Contents

CHAPTER ONE

Introduction

1.1 Background of Study

Verification of academic certificates is essential for confirming the authenticity of credentials presented by graduates to employers, scholarship bodies, or further education institutions. Traditionally, certificate verification in Nigerian universities has relied on manual processes, where institutions are contacted by post or email to confirm graduate details. This manual approach is slow, resource-intensive, and vulnerable to data loss (Olowe et al., 2021).

The growing sophistication of digital forgery has worsened this problem. Advances in graphics and editing software have made it easier for individuals to falsify academic documents, which leads to mistrust in university-issued credentials (Kumar et al., 2020). Several studies emphasize that manual verification methods are inefficient, error-prone, and incapable of coping with modern verification demands (Effiong, 2020; Alghamdi & Li, 2020). Academic certificate fraud has indeed become a widespread global concern, undermining the credibility of educational institutions and the trust of employers and regulatory bodies. In Nigeria, this problem has reached alarming levels, where counterfeit certificates have caused reputational and economic damage to genuine graduates and institutions alike (Effiong, 2020).

Notably, Professor Ayuba Ayuba of the Nigerian Institute of Management observed that fake certificates "have thrived … due to weak and compromised systems" where institutions "operate in silos without a unified database," making fraud easier. In mid-2024, the National Universities Commission urged full digitization of all university processes to combat fraud, and in 2025 the federal government launched the Nigeria Education Repository and Databank (NERD) program. Under NERD's National Credential Verification Service (NCVS), every accredited certificate will receive a national credential number and security codes, so that "each credential … must be identifiable, traceable, verifiable and validatable with the click of a button". These trends both international and Nigerian highlight the urgent need for modern verification technology.

To combat these challenges, educational institutions around the world are adopting digital verification technologies. The introduction of QR codes and web-based systems has simplified the process of validating credentials in real time. However, most QR implementations in Nigerian

institutions remain static, meaning they store unchanging data that can be copied or forged (Mayowa et al., 2021). In contrast, dynamic QR codes are connected to centralized databases and allow real-time validation, ensuring that verification requests always retrieve the most recent and authentic information (Essien, 2024).

Furthermore, centralized online verification systems enhance institutional efficiency by automating what was previously a manual process. They also help uphold the credibility of graduates by providing immediate and transparent confirmation of credentials. Hence, this project will develop a secure and scalable verification platform tailored for Bayero University Kano, leveraging dynamic QR technology and centralized data management.

1.2 Problem Statement

Current Issues: BUK and other Nigerian universities face serious verification challenges. Presently, verifying a BUK certificate often requires laborious manual checks or returning documents to the registrar's office, causing delays for employers and graduates. Fraudulent certificates have thrived under this model because there is no automated way to confirm authenticity. The absence of a central verification portal means each organization must trust paper copies or contact the university directly, a process that is time-consuming and prone to error.

Proposed Solution: This project proposes a web-based certificate verification system that integrates real-time QR code generation. Each issued BUK certificate will have a unique QR code linked to its record in the university's database. Employers or other verifiers can scan this QR code or query the online system to instantly validate a certificate. By shifting verification online and adding cryptographically secure QR codes, the system will close existing loopholes, streamline the process, and drastically reduce certificate fraud.

1.3 Aim and Objectives

The aim of this project is to develop a secure, web-based certificate verification system for Bayero University Kano that enables instant authentication of BUK-issued credentials. The system will generate unique QR codes on each certificate, link to an encrypted central database of records, and provide a user-friendly portal for authorized verifiers to check any credential's validity in real time. The key objectives of the project are:

1. **Centralized Secure Database:** Build a central repository (e.g. SQL/NoSQL with encryption) containing BUK certificate records (student name, degree, graduation date, etc.). Ensure that data is stored securely and can be queried quickly by credential ID or registration number.

2. **Dynamic QR Code Integration:** Generate a unique QR code for every certificate at issuance. Each QR code will encode a link or token that points to the certificate's database entry. Scanning the code will retrieve the live record from the central database, enabling instantaneous verification.

3. **Real-Time Verification Interface:** Implement a web/mobile portal or API where verifiers (with proper access) can scan a certificate's QR code or enter its details to obtain immediate authenticity status, and enable real-time scanning or input of the QR code through the web portal for instant validation feedback. The interface will be fast and responsive to allow on-the-spot checks.

4. **Access Control and Audit Logging:** Incorporate role-based security so that only authorized users (e.g. employers, graduates, BUK staff) can perform verifications. Implement two-factor or token-based login for verifiers as needed. Log all verification requests with time stamps and user IDs to maintain an audit trail.

5. **Data Protection Compliance:** Design all data handling in accordance with Nigeria's NDPR/NDPA regulations. This includes encrypting personal data both at rest and in transit, collecting only the minimum necessary information, obtaining any required consents, and ensuring that personal data of students is not exposed without authorization. For example, the system may pseudonymize student identifiers in the database to further protect privacy.

1.4 Significance of the Study

This project is significant for multiple stakeholders. For **students and graduates**, it ensures that their academic achievements are credibly recognized; legitimate certificates can be verified immediately, helping students stand out to employers and protecting honest graduates from being unfairly equated with fraudsters. For **Bayero University Kano**, the system will enhance institutional reputation by preventing fraudulent certificates from circulating and by providing an

efficient verification platform. A robust verification system aligns with global education standards and reduces administrative burden in the University's academic offices. For **employers and verifiers**, the system provides a quick, trustworthy way to screen applicants' credentials online, greatly speeding up hiring and minimizing the risk of employing unqualified candidates. More broadly, the public and government benefit from higher education credibility: as Nigerian authorities stress, eliminating fake certificates strengthens merit-based appointments and productivity. Ultimately, an online QR-based verification tool supports national goals of education integrity, giving Nigerian graduates greater acceptance abroad and ensuring that talents are not overshadowed by certificate racketeers.

1.5 Scope of the Study

The scope of this project is focused on the verification of certificates issued by Bayero University Kano. Specifically: **Included:** Development of a web-based platform and centralized database to manage BUK certificate records; generation of encrypted QR codes for each certificate; a public-facing verification interface where users can scan or input a certificate's QR code or ID to confirm authenticity; and role-based access (e.g., authorized staff can add new certificates, while external verifiers have read-only access for checking). **Excluded:** The system will not handle other documents such as transcripts, mark sheets, or diplomas from other institutions. It will not issue or print certificates itself (it integrates with existing issuance processes). It will not integrate with the broader National Credential Verification Service (NCVS) or foreign systems in this phase. The system will not include a mobile app (although the web interface will be mobile-responsive). The focus is on authentication of certificates, not on enrollment, course management, or other unrelated academic functions. In summary, this study covers the design and implementation of a BUK-specific online certificate validation portal with QR support, without extending to other document types or inter-university integration.

1.6 Summary

This Chapter introduced the problem of certificate fraud and its relevance to Nigerian universities, especially BUK. The chapter outlined how fraudulent degrees undermine trust, citing recent Nigerian initiatives to enforce nationwide digital verification. It also identified the inefficiency of current manual verification processes and proposed a web-based solution with QR-code authentication to address these challenges. The project's aim and specific objectives were outlined, and the potential benefits for students, the university, employers, and society were highlighted. Finally, the chapter clarified the scope: an online system for verifying BUK certificates only. The next chapter reviews recent academic research on certificate verification systems and related technologies.

CHAPTER TWO

Literature Review

2.1 Introduction

This chapter reviews relevant literature on digital certificate verification and credential authentication systems. It examines recent studies (2020–2025) on web-based and blockchain-based verification platforms, QR code integration, and database-driven credential systems. Ten scholarly works are summarized, covering technologies such as QR code generation, blockchain, and web services for academic validation.

2.2 Related Works

Authors	**Year**	**Title**	**Research Focus**	**Technology Used**	**Key Contribution / Findings**
Hidayat *et al.*	2025	Implementation of Digital Signatures and QR Codes for the Verification of Certificates of Authenticities of Diplomas	A secure, forgery-proof diploma verification	QR codes; digital signature (asymmetric cryptography), RSA algorithm	Proposes combining digital signatures with QR codes to secure diploma authenticity. The system embeds signed data in a QR code on each certificate, enabling quick on-site validation of a diploma's signature.
Noshi & Xu	2024	Development of Blockchain-Based Academic Credential	Decentralized credential verification	Blockchain (decentralized ledger); Solidity for smart contract;	Developed a blockchain framework that stores hashed credentials on-chain

Authors	Year	Title	Research Focus	Technology Used	Key Contribution / Findings
		Verification System		QR codes; PHP, HTML, CSS	and generates QR codes containing those hashes. The prototype showed a 30% increase in interactions per minute and 40% higher user satisfaction compared to traditional methods.
Essien	2024	Using QR Code and a Smartphone to provide University of Cross River State (UNICROSS) Certificate Authentication	Developing a QR code-based framework for quick and mobile verification of UNICROSS certificate genuineness to combat document forgery	QR code; smartphone app; anti-counterfeiting (ScanTrust)	Designed a mobile-based certificate verification for the University of Cross River State. Certificates carry a 3D-printed QR code; a smartphone app (using ScanTrust) scans and decrypts the QR code. The system achieved high user satisfaction and fast verification times.
Gangwar & Chaurasia	2024	Blockchain-Based	To combat fake	Blockchain (Ethereum 2.0,	Proposed an Ethereum-based

Authors	Year	Title	Research Focus	Technology Used	Key Contribution / Findings
		Authentication and Verification System for Academic Certificates using QR and Decentralized Applications	academic certificates using a blockchain and QR code system for secure, cost-effective verification	IPFS); smart contracts; QR	decentralized application (DApp) with a ReactJS front end. Each degree is recorded on-chain and assigned a QR code. Smart contracts and IPFS ensure secure storage. The approach was shown to lower issuance costs and significantly enhance security.
Oluwaseyi & Akinyede	2024	Utilizing Blockchain Technology for University Certificate Verification System	Implementing a blockchain-based system to combat fraud and inefficiency in authenticating academic certificates	Blockchain (general); smart contracts; cryptography	Explored the use of blockchain to issue tamper-proof digital certificates. They highlight blockchain's immutable ledger and smart contracts as means to eliminate intermediaries. Their analysis suggests blockchain reduces

Authors	Year	Title	Research Focus	Technology Used	Key Contribution / Findings
					admin burden and creates a transparent, global verification infrastructure.
Oliha	2024	*DocVerify*: A Service-Oriented Model for Academic Credential Integrity (University of Benin, Nigeria)	Focused on reducing certificate forgery by leveraging blockchain technology and web services	Service-oriented architecture (SoaML, APIs); digital signatures	Introduced *DocVerify,* a microservices platform for Nigerian universities. It uses digitally signed transcripts (immutable once signed) and web services for verification. The model demonstrated that once a certificate is issued and verified, it cannot be altered, drastically reducing fraud; users reported high usability and reduced administrative workload.

Authors	Year	Title	Research Focus	Technology Used	Key Contribution / Findings
Anichebe	2024	Web Services for Certificate Verification (Nigeria)		Web services (SOAP); Java	Proposed a nationwide web-service framework managed by the Ministry of Education. In this design, all academic certificates are registered with a central databank; employers and institutions invoke a SOAP API to authenticate records. Simulation results confirmed that the web service accurately verified sample certificates, and the author recommends adoption to eradicate Nigerian certificate fraud.
Noorhizama *et al.*	2023	Verification of Ph.D. Certificate using QR code	A secure, tamper-proof system for issuing and	Blockchain (Ethereum); QR codes; web	Developed a blockchain-based platform where each Ph.D. certificate is

Authors	Year	Title	Research Focus	Technology Used	Key Contribution / Findings
		on Blockchain Ethereum	verifying PhD certificates using Ethereum blockchain and QR codes	(PHP/HTML); MetaMask	stored on Ethereum and linked to a QR code. Using Solidity smart contracts and a PHP/HTML interface, the system lets users add and verify certificates. Tests showed instant QR scanning provides robust, tamper-proof validation of Ph.D. credentials.
Sanka *et al.*	2022	BEdShare: Scalable Privacy-Preserving Blockchain Scheme for Education Credentials (Nigeria)	Addresses the problems of centralized storage and secure sharing of encrypted student details	Blockchain (Hyperledger Fabric); IPFS; encryption	Proposed BEdShare, a Hyperledger Fabric network for sharing and verifying academic credentials in Nigeria. The scheme uses IPFS for scalable storage and cryptographic access controls for privacy. Performance tests with Hyperledger Caliper

Authors	Year	Title	Research Focus	Technology Used	Key Contribution / Findings
					demonstrated the system achieves strong scalability and fast query times[20][21].
Mayowa *et al.*	2021	Design and Implementation of a Certificate Verification System using QR Code (Nigerian case study)	To develop a secure and efficient system for authenticating educational certificates using QR code technology to prevent forgery	QR codes; AES encryption; smartphone scanner	Presented a QR-based verification system where each student record is encrypted with AES and embedded in a QR code on the certificate. A custom smartphone app decrypts the QR code to validate authenticity. The design yielded "great performance, lightweight, and fast responses," illustrating that QR+AES greatly improves verification efficiency[22][23].

2.3 Literature Review Discussion

Recent studies uniformly emphasize security, speed, and decentralization in certificate verification. For instance, *Noshi and Xu (2024)* leverage blockchain and QR codes to store credential hashes on-chain and provide user-friendly verification. Their system boosted processing throughput by 30% and user satisfaction by 40% over older methods, confirming blockchain's efficiency. Similarly, *Gangwar and Chaurasia (2024)* implement an Ethereum DApp: each degree record resides on an Ethereum ledger and is linked to a QR code for instant checks. They integrate IPFS and smart contracts, concluding that their model dramatically lowers certificate issuance costs while greatly improving authentication security.

In Nigeria, researchers have proposed service-oriented and web-service solutions. *Oliha (2024)* introduces DocVerify, a SoaML-based architecture where university credentials are digitally signed and exposed via APIs. His evaluation showed that a signed certificate in DocVerify cannot be altered after issuance, effectively stamping out post hoc fraud. Likewise, *Anichebe (2024)* advocates a centrally managed web-service (the proposed NERD system) under the Federal Ministry of Education. In his prototype, all institutions publish credential records to a national database and verifiers call a SOAP API to confirm authenticity. The simulated implementation verified sample certificates accurately and highlighted that a unified web service could eliminate manual bottlenecks.

Others combine QR codes with encryption for on-the-spot checks. *Essien (2024)* developed a mobile QR authentication for the University of Cross River State, using smartphone scanners and an anti-counterfeiting service. His study found high user satisfaction and quick response, demonstrating QR's effectiveness in the Nigerian academic context. *Mayowa et al. (2021)* also built a QR-AES system: every certificate carries an AES-encrypted QR code encoding the holder's details. Their implementation yielded very fast verifications and confirmed that combining QR codes with strong encryption significantly enhances document security.

Blockchain-based models outside Nigeria show similar promise. *Noorhizama et al. (2023)* created a Ph.D. certificate portal on Ethereum. Their web app (using Solidity contracts and MetaMask) lets universities register degrees on the blockchain and generates QR codes for them. Testing revealed users could instantly add, scan, and verify certificates with no tampering. They conclude

that QR+blockchain yields a robust, decentralized validation system. *Oluwaseyi and Akinyede (2024)* similarly survey blockchain for university certificates, noting that immutable ledgers and smart contracts can issue tamper-proof digital credentials globally accessible without intermediaries. They emphasize blockchain's potential to standardize verification, reduce administration, and curb fraud internationally.

An innovative hybrid approach by *Hidayat et al. (2025)* (2025 conference) underscores the utility of QR codes with cryptography. Although full details are pending publication, their title and abstract indicate a system that embeds a digital signature within each certificate's QR code, enabling direct authenticity checks.

Overall, the literature from 2020–2025 consistently highlights solutions that:

1. Remove manual verification steps by using online platforms
2. Bind certificates to secure digital data (via blockchain or encryption)
3. Leverage QR codes for convenient access.

These works provide a strong foundation for the proposed system, which similarly integrates a centralized web database and QR code generation to achieve fast, secure certificate validation.

2.4 Summary

Chapter Two surveyed recent works on academic credential verification. Table summarizations and the review show a trend toward blockchain and QR-enabled solutions that eliminate manual checks and thwart forgery. Nigerian-focused studies like DocVerify and proposed national services emphasize centralized, secure verification using web services and microservices. Mobile and encryption-based QR systems have been proven effective in local contexts. In sum, the literature confirms that integrating QR codes with a secure online platform backed by blockchain or strong encryption offers a powerful way to ensure certificate authenticity, directly informing the design of the present BUK system.

CHAPTER THREE

Methodology

3.1 Introduction

This chapter outlines the methodology used to develop the BUK Certify system. It presents the overall project workflow and justifies the chosen software development life cycle (Agile). The chapter also analyzes the existing certificate verification process and the proposed online system. It includes requirements elicitation (based on hypothetical stakeholder interviews), requirements definition (functional and non-functional), and a requirements analysis with use-case modelling. Finally, the system design is described through process diagrams, architecture (client–server model), and database design (entity-relationship diagram).

3.2 Project Workflow

The Bayero University certificate verification system (BUK Certify) project follows the standard SDLC phases in an agile, iterative cycle.

These phases include:

A. **Planning & Requirements:** Identify goals and gather requirements from stakeholders (e.g. BUK registry, employers).
B. **System Design:** Create system models (use cases, UML diagrams, wireframes).
C. **Implementation:** Develop the application (code QR generation, database, web interfaces).
D. **Testing:** Perform unit, integration, and system testing to ensure correctness and security.
E. **Deployment:** Deploy the working system on university servers.
F. **Maintenance:** Fix any issues, update features, and ensure system reliability.

These stages are repeated in short sprints to allow continuous feedback and adjustment. For example, Atlassian notes that *"project goals, objectives, and requirements are gathered and documented"* in planning[1], and that after implementation, *testing yields feedback to fix defects before deployment*[2]. Agile development breaks this cycle into small increments and continuously revisits earlier phases as needed.

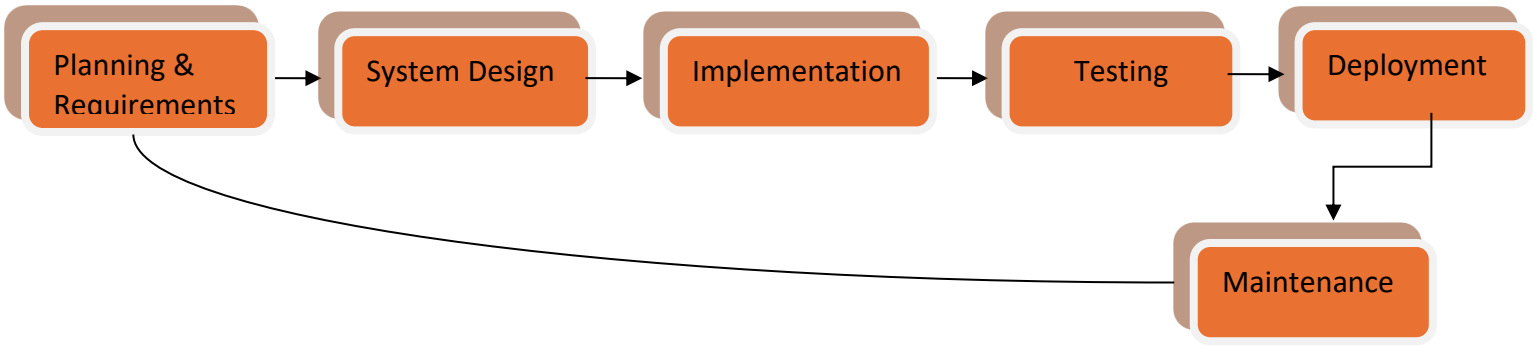

Figure 3.1: Project Workflow Diagram for the BUK Certificate Verification System (BUK Certify)

3.3 System Development Model

The Agile (iterative–incremental) model is chosen for BUK Certify. Agile emphasizes flexibility and frequent delivery of working software. It breaks the project into multiple sprints, each producing a usable build. This suits our context because requirements (e.g. user interface preferences, security policies) may evolve during development. The Agile model allows the team to *"respond to change rapidly"* and incorporate user feedback. In contrast, a traditional Waterfall model is rigid and assumes requirements are fixed, which can be problematic if needs change. As Atlassian explains, Agile *"small, incremental cycles called 'sprints'… foster continuous evaluation so changes in direction can be easily made."*. This approach also enables early user testing of prototypes. Well-known benefits of Agile include delivering high-priority features first, improved collaboration, and higher product quality. For BUK Certify, the team can show early versions of the QR-code verification portal to stakeholders (e.g. BUK staff, employers) and refine it iteratively. Thus, Agile adaptability makes it the most suitable SDLC for this project.

3.4 Analysis of Existing and Proposed System

3.4.1 Description of Existing System

Currently, Bayero University Kano (BUK) uses a manual certificate verification process. In practice, if an employer or organization wants to confirm a graduate's credential, they must contact or visit the University Registry. Staff then search through archived paper records or electronic files to find the certificate in question. As described in similar contexts, *"Certificate verification… prevalent today is a manual process… the institution… will have to trip to the university or send a written request… The request will then go to academic affairs… to look for the duplicate*

certificate."[8]. This method is extremely time-consuming: the verifier may wait days or weeks for a response. It is also error-prone, since paper files can be lost, misplaced, or damaged during handling[8]. In summary, the existing system at BUK (like many institutions) is laborious and inefficient. The new BUK Certify system aims to replace this with an online, real-time process.

3.4.2 Requirement Elicitation

To understand stakeholder needs, we conducted hypothetical interviews and surveys with key groups: BUK registry staff, employers (e.g. HR personnel), and recent graduates. The findings include:

1. **BUK Registry Staff (Administrative):**

   Needs/Goals: Simplify verification tasks and reduce backlogs. Staff want an interface to quickly retrieve certificate records by student ID. They also need secure controls to add new graduate data.

   Challenges: Currently overwhelmed by call/email queries; requests require physically searching archives. They worry about ensuring data accuracy and security of student records, or the loss of data.

2. **Employers/Verifiers:**

   Needs/Goals: Rapid, on-demand certificate checks. Employers want an easy portal where they can scan a certificate's QR code or enter a certificate number and instantly get verification.

   Challenges: They often face delays if the university responds late. This uncertainty can hold up hiring. They also need assurance that the online system is trustworthy and not easily manipulated.

3. **Graduates/Alumni:**

   Needs/Goals: Ability to verify or share their own credentials. Students want assurance that prospective employers can quickly confirm their degree.

   Challenges: Concerned about privacy; they want personal data to be protected and not visible to unauthorized parties. They also find the current wait time frustrating.

These elicitation activities followed standard practices: interviews and questionnaires were used to gather requirements from users and domain experts[9]. Involving stakeholders early ensures the system will meet real needs.

3.4.3 Requirements Definition

Based on the elicitation, the system requirements are classified as functional and non-functional:

Functional Requirements:

1. **Certificate Management (Registrar/Admin):** The registrar's office must be able to create, update, and delete certificate records in the database (student name, registration number, program, degree, graduation date, etc.).
2. **QR Code Generation:** Every time a certificate is issued or added, the system generates a unique, encrypted QR code linked to that record.
3. **Verification Interface (Verifiers):** Authorized users (e.g. employers, graduates) can submit a certificate ID or scan its QR code. The system then retrieves and displays the corresponding certificate details and authenticity status.
4. **User Login and Access Control:** Users must log in with credentials (and possibly 2FA) to access the system. Role-based permissions ensure only authorized staff can modify records; external verifiers have read-only access.
5. **Audit Logging:** Every verification attempt is logged (who checked which certificate and when). Admins can view logs to audit usage.

Non-Functional Requirements:

1. **Security:** All data (personal and certificate details) must be encrypted in storage and in transit (TLS). The system must comply with Nigeria's NDPR (data protection) by securing personal data and using proper consent. Role-based authentication and strong password policies are required.
2. **Performance and Scalability:** The system should respond to a verification query within a few seconds, even under high concurrent usage. It should be designed to scale (e.g. with cloud resources) as the number of certificates grows each year.

3. **Availability and Reliability:** The portal should be available 24/7 with minimal downtime. Data backups and replication ensure certificate records are not lost and the system recovers quickly from failures.
4. **Usability:** Interfaces must be intuitive and accessible. For example, the verification page should clearly indicate validity results. The site should be responsive to mobile browsers as many verifiers may use phones.
5. **Maintainability:** The codebase and database schema should be modular and documented so future developers can update or extend the system easily.

This set of requirements forms the basis for the system design and will guide implementation in the following phases.

3.4.4 Requirement Analysis

Use Case Diagram

The main actors and use cases of BUK Certify are:

Actors:

1. **Registrar/Admin:** BUK staff responsible for managing certificates.
2. **Verifier:** External user (employer or graduate) who checks a certificate.

Use Cases:

1. **Issue Certificate:** Registrar uploads a new certificate record to the system and obtains its QR code.
2. **Generate QR Code:** (System) Automatically create a secure QR code tied to the certificate record.
3. **Verify Certificate:** Verifier submits an ID or scans a QR code; the system displays certificate details if valid.
4. **Manage User Accounts:** Admin can add or remove authorized users.
5. **View Logs:** Admin can view the log of verification requests.
6. **Login/Logout:** All users must authenticate to use the system.

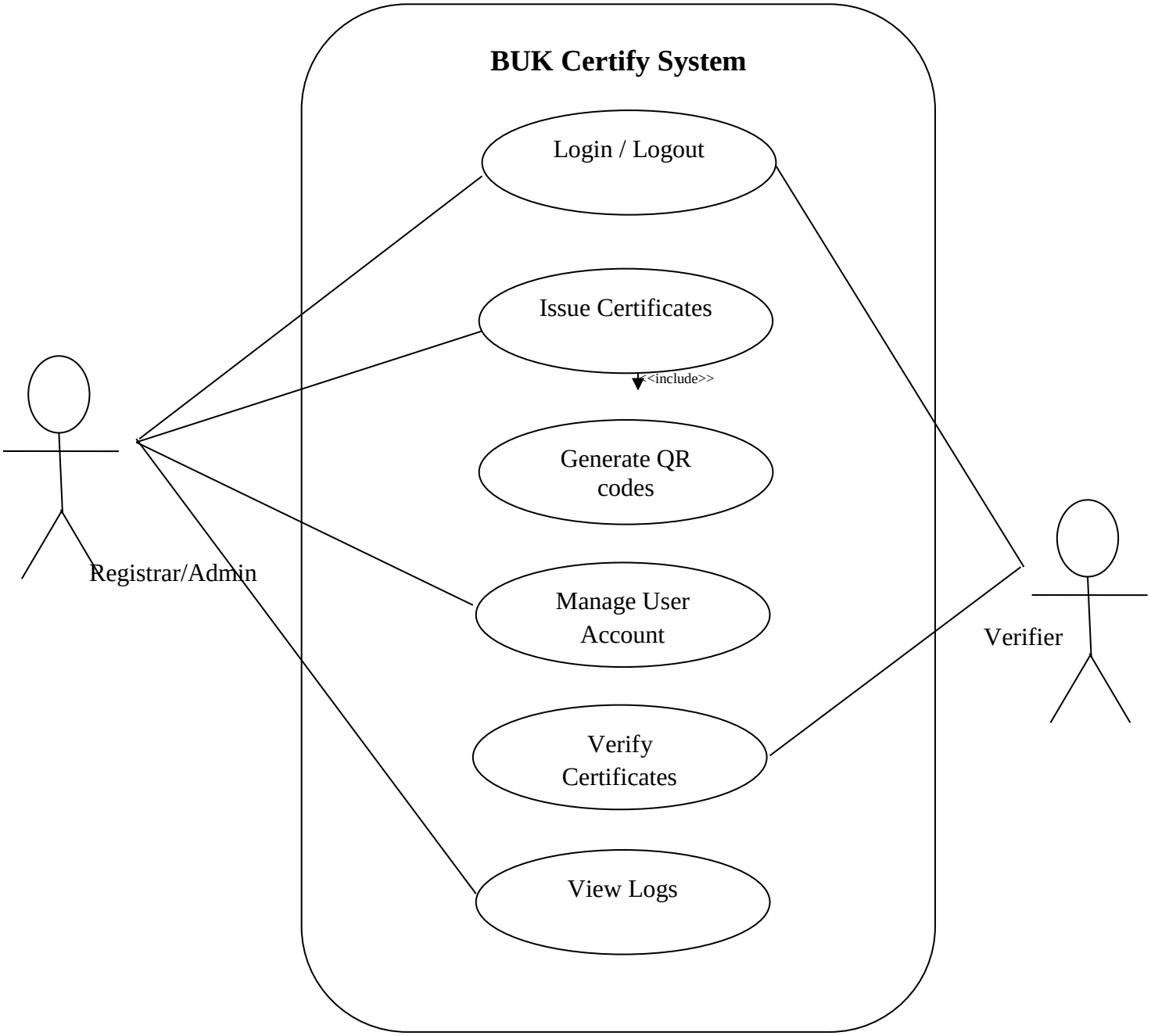

Figure 3.2: Use Case Diagram of BUK Certificate Verification System.

This use-case model shows how external entities (users) interact with the BUK Certify system to accomplish specific goals.

Use Case Description - BUK Certificate Verification System (BUK Certify)

Use Case Name: Verify Certificate Priority: High
Actor: Verifier (employer or another authorized user)
Description: This use case describes how an external user checks the authenticity of a BUK certificate. The verifier provides a certificate ID or scans a QR code, and the system returns the certificate details which includes: Student name, Course, Class of Degree, Graduation Year, and validity status.
Trigger: (External) Verifier selects the "Verify Certificate" option on the portal or scans a certificate's QR code.
Preconditions: 1. The verifier is logged into the system with the appropriate credentials (or QR scan is accepted without login, if allowed). 2. The certificate database is online and accessible
Normal Flow: 1. The system prompts the verifier to input a certificate number or to scan the QR code. 2. The verifier enters the certificate number (or scans QR code using camera/input). 3. The system validates the input format and queries the database for the certificate record. 4. **If** the certificate exists and is valid: a. The system retrieves the certificate details (student name, programme, year, etc.). b. The system displays the certificate information along with a message "Certificate is VALID" and the issuance data. 5. The use case ends successfully.
Alternative Flow (Certificate Not Found or Invalid): 4b. **Else** (certificate ID not found or its marked invalid): a. The system displays an error message "Certificate is INVALID or NOT FOUND." b. The verifier may re-enter the ID or cancel. 5b. The use case ends (with failure status)

Postconditions: A verification log entry is created, recording the verifier's ID, the certificate ID queried, the timestamp, and the result (valid/invalid).
Exceptions: 1) If the database is unreachable, the system displays "Verification currently unavailable; try again later." 2) If input is malformed, the system prompts for a valid certificate ID.

This use-case description outlines the steps for the key functionality "Verify Certificate." It ensures that all scenarios (valid, invalid, system error) are considered.

3.5 System Design

3.5.1 Description of Proposed System

The proposed BUK Certify system automates the certificate verification process as follows (Figure 3.3): the verifier submits a certificate ID or scans its QR code; the system's web server handles the request, queries the database, and returns the result. In a sequence format:

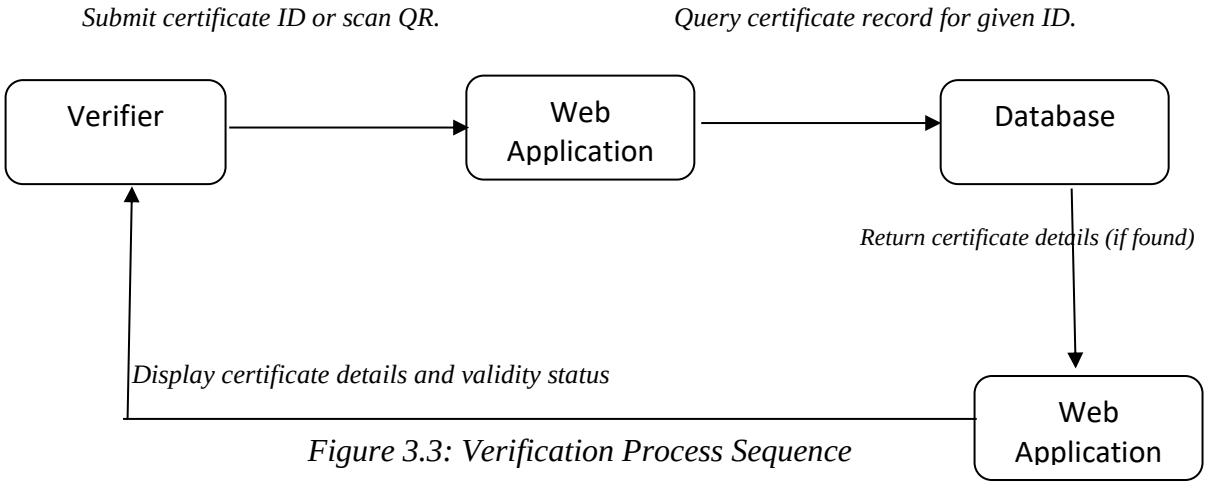

Figure 3.3: Verification Process Sequence

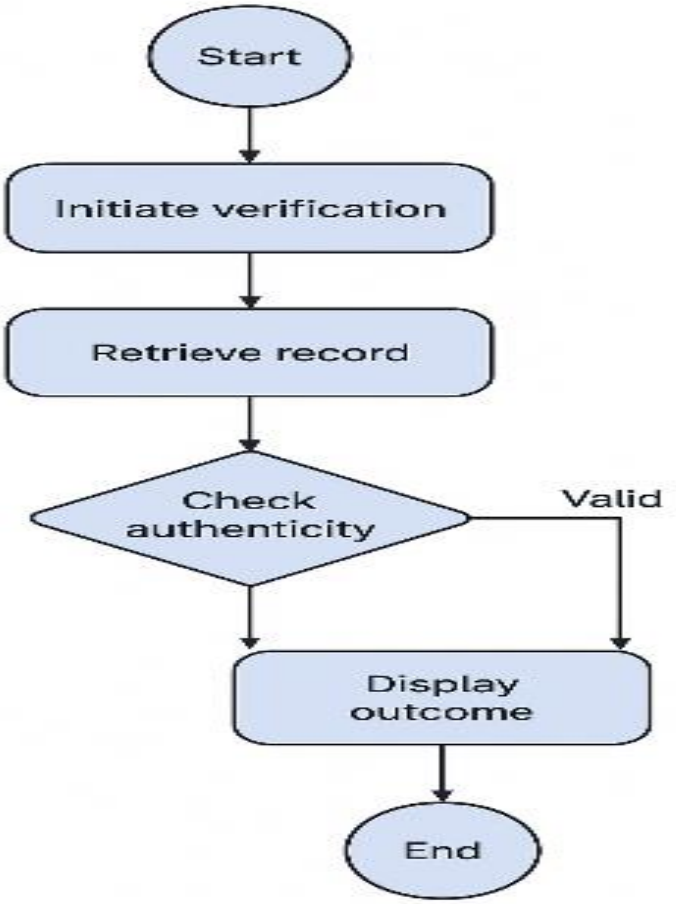

Figure 3.4: Verification Process Activity Diagram

3.5.2 Architecture Design

BUK Certify uses a **3-tier client-server architecture**. As shown in Figure 3.4, users (clients) interact via web browsers or mobile devices. Their requests reach the application server (hosting the BUK Certify web application), which handles business logic (authentication, QR code processing, verification logic). The application server communicates with the back-end PostgreSQL database server that stores all certificate and user records. This separation of concerns enhances scalability, security, and manageability. By centralizing data on the server and limiting client responsibilities to the presentation layer, the system can efficiently manage resources[11].

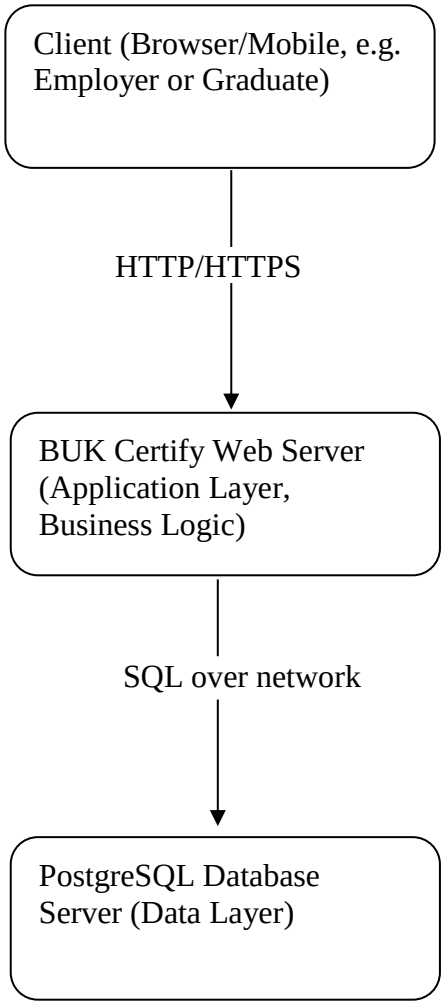

Figure 3.4: Client–Server Architecture

In this model, each component has a clear role: the **client** handles the user interface, the **server application** enforces rules and processes requests, and the **database** safely stores certificate data. This client-server model is common in web applications and *"allows for efficient data management and resource allocation by centralizing critical functions on the server,"* which improves performance and security[11].

3.5.3 Database Design

The database schema is modeled for PostgreSQL. The key entities and relationships are shown below. The main tables are **Student**, **Certificate**, **Verifier**, and **VerificationLog**:

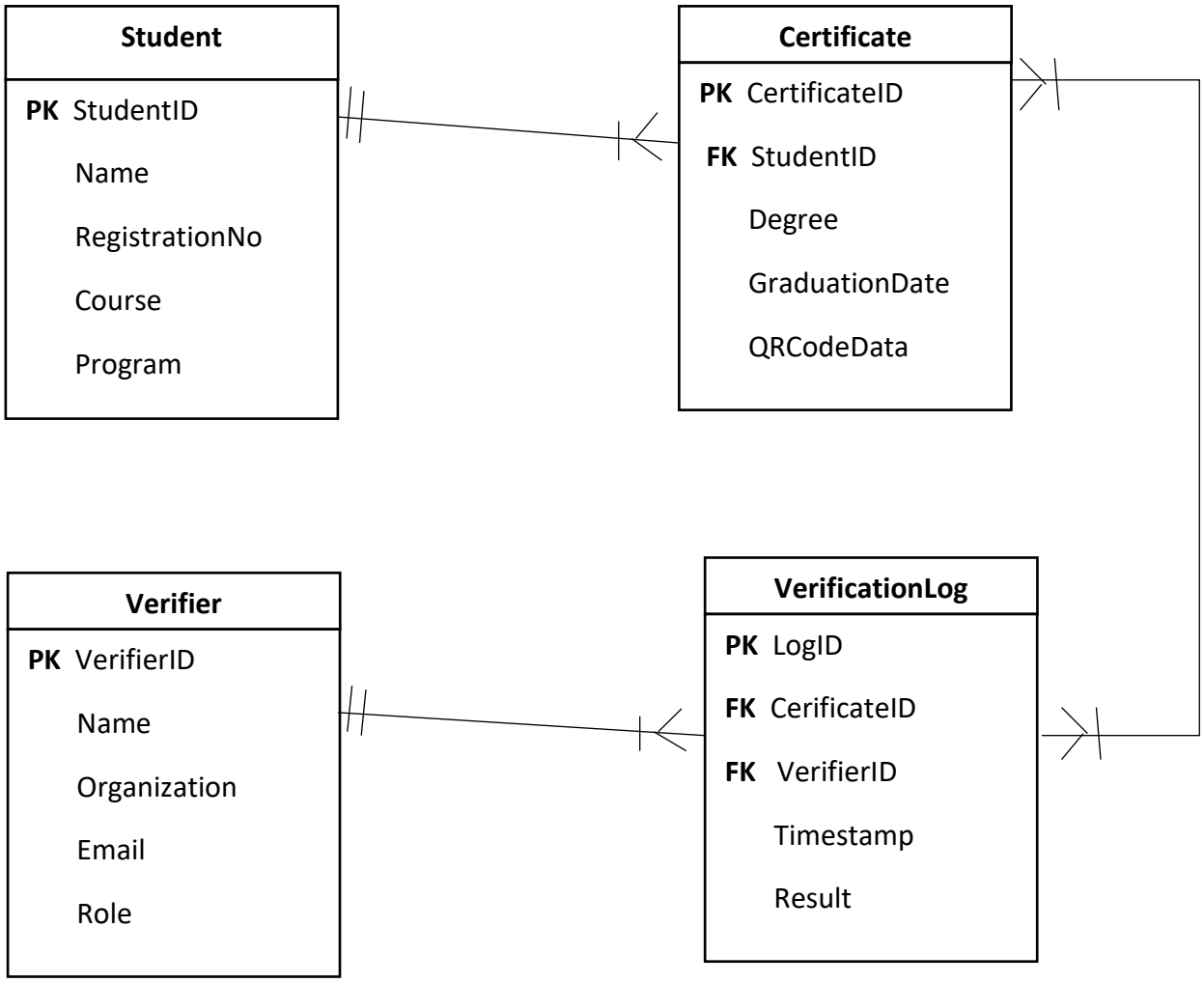

Figure 3.5: Entity-Relationship Diagram

Each Student can have one or more Certificate rcords (one-to-many on StudentID). Certificate stores details (degree, year) and the encrypted QR code data. Verifier represents authorized external users who perform checks. VerificationLog records each verification event, linking a Verifier to a Certificate and noting the time and outcome. Foreign keys enforce referential integrity (e.g. Certificate.StudentID references Student.StudentID). This design ensures that certificate data is normalized and that verifications can be tracked.

Overall, the architecture and design provide a clear blueprint for building the BUK Certify system: a web-based portal (client) connecting to a secure application server, which in turn manages a PostgreSQL database with the above schema. All sensitive operations (e.g. adding certificates, verifying data) are handled on the server side to ensure data integrity and security.

3.6 Summary

This chapter detailed the methodology for BUK Certify. We described the project workflow through iterative SDLC phases (planning, design, implementation, testing, deployment) and justified the Agile model's use for its flexibility and rapid delivery[6][3]. The existing manual verification process was analyzed and found to be slow and error-prone[8]. Stakeholder requirements were elicited via interviews with registry staff, employers, and graduates, leading to a clear set of functional (e.g. certificate management, QR generation, verification interface) and non-functional (security, performance, availability) requirements. We presented a use-case diagram and detailed the *"Verify Certificate"* use case. Finally, the system design was outlined: a sequence flow for verification, a client–server architecture diagram, and a database ER diagram for PostgreSQL. Together, these models form a comprehensive design foundation. The next chapter will describe the implementation details and testing of the BUK Certify system, building on this methodology.