RAJALAKSHMI
ENGINEERING COLLEGE
An AUTONOMOUS Institution
Affiliated to ANNA UNIVERSITY, Chennai

25 years OF ACADEMIC EXCELLENCE

Department of Artificial Intelligence and Data Science

Enabling a Secure Communication System in Legacy Application and Preventing Phishing and MIMT Attacks

Mrs.Thamizharasi
Professor

Guruprasath P
221801014
Harshini MD
221801017

Problem Statement and Motivation

□ Many existing systems lack robust encryption and integrity checks, making them vulnerable to unauthorized access, data manipulation, and breaches.

MOTIVATION:

□ Enhancing encryption and integrity measures is essential to protect sensitive data from evolving cyber threats and unauthorized access.

□ Strengthening data security will improve the reliability and trustworthiness of digital systems, ensuring users can operate with confidence.

Objectives

- To develop a comprehensive security framework to address vulnerabilities in digital communication systems. By enhancing encryption, improving data integrity checks, and preventing data manipulation, the framework aims to create a secure environment for data transmission and storage.

    - **Strengthen Encryption:** Implement robust encryption for secure data transmission and storage.**Ensure Data**
    - **Integrity:** Introduce mechanisms for verifying data accuracy and detecting unauthorized changes.**Prevent**
    - **Manipulation:** Develop methods to detect and prevent data tampering.

Abstract

The research focuses on developing a secure communication platform to address vulnerabilities in digital systems by implementing robust encryption, comprehensive data integrity checks, and manipulation prevention mechanisms. The platform will enable secure transmission and storage of sensitive information, ensuring data confidentiality and integrity. By integrating advanced security measures, the solution will provide a reliable and user-friendly environment for secure communications, protecting against unauthorized access and enhancing trust in digital interactions.

Introduction and Overview of the Project

In today’s digital age, safeguarding sensitive data is crucial due to the rise in cyber threats. This project aims to develop a secure communication platform that utilizes GnuPG (GPG) for encryption and digital signatures. Built with Flask, the application enables users to generate RSA key pairs, encrypt files for designated recipients, and verify signatures. Key functionalities include user-friendly interfaces for key generation, file encryption, and decryption with signature verification. By integrating robust encryption methods with an intuitive design, this platform enhances data confidentiality, integrity, and authenticity, fostering trust in secure digital communications.

Literature Survey

S.no	Author	Year	Techniques / Methods	Drawbacks
01	S. Khan, F. et. all	2022	Advancement in Vehicular Public key Infrastructures. (VPKI)	Implementation is relatively hard.
02	Mauro Barni. et. all	2023	Digital Watermarking Robust Hashing Steganography and Steganalysis Biometrics	Challenges in adapting to rapid technological advancements, such as deepfakes and synthetic mediaNeed for evolving legal frameworks to manage technological advancements and prevent misuseBalancing the benefits of new technologies with privacy concerns and potential misuse
03	Jingwei Jiang. et. all	2024	Quantum-Resistant Password-Authenticated Symmetric Searchable Encryption(QPASE) Lattice-Based Cryptography Threshold Oblivious Pseudorandom Function	Challenges in adapting traditional cryptographic schemes to post-quantum environments
04	Jingwei Jiang. et. All	2024	Quantum-Resistant Password-Protected Secret Sharing(PPSS) Lattice-Based CryptographyQuantum-Resistant Data Outsourcing	Challenges in ensuring robustness against various quantum computing attacks Potential performance trade-offs compared to non-quantum-resistant schemes

S.no	Author	Year	Techniques / Methods	Drawbacks
05	V.G. Karantaev. et. all	2023	Implementation of Cryptographic Measures in Digital SubstationsSecure Inter-Network Communication for IEC 61850-8-1 (MMS) Protocol	Challenges in effectively securing digital communication protocols used in highly automated substations
06	Vincenzo De Angelis. et. all	2022	Digital Health (eHealth) Innovation and ChallengesIntegration of 6G Wireless Networks in Healthcare	Existing network infrastructures may not fully support the digitalization of healthcare.
07	Cristian Bermudez Serna. et. all	2023	Post-Quantum Cryptography (PQC) for Shared Mutual Authentication (SMA)Implementation of Kyber Algorithm in SMA	Kyber-based SMA requires more random bytes and has a longer execution time compared to baseline mechanisms.
08	Mi Song, Ding Wang	2024	Two-Factor AuthenticationAttribute-Based Password Authenticated Key Exchange (AB-PAKE)Flexible and Fine-Grained AuthorizationPrivacy Preservation and Dynamic Access Control	Although the protocol is round-optimal and reduces pairing operations, its implementation and management of storage devices could be complex.

Existing System

- The existing systems focus on advancements in cryptographic techniques to address current and future security challenges. Technologies like Vehicular Public Key Infrastructure (VPKI), quantum-resistant cryptography, and biometric-based security are being developed to enhance digital security. These systems face challenges such as adapting to rapid technological changes, ensuring robustness against quantum computing, and managing infrastructure constraints. Quantum-resistant methods are emphasized to ensure future-proofing, while steganography and watermarking enhance privacy. In healthcare, intelligent networks and digital innovations must align with existing infrastructures for proper implementation.

Drawback of Existing System

- **Adaptation to Technology**

  Systems need frequent updates to stay secure with rapidly evolving technologies.

- **Complex Implementation**

  Advanced cryptographic techniques are difficult to implement and manage.

- **Performance Issues**

  High security measures often slow down real-time systems like IoT and vehicles.

- **Infrastructure Limits**

  Older infrastructure may struggle to support modern cryptographic systems, especially in healthcare.

Proposed System

- □ **Quantum-Resistant**

  Protects data from future quantum threats with advanced encryption.

- □ **Automated Key Generation**

  Simplifies encryption by automating the key creation process.

- □ **Seamless Integration**

  Works with existing infrastructures without major upgrades.

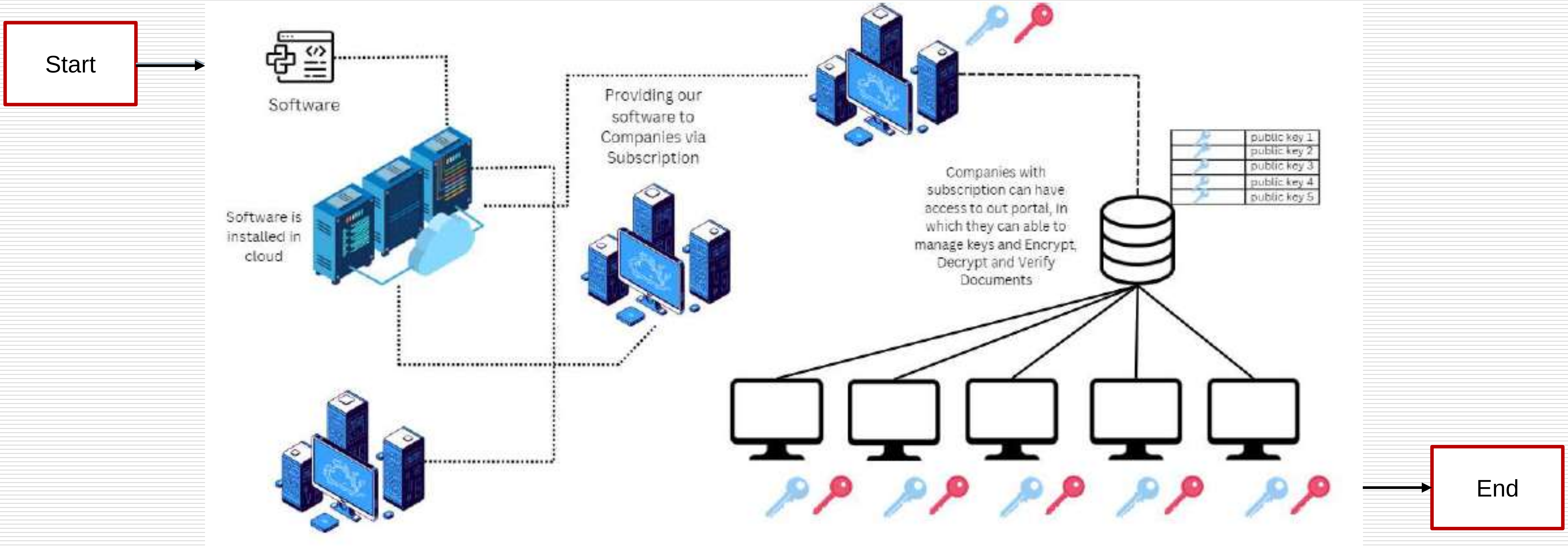
- □ **Scalable Design**

  Handles more data and users efficiently while maintaining security.

- □ **Optimized Performance**

  Ensures high security without slowing down real-time applications.

System Architecture



Start

End

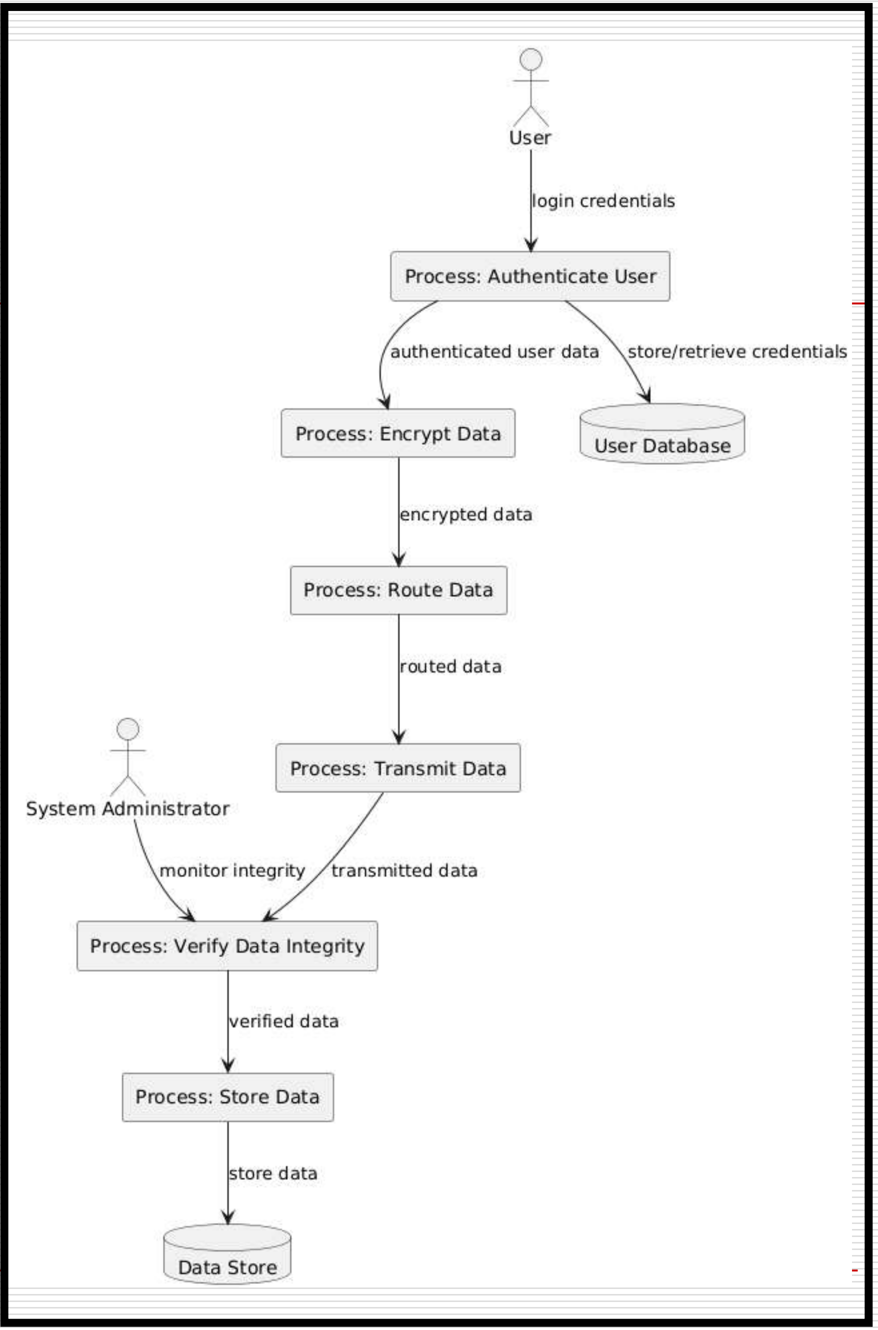
Software
Software is installed in cloud
Providing our software to Companies via Subscription
Companies with subscription can have access to out portal, in which they can able to manage keys and Encrypt, Decrypt and Verify Documents
public key 1
public key 2
public key 3
public key 4
public key 5

List of modules

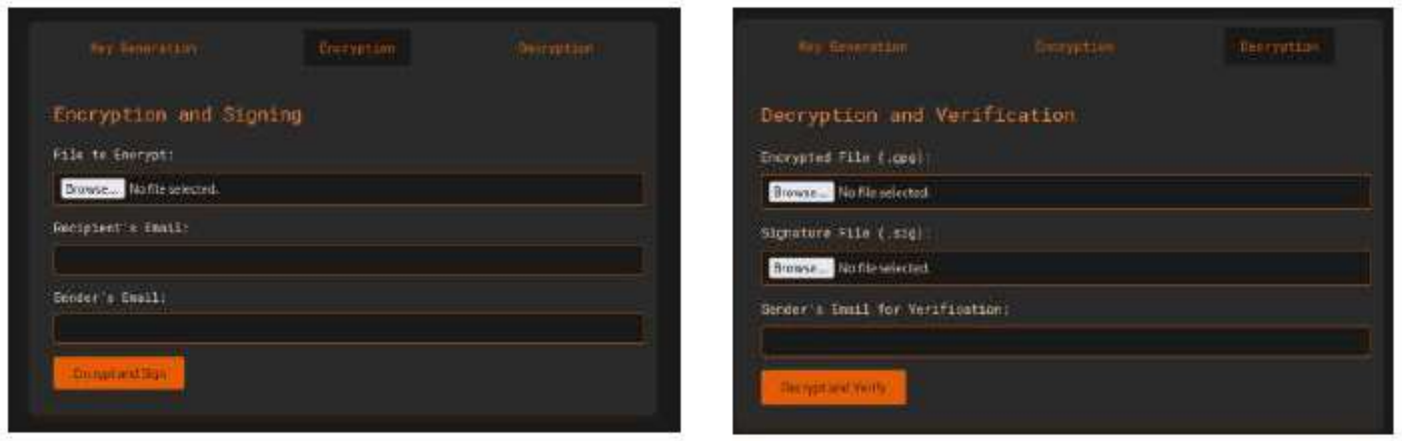
- Setting Up Key Generation
- Uploading File for Encryption
- Encrypting the File
- Signing the Encrypted File
- Uploading Encrypted File and Signature for Verification
- Verifying the Signature
- Decrypting the File
- Downloading the Decrypted File

DFD Diagram Level 1

- **User** interacts with the **Authenticate User** process by providing login credentials.
- **Authenticate User** process communicates with the **User Database** to store and retrieve credentials.
- **Authenticate User** sends authenticated data to the **Encrypt Data** process.
- **Encrypt Data** process encrypts the data and passes it to the **Route Data** process.
- **Route Data** process routes the data and sends it to the **Transmit Data** process.
- **Transmit Data** process sends the data to the **Verify Data Integrity** process.
- **Verify Data Integrity** process checks the data and sends it to the **Store Data** process.
- **Store Data** process stores the data in the **Data Store**.



Outputs



Encryption and Signing

File to Encrypt:

Browse... No file selected.

Recipient's Email:

Sender's Email:

Decryption and Verification

Encrypted File (.gpg):

Browse... No file selected.

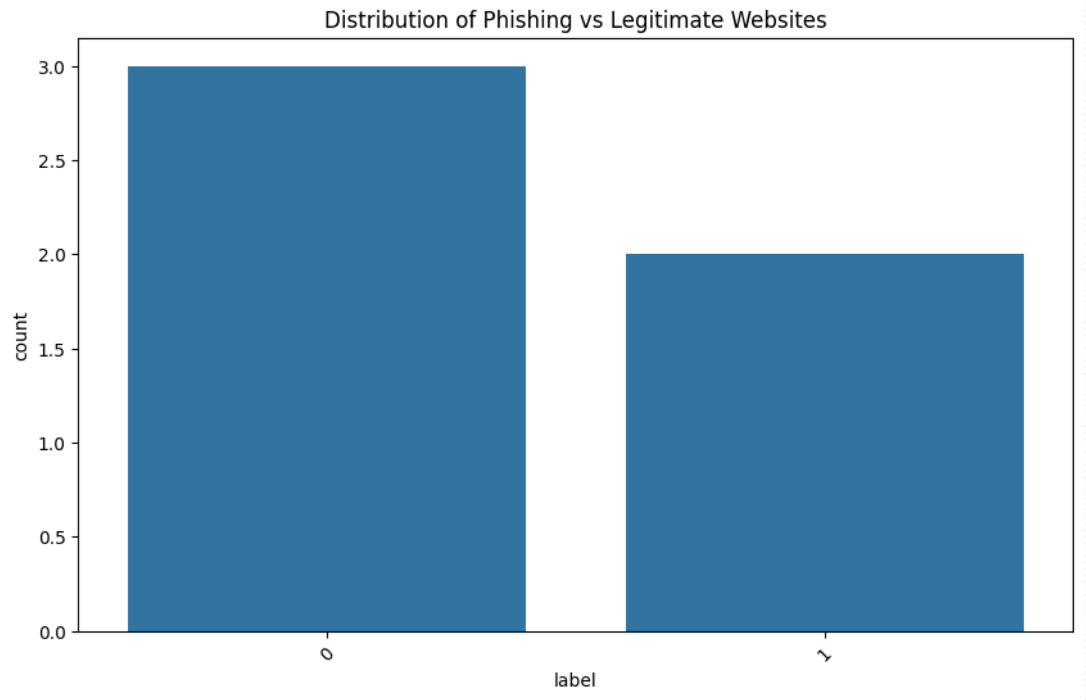
Signature File (.sig):

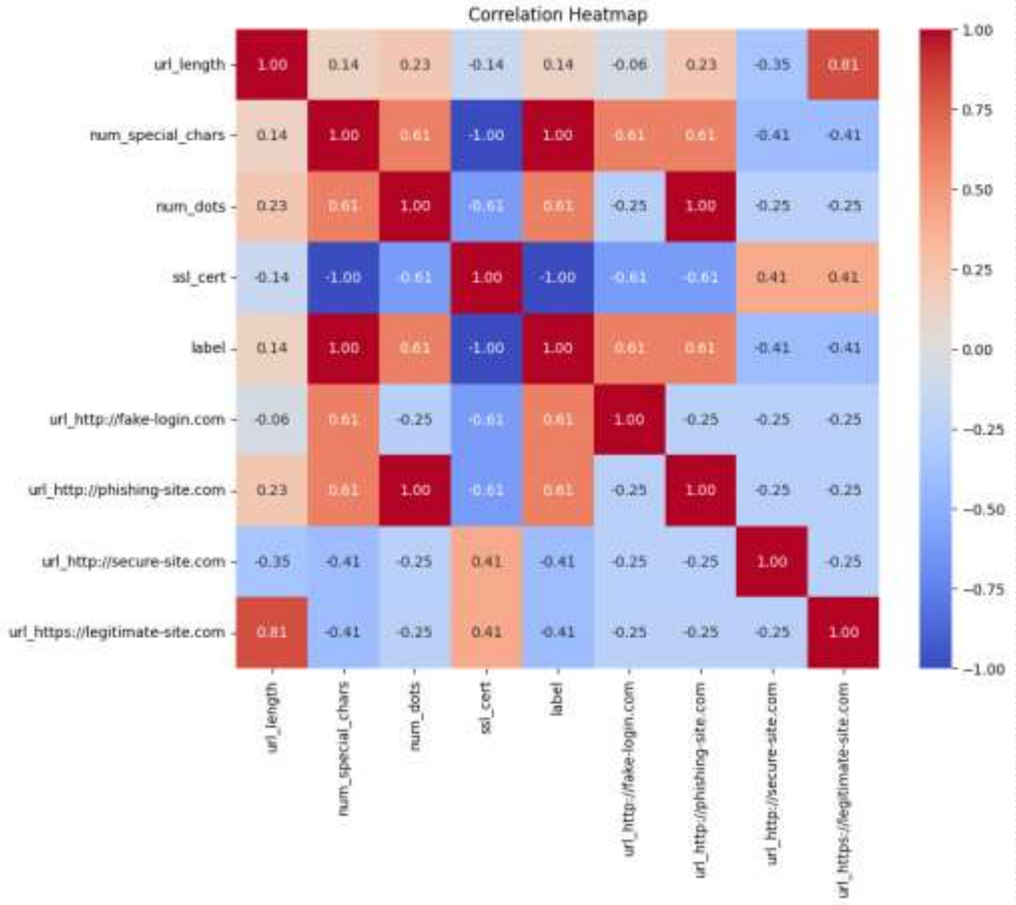
Browse... No file selected.

Sender's Email for Verification:

The project output is a secure communication platform that enables users to exchange files with high levels of confidentiality and integrity. It includes features for generating RSA key pairs, encrypting files with the recipient's public key, and creating digital signatures using the sender's private key to ensure authenticity. Recipients can verify signatures before decrypting files with their private keys, ensuring that only authorized parties can access sensitive information. Built on a user-friendly Flask web interface, the platform streamlines the process of secure file transfer while enhancing cybersecurity practices for users.

Analysis


Distribution of Phishing vs Legitimate Websites
count
3.0
2.5
2.0
1.5
1.0
0.5
0.0
0
1
label


Correlation Heatmap
url_length 1.00 0.14 0.23 -0.14 0.14 -0.06 0.23 -0.35 0.81
num_special_chars 0.14 1.00 0.61 -1.00 1.00 0.61 0.61 -0.41 -0.41
num_dots 0.23 0.61 1.00 -0.61 0.61 -0.25 1.00 -0.25 -0.25
ssl_cert -0.14 -1.00 -0.61 1.00 -1.00 -0.61 -0.61 0.41 0.41
label 0.14 1.00 0.61 -1.00 1.00 0.61 0.61 -0.41 -0.41
url_http://fake-login.com -0.06 0.61 -0.25 -0.61 0.61 1.00 -0.25 -0.25 -0.25
url_http://phishing-site.com 0.23 0.61 1.00 -0.61 0.61 -0.25 1.00 -0.25 -0.25
url_http://secure-site.com -0.35 -0.41 -0.25 0.41 -0.41 -0.25 -0.25 1.00 -0.25
url_https://legitimate-site.com 0.81 -0.41 -0.25 0.41 -0.41 -0.25 -0.25 -0.25 1.00
url_length
num_special_chars
num_dots
ssl_cert
label
url_http://fake-login.com
url_http://phishing-site.com
url_http://secure-site.com
url_https://legitimate-site.com
1.00
0.75
0.50
0.25
0.00
−0.25
−0.50
−0.75
−1.00

References.

[1] A. Shamir, "How to Share a Secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612-613, Nov. 1979. doi: 10.1145/359168.359176.

[2] P. Rogaway, "Formalizing Human Evaluation of Symmetric Encryption," *Proceedings of the 2017 IEEE European Symposium on Security and Privacy (EuroS&P)*, London, UK, 2017, pp. 199-214. doi: 10.1109/EuroSP.2017.36.

[3] W. Diffie and M. E. Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644-654, Nov. 1976. doi: 10.1109/TIT.1976.1055598.

[4] R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120-126, Feb. 1978. doi: 10.1145/359340.359349.

Thank You