Digital Signature Based Document Verification System

R. Sai Kartik – 22CSB0A05

K. Manideep – 22CSB0A09

Y. Eeswar – 22CSB0A31

Table of Contents

[1 Introduction 1](#_Toc193973869)

[1.1 Problem addressed in the Assignment 1](#_Toc193973870)

[1.2 Why the problem is important 2](#_Toc193973871)

[1.3 How the existing solutions solved this problem 2](#_Toc193973872)

[1.4 Key contributions of our project 2](#_Toc193973873)

[2 Objectives 3](#_Toc193973874)

[3 Implementation and Results analysis 3](#_Toc193973875)

[3.1 Conceptual diagram 3](#_Toc193973876)

[3.2 Flowcharts 4](#_Toc193973877)

[3.3 Algorithms 7](#_Toc193973878)

[4 Conclusion 8](#_Toc193973879)

[5 Learning outcomes 8](#_Toc193973880)

[6 Source code 9](#_Toc193973881)

[7 References 9](#_Toc193973882)

# Introduction

## Problem addressed in the Assignment

The primary problem this project addresses is the critical challenge of verifying the authenticity and integrity of academic grade sheets in professional credential verification processes. In today's competitive job market, students frequently submit academic documents to potential employers, creating a significant vulnerability where document fraud and tampering can compromise the recruitment ecosystem. Traditional verification methods rely on manual checks, which are inherently time-consuming, resource-intensive, and susceptible to human error and deliberate manipulation.

By implementing a sophisticated digital signature and cryptographic verification system, the project provides a robust technological solution that ensures grade sheets remain unaltered from their point of origin through their entire lifecycle. The system establishes a secure, transparent mechanism that allows educational institutions, students, and prospective employers to validate academic credentials with unprecedented reliability, efficiency, and trust.

The innovative approach transforms document verification from a vulnerable, manual process into a seamless, cryptographically secured workflow that protects the integrity of academic records and streamlines professional credential validation.

## Why the problem is important

* **Preventing Fraud**: Fake or altered grade sheets are a common issue in academic and employment verification.
* **Ensuring Authenticity**: Ensures companies make hiring decisions based on authentic credentials
* **Efficient Verification**: Automating the process reduces human effort and ensures faster results.
* **Data Integrity**: Using cryptographic techniques guarantees that documents remain unaltered.
* **Trust**: Creates a trusted ecosystem between educational institutions and employers

## How the existing solutions solved this problem

* **Manual Verification**: Involves physical submission and review of documents, which is time-consuming and susceptible to errors.
* **Third-Party Verification Services**: Centralized credential verification providers, Expensive and often involve delays. May still require manual steps
* **Basic Digital Records**: Simple digital copies without cryptographic verification, Easy to forge or alter
* **National Academic depository**: verification of academic documents is done digitally through DigiLocker, ensuring authenticity and preventing forgery

## Key contributions of our project

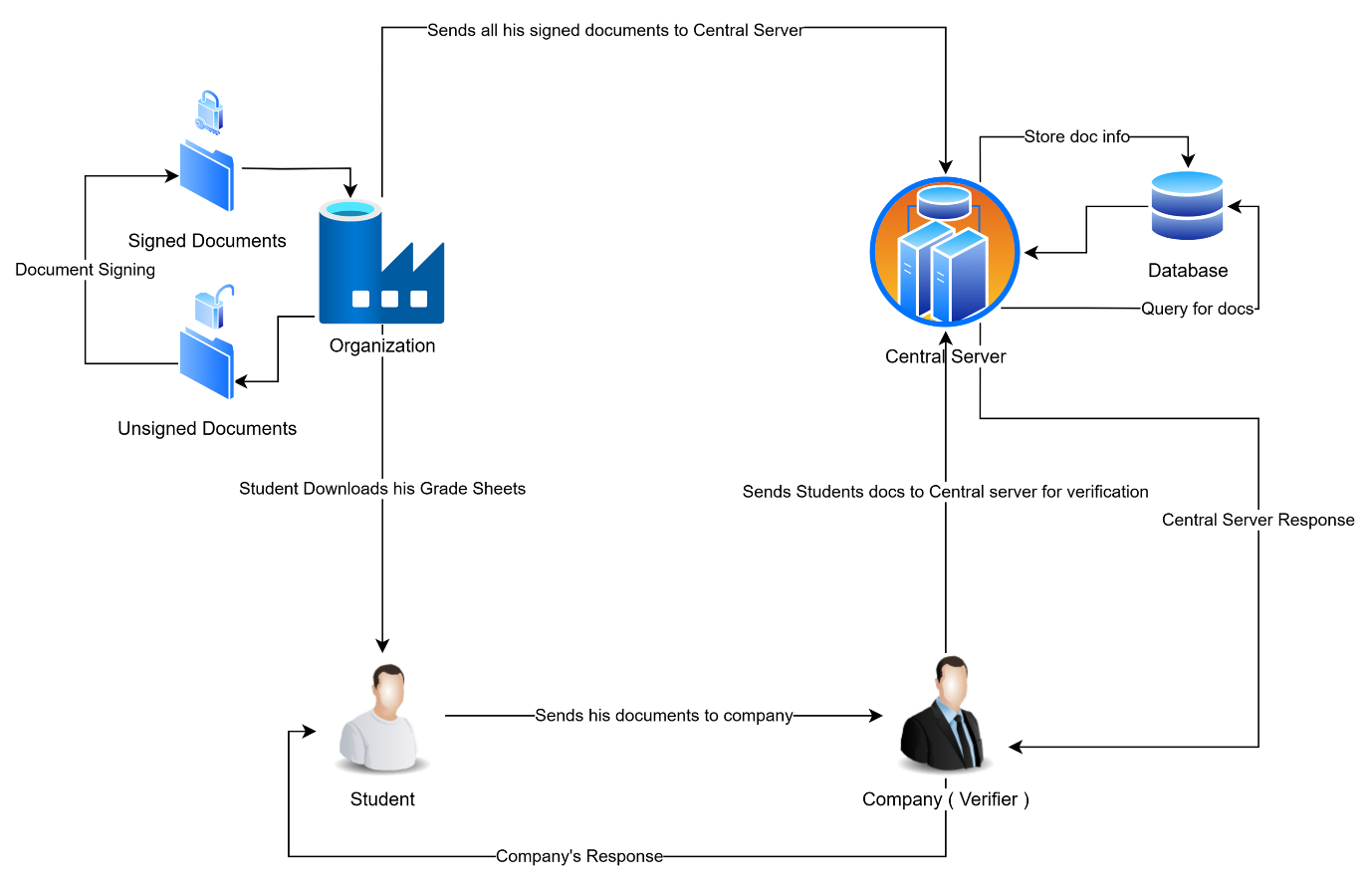
* **Efficient Data Management**: Storing Hash or Digital Signature of the document along with its Unique ID, associated Organization in the database instead of storing entire document
* **Tamper Detection:** Designed a tamper-proof system by comparing the submitted document’s hash with the stored hash retrieved from database, ensuring the detection of any unauthorized modifications.
* **Reduced Dependency on Physical Certificates:** Eliminates the need for manual verification, reducing paperwork and increasing trust in digital documents.
* **Decentralized Trust with Centralized Validation:** Organizations independently sign documents, while the central server acts as a trusted verifier without storing actual documents.

# Objectives

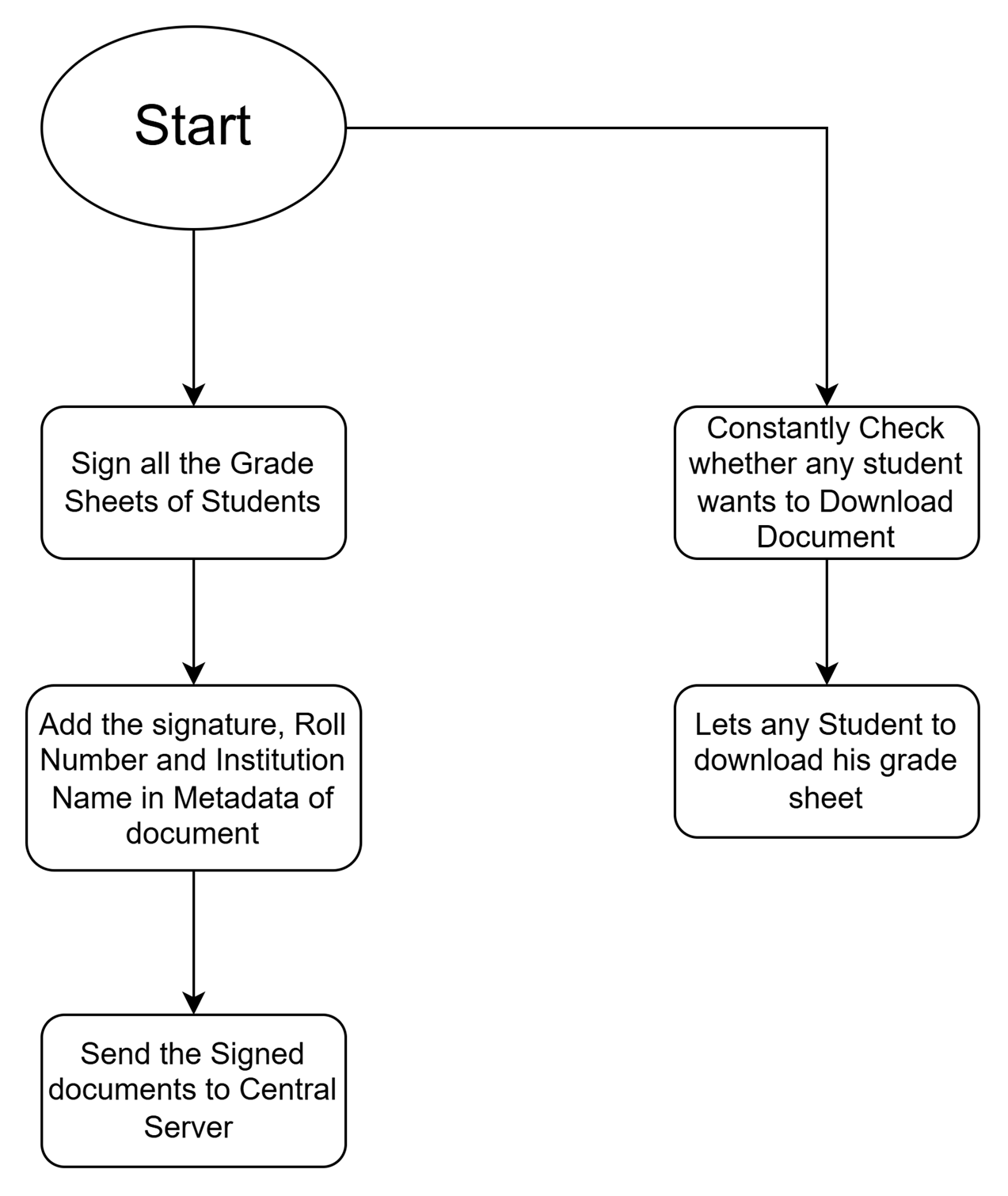
* **Ensure Document Integrity and Authenticity**: Provide a secure and reliable system using digital signatures to verify that academic grade sheets have not been tampered with.
* **Facilitate Efficient Verification**: Enable organizations, companies, and the central server to perform quick and automated verification of student grade sheets using a centralized database and cryptographic techniques.

# Implementation and Results analysis

## Conceptual diagram

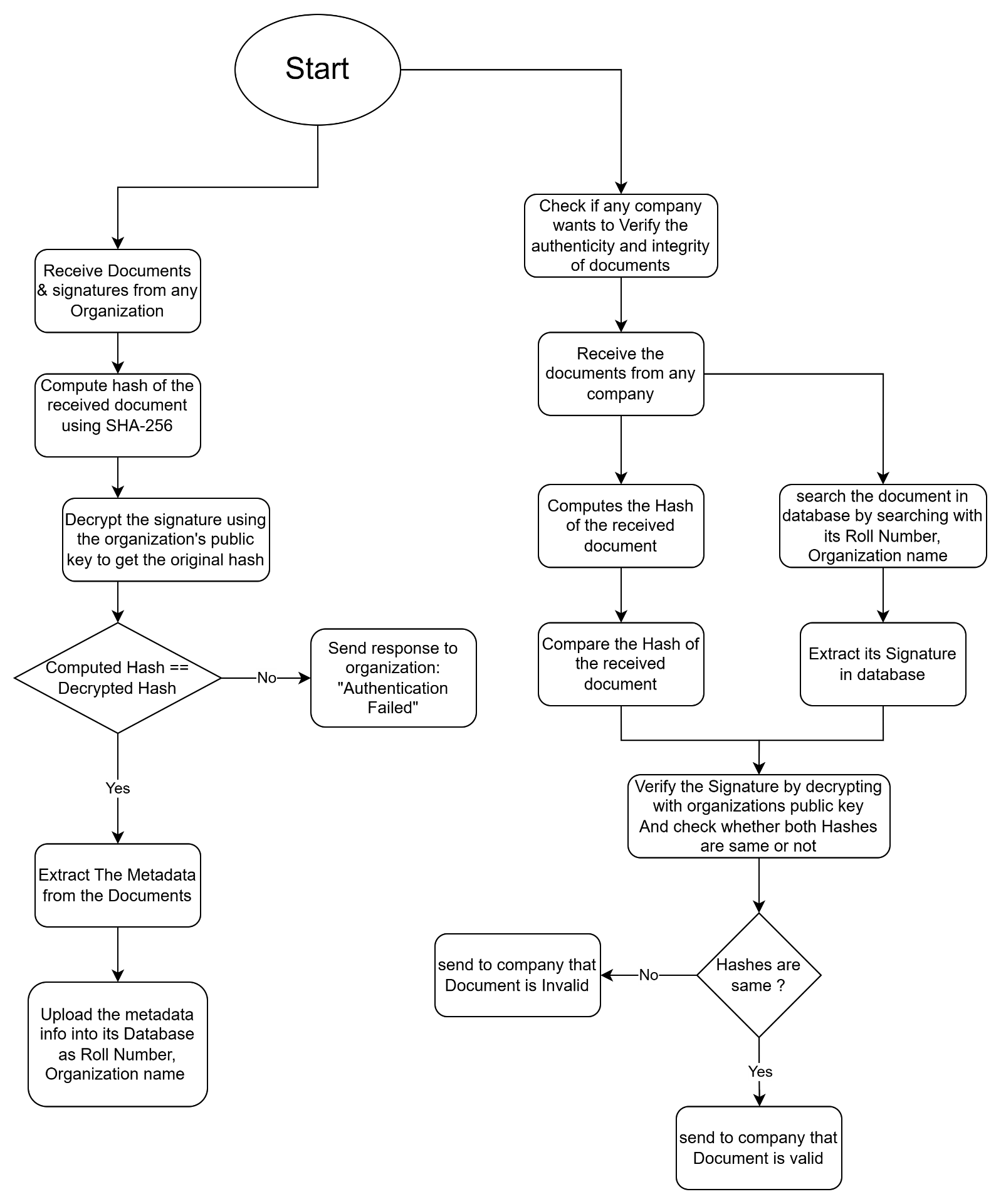


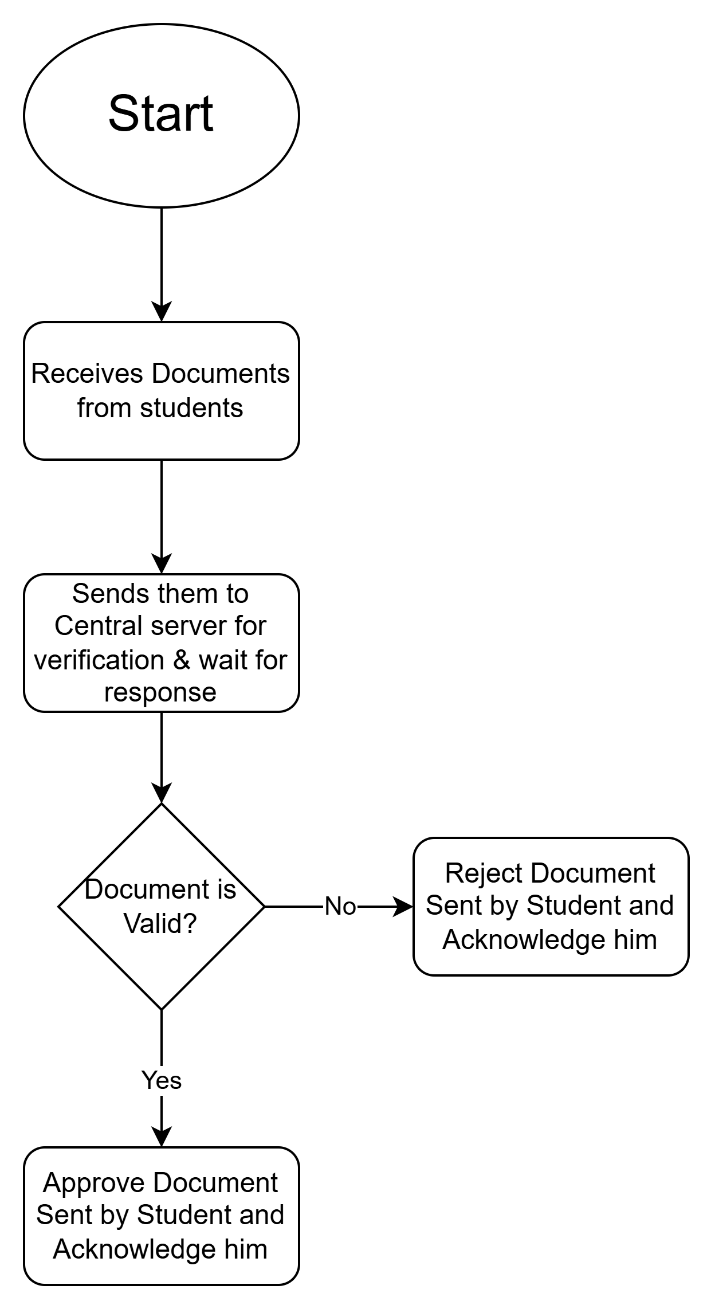
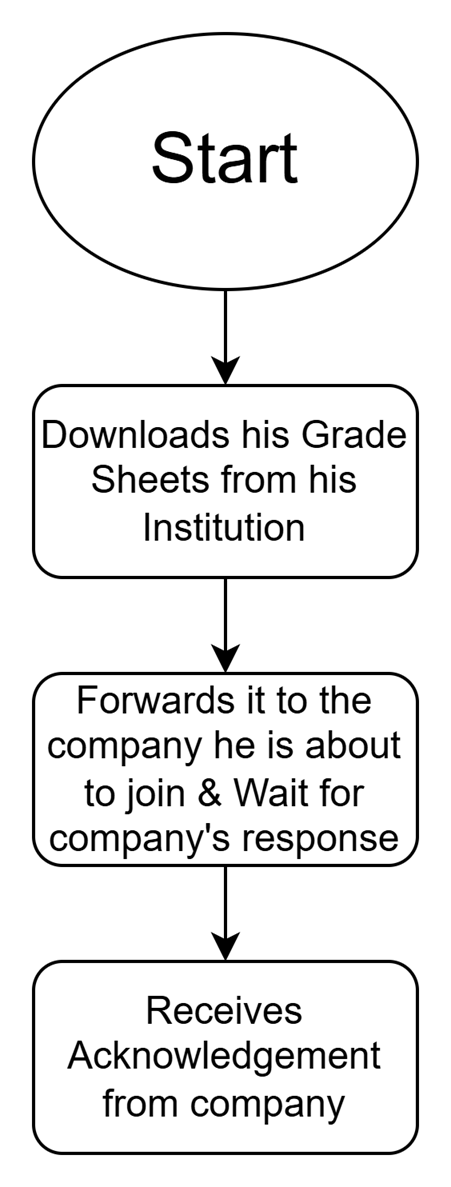
## Flowcharts



**Organization Flowchart**

**Central Server Flowchart**



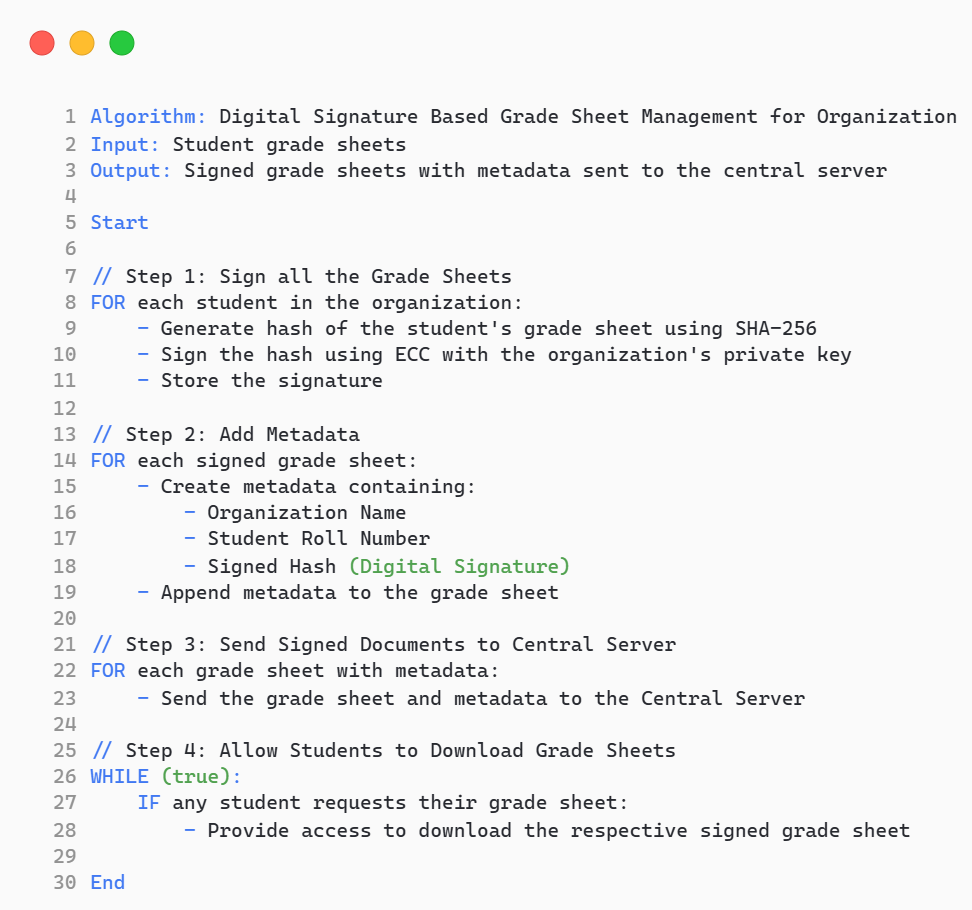
 

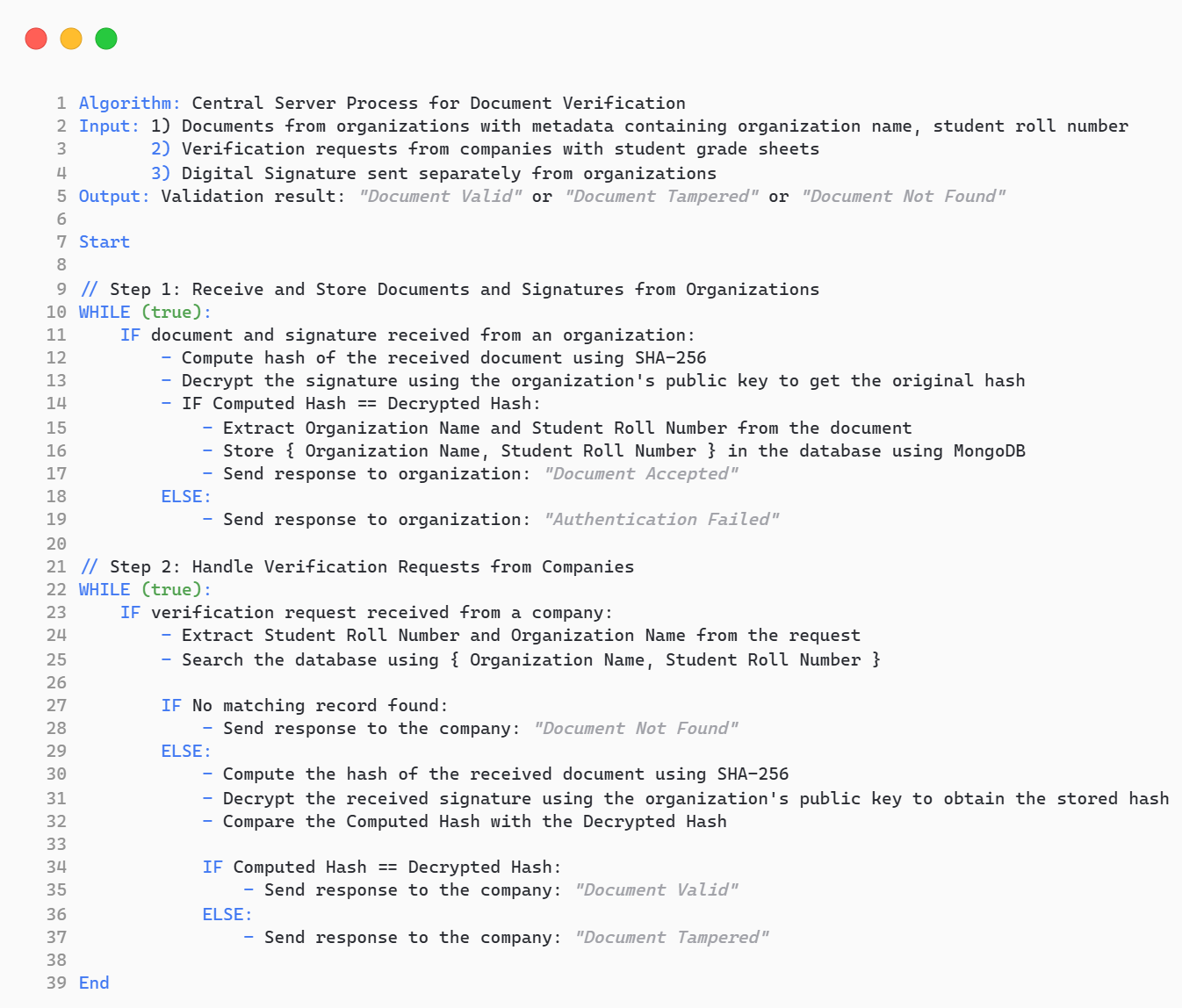
**Company Flowchart**

**Student Flowchart**

## Algorithms

**Organization**





**Central Server**

# Conclusion

This project successfully implements a Digital Signature-Based Document Verification System to ensure the authenticity and integrity of academic grade sheets. By leveraging public-key cryptography, organizations digitally sign student documents, allowing the central server to verify them using stored hashes. Companies can efficiently validate documents by comparing hashes, preventing tampering and forgery. The system enhances security, trust, and automation in credential verification, eliminating manual checks and reducing fraud risks. MongoDB ensures efficient storage and retrieval of records. Overall, this solution provides a scalable, secure, and reliable method for academic and corporate institutions to verify documents seamlessly.

# Learning outcomes

* **Understanding of Digital Signatures**: Gained practical experience in implementing Elliptic Curve Cryptography (ECC) for secure digital signatures and verifying document authenticity.
* **Cryptographic Application Development**: Developed a comprehensive system using C for secure communication and authentication between organizations, a central server, students, and companies.
* **Database Management**: Learned to integrate and manage a MongoDB database for storing and retrieving encrypted data efficiently.
* **Data Integrity Verification**: Applied cryptographic hashing techniques to ensure the integrity of documents during the verification process.
* **Client-Server Communication**: Gained insights into designing and implementing a secure client-server communication model for real-world applications.
* **Centralized Verification System**: Explored the design of a trusted central authority for document validation.
* **Problem Solving and System Design**: Developed critical problem-solving skills by addressing security challenges and ensuring data authenticity using public-key cryptography.
* **Real-World Implementation**: Applied cryptographic concepts to solve a practical problem in academic and corporate credential verification.
* **Project Development Skills**: Improved C programming, and teamwork while building the project.

# Source code

GitHub Link: <https://github.com/eeswar55555/Digital-Signature-Based-Document-Verification-System>

# References

* **MongoDB Documentation** — Official documentation for understanding database management and integration: <https://www.mongodb.com/docs/>
* **RFC 6090**: Fundamental ECC Algorithms — Provides detailed explanations on Elliptic Curve Cryptography: <https://datatracker.ietf.org/doc/html/rfc6090>
* **OpenSSL Documentation** — Useful for implementing ECC-based digital signatures using C: <https://www.openssl.org/docs/man3.0/man3/EVP_PKEY_sign.html>