System Requirements:

1. Network Security Requirements

- **Firewall Configuration**: Implement multi-layered firewalls with strict access control policies to block unauthorized traffic.
- **Intrusion Detection and Prevention Systems (IDPS)**: Deploy tools to monitor and mitigate suspicious activities and attacks (Ex. DDoS, brute force).
- **Network Segmentation**: Separate critical financial data from less sensitive network segments to limit access.
- **Secure Communication Protocols**: Enforce encryption (TLS 1.3) for all data in transit across networks.
- **VPN Access**: Use a corporate VPN for all remote connections, with multi-factor authentication (MFA).

2. Data Security Requirements

- **Encryption**:
  - **At Rest**: Use AES-256 encryption for sensitive data stored in databases, backups, and cloud storage.
  - **In Transit**: Secure all communication using HTTPS or similar protocols with certificates managed through a Public Key Infrastructure (PKI).
- **Data Loss Prevention (DLP)**: Implement tools to detect and prevent unauthorized data exfiltration.

3. Endpoint Security Requirements

- **Anti-Malware Protection**: Install and regularly update endpoint detection and response (EDR) solutions across all devices.
- **Device Control**: Restrict use of external USB drives and other peripherals to prevent malware injection.
- **Patch Management**: Regularly patch all software and operating systems to address known vulnerabilities.

4. Identity and Access Management (IAM)

- **Multi-Factor Authentication (MFA)**: Enforce MFA for all user accounts, particularly for administrative access.
- **Privileged Access Management (PAM)**: Use tools to monitor and control privileged accounts.
- **Single Sign-On (SSO)**: Implement SSO with centralized authentication systems for efficiency and security.

5. Application Security Requirements

- **Secure Software Development Lifecycle (SDLC)**: Integrate security into all stages of application development.
- **Vulnerability Scanning**: Perform regular automated scans of applications and APIs.
- **Web Application Firewall (WAF)**: Protect web applications from common threats (e.g., SQL injection, cross-site scripting).
- **Secure Coding Practices**: Enforce OWASP Top 10 principles and regular code reviews.

6. Cloud Security Requirements

- **Shared Responsibility Model**: Clearly define roles between the institution and cloud providers.
- **Data Encryption**: Apply client-side encryption for sensitive data stored in the cloud.
- **Audit Logs**: Enable logging and monitoring of all cloud activity with regular review.

7. Monitoring and Incident Response

- **Threat Intelligence Integration**: Use threat intelligence feeds to identify new vulnerabilities.
- **24/7 Security Operations Center (SOC)**: Maintain continuous monitoring for rapid incident detection and response.
- **Incident Response Plan (IRP)**:
  - Clearly define steps to handle incidents.

    - Include regular simulation exercises to test the IRP.

8. Training and Awareness

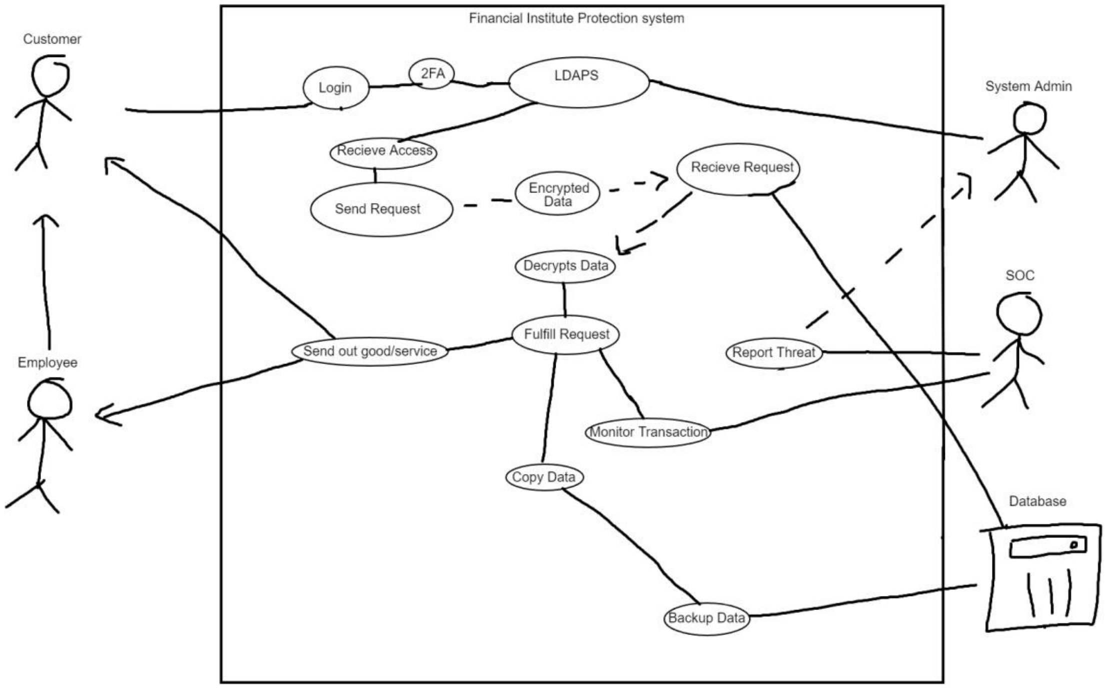
- **Employee Awareness Programs**: Conduct regular training sessions to educate employees about phishing and other cyber threats.
- **Simulated Attacks**: Test employee readiness with phishing simulations.
- **Access Reviews**: Periodically review user access to ensure appropriateness and revoke unnecessary permissions.

9. Backup and Disaster Recovery

- **Data Backup**: Use automated, encrypted backups stored in geographically separate locations.
- **Disaster Recovery Plan (DRP)**:
    - Define recovery time objectives (RTOs) and recovery point objectives (RPOs).
    - Conduct regular disaster recovery drills.

10. Physical Security

- **Data Centers**: Implement biometric access controls and 24/7 surveillance for all data centers.
- **Device Security**: Physically secure all workstations, laptops, and servers with locks and secure configurations.



Timeline:

- Completed all parts so far, finish final before December 9th