).
7. Awaji, B., Solaiman, E. and Albshri, A., 2020, July. Blockchain-based applications in higher education: A systematic mapping study. In Proceedings of the 5th international conference on information and education innovations (pp. 96-104).
8. Kornecki, A. and Zalewski, J., 2009. Certification of software for real-time safety-critical systems: state of the art. Innovations in Systems and Software Engineering, 5, pp.149-161.
9. Bertoldi, P. and Rezessy, S., 2008. Tradable white certificate schemes: fundamental concepts. Energy efficiency, 1(4), pp.237-255.