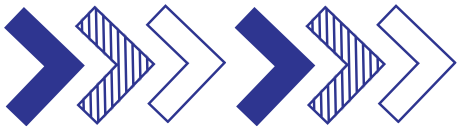
2024

09/12

S.A.F.E

SLIIT AUTHENTICATION FEATURED ENVIRONMENT

PROJECT PROPOSAL

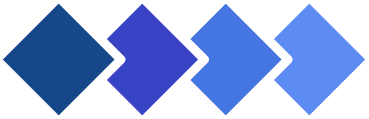


Presented for :

MS Club, SLIIT

Presented by :

Team CODE_Geass



The Introduction

In the evolving landscape of education, institutions face increasing demands for secure communication, effective document management, and streamlined support systems. These challenges can significantly impact the academic experience and operational efficiency of educational environments. To address these issues, our proposal outlines a solution designed to enhance security, improve communication, and optimize support systems within educational institutions.

Background and Context

Educational institutions are continuously seeking ways to safeguard sensitive information, ensure seamless communication, and manage academic resources effectively. Traditional methods often fall short in providing the necessary security and efficiency, leading to vulnerabilities such as phishing attacks, unauthorized access to documents, and inefficient support systems

Objective of the Proposal

The objective of this proposal is to present a comprehensive solution that addresses these key challenges. Our solution aims to:

- Enhance the security of email communications.
- Facilitate secure and efficient student-to-student interactions.
- Provide controlled and secure document management.
- Streamline the delivery of targeted notifications.
- Simplify the issue reporting and resolution process.
- Implement advanced security measures to protect user accounts.

Scope of the Project

This proposal focuses on developing a platform that integrates these features into a unified system. The project will cover the design, implementation, and evaluation phases, ensuring that the solution effectively meets the needs of educational institutions and delivers tangible improvements in security, communication, and support.

Overview

Our proposed solution addresses critical challenges faced by educational institutions by integrating advanced features to enhance security, streamline communication, and optimize document management and support systems.

Key Highlights:

- **Secure Communication**: Protects against phishing and email spoofing, ensuring that communication within the institution remains confidential and authentic.
- **Efficient Document Management**: Provides secure tools for uploading, sharing, and managing academic resources, safeguarding sensitive materials from unauthorized access.
- **Centralized Notifications**: Facilitates the effective distribution of important information, ensuring that notifications reach the intended recipients without being overlooked.
- **Streamlined Support**: Introduces an integrated ticketing system to simplify issue reporting and resolution, improving support efficiency and responsiveness.
- **Enhanced Security**: Implements biometric and PIN-based authentication to protect user accounts and sensitive information, addressing weaknesses associated with traditional password protection.

This overview provides a snapshot of the solution's core components and benefits, setting the stage for a more detailed exploration of the problem, proposed solution, implementation plan, and commercialization strategy.

1.The Background

1.1 Problem

1.1.1 Authenticate Email and Secure Communication

i. **Phishing Attacks**: Students might receive phishing emails that tricks them into revealing their credentials, leading to unauthorized access to their account and personal data.
ii. **Email Spoofing**: Attackers must impersonate university officials or students, sending misleading emails that appear legitimate.

1.1.2 Secure Student-To-Student Communication

i. **Unsecure Communication Channels**: Students may use unsecure or third party platforms to communicate, which could be susceptible to interception or unauthorized access.
ii. **Difficulty in Reaching Peers/Seniors**: In larger institutions (such as SLIIT) students might struggle to find and communicate with the right peers, specially for important academic matter.

1.1.3 Controlled Document sharing

i. **Insufficient Educational Documents**: Most students struggle to find right Past Papers (Mid / Final), Model Papers, Lecture Documents, Assignment Examples & Reference Materials.
ii. **Unauthorized Access to Sensitive Academic Materials**: Documents shared through unsecured channels might be accessed by unauthorized individuals, risking plagiarism or intellectual property theft.

1.1.4 Centralized and Targeted Notifications

i. **Missed or Ignored Important Notifications**: Critical notices from the Management, Faculty or Student Services might get lost in email clutter or go unnoticed by students, leading to missed deadlines or uninformed decisions.
ii. **Difficult in reaching specific groups**: Management may struggle to communicate effectively with specific student groups related to specific faculties/ years/ semesters leading to inefficiencies.

1.1.5 Streamlined Ticketing System

i. **Inefficient issue resolution**: Student may face delays or difficulties in reporting and resolving issues through existing systems, leading to frustration & unresolved problems.
ii. **Having complex steps to raise a ticket**: Without simplified ticketing system students may ignore to raise a ticket when needed which may lead to unreported or unresolved issues, affecting student experience & academic performance.

1.1.6 Enhanced Security with Bio Metric Lock & Pin

i. **Unauthorized Access to Accounts**: If a student's credentials are compromised, their entire account & sensitive information could be at risk.
ii. **Weak Password Protection**: Students might use weak or reused passwords, making their accounts vulnerable to attack.

1.2 Our Solution

1.2.1 Regarding: Authenticate Email and Secure Communication

i. **Authentication & create a Direct E-mail Delivery**: By authenticating emails and delivering them directly to the app, it ensures that only genuine emails reach the students. This prevent phishing emails and other malicious content from compromising student's accounts.
ii. **Confidentiality, Integrity & Authenticity**: The app protect the Integrity of communication by ensuring that emails can't be tempered with & only authorized users can access the content, thus maintain Confidentiality.

1.2.2 Regarding: Secure Student-To-Student Communication

i. **Secure Messaging**: By providing secure platform for student-to-student communication, the app ensures that important academic discussions remains private and safe from external threats.
ii. **Facilitated Academic Collaborations**: The feature, streamlines communication, making it easier for students to collaborate on projects, study groups & other academic activities.

1.2.3 Regarding: Controlled Document sharing

i. **Secure Document Upload & Management**: This feature allows students & lecturers to securely upload and share documents, with control over who can view or download them. This prevents unauthorized access and ensures that academic materials are shared securely and effectively.

1.2.4 Regarding: Centralized and Targeted Notifications

i. **Targeted Notifications**: This allows management to post notices targeted to specific groups, ensuring that the right students receive relevant information. Notifications are centralized & cannot be easily overlooked.
ii. **Accountability and Traceability**: By requiring management to specify their position and target audience, the app increases accountability and ensures that communications are traceable and legitimate.

1.2.5 Regarding: Streamline Ticketing System

i. **Integrated Ticketing System**: By incorporating a ticketing system within the app, students can easily report issues directly to the relevant departments. This streamlines the resolution process and ensures that issues are addressed promptly.
ii. **Improved Student Support**: The app provides a dedicated and secure channel for students to raise concerns, leading to faster and more efficient support from the administration.

1.2.6 Regarding: Enhanced Security with Biometric Lock and PIN

i. **Biometric and PIN Security**: By using biometric locks and PINs, adds an extra layer of security, ensuring that not even app itself can't be access without the authorized user.
ii. **User-Friendly Security**: By making strong security measures easy to use, the app encourages students to adopt safer practices without inconvenience.

1.3 Technical Aspect of the Solution

1.3.1 Authenticate Email and Secure Communication

Step 01:

- Login to the S.A.F.E. Web Application.
- Then head over to Security option.
- Choose Authenticator App. Get the QR code.

Step 02:

- In the Mobile App Login to S.A.F.E. App using your campus credentials.
- Choose Authenticator bottom right conner.
- Choose Scan QR option.

Step 03:

- After scanning the QR code, you will get a string with 6 characters.
- Type that code in the Web Application.
- The process will complete after the Web Application verify your code.

1.3.2 Secure Student-To-Student Communication

- Login to the S.A.F.E. Mobile App.
- Choose the Message option bottom right conner.
- Find the contact vie Registration Number.
- Continue to communicate.

1.3.3 Controlled Document sharing

- Login to the S.A.F.E. Mobile App.
- Choose the Upload option bottom right conner.
- Find the contact vie Registration Number.
- Continue to communicate.

1.3.4 Centralized and Targeted Notifications

- Login to the S.A.F.E. Mobile App.
- The filtered notifications can be seen in the interface of the app after the user login.

1.3.5 Streamline Ticketing

- System Login to the S.A.F.E. Mobile App.
- Choose the “Raise a Ticket” option.
- Fill the form and Submit

1.3.6 Enhanced Security with Biometric Lock and PIN

- Login to the S.A.F.E. Mobile App.
- Go to Settings option Choose “Add Fingerprint” or “Add PIN”

1.4 Frameworks, APIs and Platforms

1.4.1 Authentication and Secure Communication

- Frameworks
  - Flutter: Use Flutter to create a cross-platform mobile app.
- APIs:
  - OAuth 2.0: Implement OAuth 2.0 for email authentication.
  - SMTP/IMAP APIs: Interact with email servers for direct delivery and retrieval.
  - OpenSSL or Cryptography Libraries: Ensure encryption and integrity checks.

1.4.2 Secure Student-To-Student Communication

- Frameworks:
  - Flutter: Implement secure messaging features.
- APIs:
  - End-to-End Encryption Libraries (e.g., Signal Protocol): Ensure privacy.
  - WebSocket APIs: Enable real-time communication.

1.4.3 Controlled Document Sharing

- Frameworks:
  - Flutter: Create a document upload and management feature.
- APIs:
  - Amazon S3 or Google Cloud Storage APIs: Securely store and manage documents.
  - Access Control Lists (ACLs): Control document permissions.

1.4.4 Centralized and Targeted Notifications

- Frameworks:
  - Flutter: Implement push notifications.
- APIs:
  - Firebase Cloud Messaging (FCM): Send targeted notifications.
  - Role-Based Access Control (RBAC): Specify user groups.

1.4.5 Streamlined Ticketing System:

- Frameworks:
  - Flutter: Create a ticketing system within the app.
- APIs:
  - RESTful APIs: Handle ticket creation and management.
  - Database (e.g., SQLite): Store ticket data.

1.4.6 Enhanced Security with Biometric Lock and PIN:

- Frameworks:
  - Flutter: Implement biometric and PIN security.
- APIs:
  - Biometric Authentication APIs (e.g., Android Fingerprint API, iOS Touch ID): Enhance security.

Platforms: iOS and Android

1.5 Implementation plan

1.5.1 Project Planning and Requirements Gathering:

- Define the scope and objectives of your educational app.
- Identify stakeholders (students, instructors, administrators) and gather their requirements.
- Outline the features and functionalities needed for the app and AI grading system.

1.5.2 System Architecture Design

- Design the overall architecture:
  - Front-end: Use Flutter for cross-platform mobile app development.
  - Back-end: Choose Node.js or Django for data processing, user authentication, and API endpoints.
- AI components: Decide on using PyTorch or TensorFlow for AI model development.

1.5.3 Data Collection and Preparation:

- Collect relevant data (student submissions, rubrics, past grades) for training the AI model.
- Preprocess the data by cleaning, normalizing, and annotating as required.

1.5.4 Exploratory Data Analysis (EDA):

- Analyze collected data to understand its characteristics and patterns.
- Visualize data distributions, correlations, and insights to guide model development.

1.5.5 Feature Engineering:

- Create relevant features from raw data to enhance AI model learning.
- Optimize the feature set through selection and transformation.

1.5.6 Model Development:

- Select appropriate machine learning or deep learning algorithms for grading.
- Develop and train the AI model using the prepared dataset.
- Fine-tune hyperparameters and use cross-validation for optimal performance

1.5.7 Model Evaluation:

- Evaluate the trained model using validation and test datasets.
- Use metrics (e.g., accuracy, precision, recall) to assess performance.
- Ensure the model generalizes well and meets accuracy standards.

1.5.8 Integration with Mobile App:

- Develop the mobile app using Flutter:
    - Implement submission portals, feedback displays, and performance dashboards.
    - Integrate the AI model with the back-end to process submissions and return grades.

1.5.9 User Interface Design:

- Design an intuitive interface for students and instructors.
- Ensure usability and accessibility.

1.5.10 Testing:

- Perform unit testing, integration testing, and end-to-end testing.
- Conduct user acceptance testing (UAT) to gather feedback and make necessary adjustments.

1.5.11 Deployment:

- Deploy the mobile app and AI model to a production environment.
- Set up server infrastructure (e.g., AWS, Azure, or GCP) for scalability and reliability.
- Implement monitoring and logging.

1.5.12 Monitoring and Maintenance:

- Continuously monitor performance, address bugs, and enhance security.
- Collect user feedback for iterative improvements.
- Regularly update the AI model with new data.

1.5.13 Documentation and Reporting:

- Document the development process, system architecture, and usage guidelines.
- Generate reports and visualizations to communicate effectiveness to stakeholders.

2 User Scenario

Please Refer the “User Scenario” Guide

3 Conclusion

In summary, our solution offers a comprehensive approach to improving secure communication, document management, and support systems within educational institutions. With features like secure email authentication, controlled document sharing, targeted notifications, streamlined ticketing, and advanced biometric security, we aim to enhance operational efficiency and user experience.

Key Benefits:

- Enhanced Security: Safeguards against unauthorized access and data breaches.
- Improved Communication: Ensures secure and efficient interactions.
- Efficient Document Management: Protects and organizes academic resources.
- Centralized Notifications: Delivers important information effectively.
- Streamlined Support: Facilitates prompt issue resolution.

We are excited about the potential impact of this solution and look forward to the opportunity to discuss how it can meet your needs. Thank you for considering our proposal.

END