Semester Project Proposal

Information Security (CS-251L)

Project Title

ProtectX Gateway

Submitted to

Miss Wasifa Kanwal

Group Members

Syed Bilawal Shah [UW-24-CS-BS-068]

Syed Muhammad Taqi [UW-24-CS-BS-071]

Jawad Hussain [UW-24-CS-BS-108]

Session

BSCS – 3rd B [Fall-2025]

Date of Submission

16th December 2025

1. Abstract

This project aims to provide a secure way for agencies to send confidential documents over the internet. Normally, sensitive documents can be intercepted or leaked during communication. To solve this problem, the proposed system converts documents into encrypted text using strong encryption algorithms before sending them. Only the intended receiver will be able to decrypt and read the original file.

The project will also include a small honeypot and intrusion-monitoring component to detect suspicious access attempts. This provides an early warning system if a hacker tries to steal or access sensitive information. The expected benefit is improved confidentiality, data security, and basic intrusion detection for organizations that deal with critical information.

---

2. Background and Justification

Organizations and government agencies regularly share confidential documents with their partners. Traditional email or file-sharing methods are not secure enough because attackers can intercept data. Many existing systems focus either on encryption or intrusion detection, but not a combination of both in a simple tool. Our project will enhance existing work by providing a lightweight solution that performs secure document encryption along with a basic honeypot-based intrusion monitoring system through an easy-to-use Streamlit interface.

---

3. Project Methodology

The project will be developed in Python. Streamlit will be used to create a clean and simple user interface for uploading and downloading files. The document encryption module will be implemented using AES and RSA encryption libraries. The honeypot will be built using a lightweight Python socket program which logs suspicious access attempts. An intrusion monitoring module will read these logs and show warnings on the dashboard. Testing will be performed with sample PDF, DOCX, and TXT files, and simulated intrusion attempts.

---

4. Project Scope

The system will provide document upload, text extraction, AES/RSA encryption, encrypted file download, decryption on receiver side, honeypot activity logging, and a small intrusion-alert dashboard.

The system will *not* include advanced penetration detection, real-time network scanning, large-scale threat intelligence, or full-scale enterprise-level firewalls. It will also not perform cloud storage or multi-user authentication. The focus is only on secure document transformation and basic intrusion monitoring.

---

5. High-Level Project Plan

Activity	Time Allocated	Resources
Understanding problem & requirements	1 week	Internet, course material
Learning Streamlit & crypto libraries	1 week	Python, Streamlit docs
Developing encryption/decryption module	2 weeks	Python cryptography
Building honeypot & IDS scripts	2 weeks	Python sockets
Integrating system into Streamlit UI	1 week	Python, Streamlit
Testing & documentation	1 week	Sample files, logs

---

6. References

- Streamlit Documentation
- Python Cryptography Library Documentation
- Research articles on Honeypots and ID