ITE 3962 – Final Year Project

Project Proposal

Multi Institutes Certificate Verification System

Submitted by:

Index: E2447028

Name: M.I.J.F.N.Isham

Bachelor of Information Technology (External Degree)

Faculty of Information Technology

University of Moratuwa

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

Abbreviation	Description
QR	Quick Response (Code)
OTP	One-Time Password
UI	User Interface
PDF	Portable Document Format
API	Application Programming Interface
URL	Uniform Resource Locator
FAQs	Frequently Asked Questions
AI	Artificial Intelligence
CSV	Comma Separated Values
PM	Process Manager
GIT	Global Information Tracker

LIST OF APPENDICES

1. Introduction

In the modern digital era, where information can be shared instantly across the globe, there is an increasing demand for educational and professional certificates to be issued, accessed, and verified electronically. Traditional paper-based certificates, though still in use, come with several critical challenges, including vulnerability to forgery, difficulties in physical storage, high risk of damage or loss, and the time-consuming process of manual verification. These issues pose significant obstacles not only for students and graduates but also for educational institutions, employers, and verification authorities.

Moreover, with the rise of online education, international programs, and short-term skill-based courses, a growing number of institutions are generating thousands of certificates each year. Managing and verifying these certificates manually is inefficient, error-prone, and impractical in the long run. Employers and other verifiers often struggle to confirm the authenticity of certificates due to lack of centralized systems and verification tools.

This project proposes a comprehensive, multi-institute digital certificate management and verification system, designed to eliminate these issues through the use of modern technology. The system will allow multiple institutions to register and manage their students, courses, and certificate issuance processes independently but within a unified platform. Certificates will be generated digitally, stored securely, and equipped with unique QR codes that link to an online verification portal. Each certificate will also carry a unique certificate code and award date, allowing verifiers to cross-check credentials with minimal effort.

The proposed system also includes automation features such as:

- Automatic certificate code generation based on institution ID and award date
- Real-time email notifications to students upon certificate issuance
- PDF certificates with embedded QR codes
- A public interface where certificates can be verified either by entering the code and award date or by scanning the QR code.
- OTP sent for Institute for verify the Institute.

This solution not only ensures the authenticity and traceability of certificates but also makes them easily shareable across digital platforms such as LinkedIn, email, and other social networks. By doing so, it empowers students to showcase their achievements more effectively while giving institutions a powerful tool to streamline and secure their certification processes.

In essence, this project aims to modernize the certificate management ecosystem, ensuring that digital credentials are trustworthy, accessible, and verifiable anytime and anywhere.

2. Background & Motivation

For decade, educational and professional institutions have relied on traditional paper-based certificates as proof of achievement, course completion, and qualification. While this method has been the norm, it suffers from significant limitations and vulnerabilities in today's fast-paced, digital-first world. physical certificates can be easily forged, lost, damaged, or tampered with, and institutions often lack the tools or systems needed to validate them efficiently. As a result, verification processes become, manual, slow, and unscalable, especially when dealing with large volumes of certificates or when verification is requested by third parties such as employers or government bodies.

This challenge has been further amplified by the rise of:

- Remote and online education platforms (e.g., MOOCs like coursera, udemy, and edx)
- Hybrid learning environments post-COVID-19,
- And global job markets, where candidates apply across borders with credentials that must be authenticated quickly.

In these scenarios, employees and educational evaluators often find it difficult to trust or verify certificates, particularly when there's no centralized or recognized authority behind the issuance. Moreover, institutions face the burden of storing physical records, responding to manual verification requests, and ensuring that duplicate or fake certificates are not distributed under their name.

This situation reveals a clear gap in the certificate lifecycle: from issuance to verification to usage in professional or academic settings. There is an urgent t need for a system that:

This situation reveals a clear gap in the certificate lifecycle: from issuance to verification to usage in professional or academic settings. There is an urgent t need for a system that:

- Digitizes the entire certification process,
- Ensures date integrity and security,
- Makes verification easy and instant,
- And reduces administrative load on institutions.

The motivation for this project stems from these very pain point. By creating a web-based, multi-institute digital certificate management and verification system, the goal is to eliminate forgery, simplify verification, and enhance trust and efficiency for all stakeholders involved.

In addition to security and convenience, this project is also inspired by the idea of empowering students-enabling them to receive, download, print, and share their certificates online through personalized URLs or QR codes. It also supports institutions by automating the certificate issuance process, managing students records more effectively, and presenting a professional, tech-enabled solutions to modern problems.

Overall, this project is not just a technical solution but a step forward toward digital transformation in the educations sector, ensuring that credentials are credible, portable, and future-ready.

3. Problem you address in brief

The current systems used by many educational institutions for issuing and managing student certificates are outdated, vulnerable, and inefficient. Most institutions still rely on manual, paper-based certificate issuance, which introduces several critical problems that affect students, institutions, and external verifiers alike.

a) Certificate Forgery and Duplication

One of the most serious challenges is the widespread possibility of certificate forgery. Without secure digital systems or authentication mechanisms, it is relatively easy for individuals to create fake certificates that appear legitimate. These forged certificates can be used to apply for jobs, further studies, or even immigration, leading to significant legal, financial, and reputational risks for institutions and employers. The lack of embedded security features, such as QR codes, digital signatures, or unique verification codes, makes it difficult to differentiate genuine certificates from falsified ones.

b) Manual and Time-Consuming Verification

In the absence of a centralized verification platform, employers and third-party agencies must manually contact institutions to verify the authenticity of certificates. This process is often time-consuming, involving emails, calls, and delays in response. Institutions, especially those dealing with large student populations, face administrative overload in responding to numerous verification requests, resulting in inefficiencies and frustration for all parties involved.

c) Risk of Loss or Misplacement of Certificates

Student often lose or damage their physical certificates, especially over time. Requesting replacements involves manual procedures, identity verification, fees, and delays. Furthermore, students have no easy way to digitally access or share their credentials for job applications or further studies, placing them at a disadvantage in an increasingly digital world.

d) No Centralized Platform for Multiple-Institute Certificate Management

Most systems currently in use are institution-specific and isolated, meaning that each organization manages its own certificate process without any interoperability or shared standards. There is no unified system where multiple institutions can manage, issue, and verify certificates within a

common, secure platform. As a result, scalability is poor, and institutions must often invest in their own expensive, custom solutions, which many smaller or mid-sized institutions cannot afford.

These issues highlight a clear need for a centralized, secure, and automated system that not only enables multi-institution certificate management but also ensures that verification is quick, accurate, and tamper-proof. By addressing these core problems, this project aims to bring transparency, efficiency, and trust to the certification process across the education sector.

4. Aim & Objectives

- Aim

The primary aim of this project is to design and develop a secure, scalable, and centralized web-based platform that enables multiple educational institutions to digitally issue, manage, and verify student certificates using automated authentication features, including QR code technology and real-time verification mechanisms. The system is intended to streamline certificate workflows, eliminate the possibility of forgery, reduce administrative burdens, and offer a user-friendly experience for students, institutions, and verifiers.

- Objectives

1) Design a multi-institute dashboard with authentication and verification workflows.
2) Enable secure certificate generation with automated code and dynamic content fields.
3) Generate QR codes with embedded verification links.
4) Notify students via email with downloadable digital certificates (PDF)
5) Allow real-time verification through QR code or unique certificate URL
6) Allow students to share certificates on social media via unique URLs.
7) Prevent certificate forgery and provide audit trails for verifications.

5. Proposed Solution

The project proposes a web-based certificate management and verification system designed to support multiple educational institutes. The system allows institutes to issue digital certificates with automated authentication, QR code integration, and real-time email notifications.

Institutes can manage courses, add students, upload certificate templates, and generate certificates with dynamic content like names, dates, and codes. A unique certificate code is automatically generated for each certificate, and a QR code is embedded for easy verification.

Users (students, employers, and third parties) can verify certificates through a public verifications portal by entering the certificate code and award date or scanning the QR code. Additionally, students receive certificates via email in PDF format with a unique URL, which they can print or share on social media.

The system will feature dashboards for super admin and institute admins, ensuring full control, verification transparency, and prevention of forgery or duplication of certificates.

Additional features:

Module	Description
AI Chatbot Support	Integrated chatbot to help users with FAQs or issue reports
Certificate Revocation	Revoke issued certificates if required and update status

Table 1- Additional Features

Advance Feature Implementations:

- Blockchain-backed certificate hashes (for unalterable verification)
- Bulk import/export options (CSV/Excel for institutes)
- API access for employers and third parties

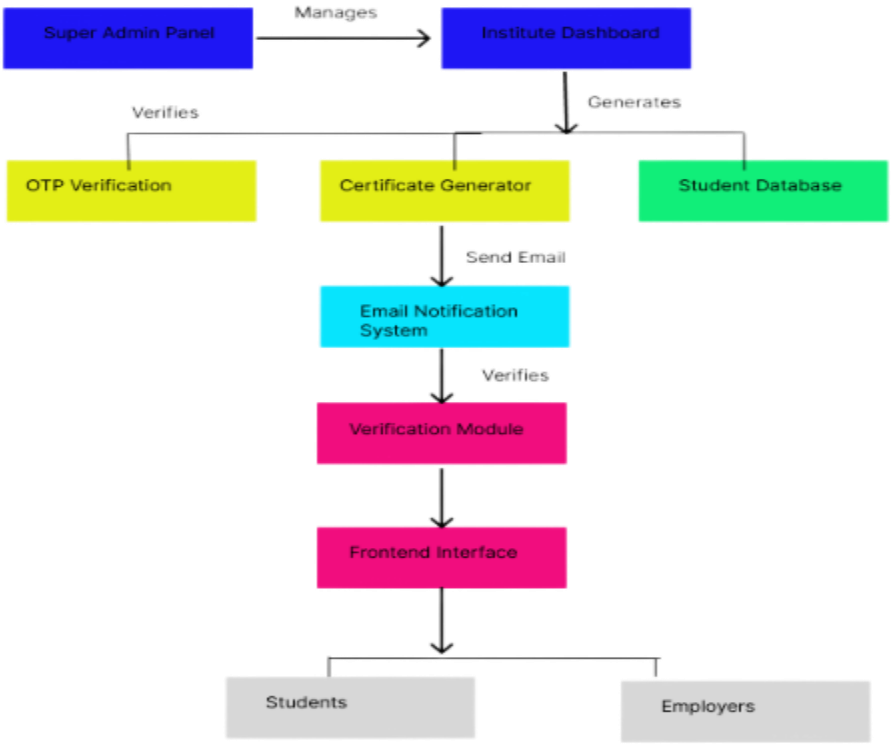

Figure 1- System Architecture

6. Resource Requirements

Layer	Technology
Frontend	React.js,
Backend	Node.js + Express.js
Database	MongoDB
AI chatbot	DialogFlow
UI Framework	Tailwind CSS
Version Control	GIT, GIT hub
PM2	Node Process Manager
NGINX	Reverse Proxy + Static Hosting
Security	JWT authentication

Table 2- Technical Requirements

Module	Feature
Super Admin Dashboard	Approve/verify institutes, manage access
Institute Dashboard	Add courses, students, certificate templates
Certificate Generator	Auto-generate code + QR + PDF
Certificate Verification	Public verification by QR scan or manual entry
Email Notification	Student receives certificate + link, code
Institute Verification	OTP receives
Social Sharing	Unique certificate URLs for social medias
AI chatbot	Help students or employers interact with the system

Table 3 - Functional Requirements

Reference List

[1] R. Luckin et al., “Intelligence Unleashed: An Argument for AI in Education,” Pearson Education, 2016.

[2] A. Hanspal, “Increasing the Value of Digital Credentials,” EdTech Digest, May 9, 2024. [Online]. Available: https://www.edtechdigest.com/2024/05/09/increasing-the-value-of-digital-credentials/

[3] Council of Europe, “Spotting the fakes: addressing education fraud in a digital age,” Council of Europe - Education, [Online]. Available: https://www.coe.int/en/web/education/-/spotting-the-fakes-addressing-education-fraud-in-a-digital-age.

Appendix A – Plan of Actions

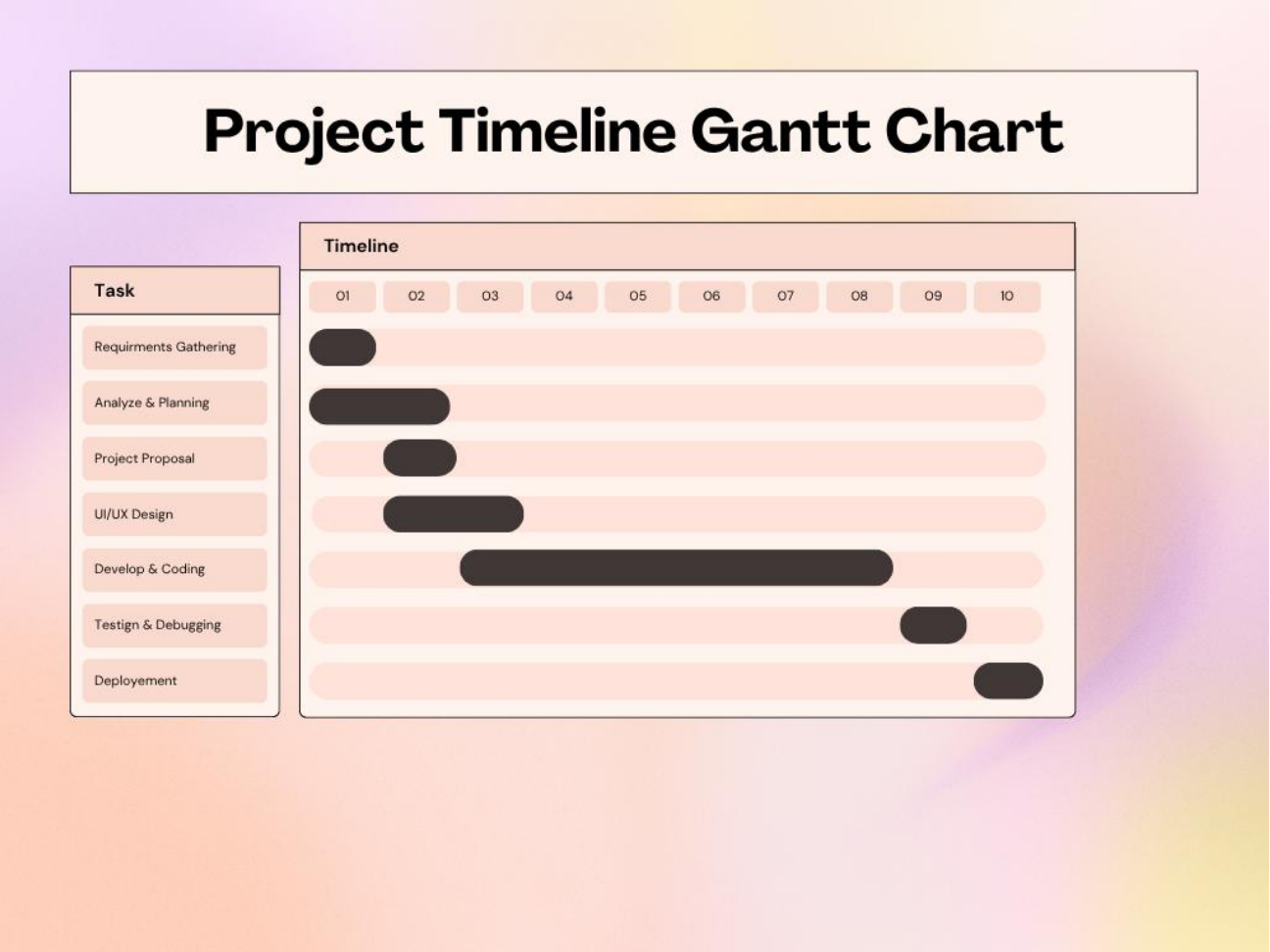

Figure 2 Project Timeline