“AUTHENTICATION AND ENCRYPTION SYSTEM FOR ONLINE BANKING SYSTEM”

A PROJECT REPORT

Submitted to

SAVEETHA INSTITUTE OF MEDICAL AND TECHNICAL SCIENCES

Inpartial fulfilment of the award of the degree of

BACHLOR OF ENGINEERING IN

CO0MPUTER SCIENCE AND ENGINEERING

BY

V. THIRUPATHIRAO

192211896

SK. JANIBASHA

192211136

Supervisor

Dr. G. Jayandhi

CSA5148-CRYPTOGRAPHY AND NETWORK SECRUITY FOR IDENTITY VERFICATIONN

SAVEETHA SCHOOL OF ENGINEERING

SAVEETHA INSTITUTE OF MEDICAL AND TECHNICAL SCIENCES

CHENNAI - 602105

JUNE 202

Subject code/Name: CSA5148/Cryptography and Network Security for Identity Verification

Aim

The primary aim of this paper is to design and implement a secure authentication and encryption system for online banking platforms to protect user data and financial transactions from unauthorized access and cyber threats. The specific objectives include:

Abstract

With the rapid growth of online banking systems, ensuring the security and integrity of user data has become paramount. This paper presents an authentication and encryption system designed to protect online banking systems from unauthorized access and data breaches. The proposed system combines multi-factor authentication (MFA) and advanced encryption techniques to secure user transactions and sensitive information.

The authentication process employs a combination of passwords, biometrics (such as fingerprint or facial recognition), and one-time passwords (OTPs) to verify the identity of users. This multi-layered approach significantly reduces the risk of unauthorized access, as it requires multiple forms of verification that are difficult to replicate or steal.

On the encryption front, the system utilizes robust algorithms such as Advanced Encryption Standard (AES) and RSA to encrypt data both in transit and at rest. These algorithms ensure that even if data is intercepted, it remains unintelligible to unauthorized parties. Furthermore, the system incorporates Public Key Infrastructure (PKI) for secure key management and distribution, enhancing the overall security framework.

Additionally, the proposed system includes regular security audits and updates to address emerging threats and vulnerabilities. By integrating these advanced security measures, the system aims to provide a secure and reliable online banking experience, protecting users' financial information and fostering trust in digital banking services.

The implementation of this system demonstrates a significant improvement in the security of online banking platforms, highlighting the importance of combining authentication and encryption mechanisms to safeguard sensitive data. Future work will focus on enhancing the system's resilience against sophisticated cyber-attacks and exploring new technologies to further strengthen online banking security.

PROBLEM STATEMENTS:

Online banking, also known as internet banking, is an electronic payment system that enables customers of a bank or other financial institution to conduct a range of financial transactions through the financial institution's website. Online banking facilities typically have many features and capabilities in common, but also have some that are application specific. The common features fall broadly into several categories: - A bank customer can perform non-transactional tasks through online banking, including: (i) Viewing account balances (ii)

Viewing recent transactions (iii) Downloading bank statements, for example in PDF format (iv) Viewing images of paid cheques (v) Ordering cheque books (vi) Download periodic account statements (vii) Downloading applications for M-banking, E-banking etc.

Draw the steps and elucidate which type of authentication and encryption will be best suited for the Online Banking System.

1.What are the primary features and capabilities of online banking systems and how do they facilitate financial transactions for customers?

2.How does the secure file transaction from the server to the disk is encrypted in online banking system?

3.For the security authentication what are the prevention techniques used for online banking system?

4.what is the role of SSL in the online banking system application?

PROPOSED DESIGN WORK:

1.Identifying the key components:

Public Key Infrastructure (PKI):

- Used for secure key exchange, digital signatures, and certificate management.
- In online banking, PKI facilitates the issuance and management of digital certificates used for authentication and encryption.

Symmetric and Asymmetric Encryption:

- Symmetric encryption is used for encrypting large volumes of data efficiently, while asymmetric encryption is employed for key exchange and digital signatures.
- AES is commonly used for symmetric encryption, while RSA is popular for asymmetric encryption.

Hash Functions:

- Cryptographic hash functions like SHA-256 are used for data integrity verification.
- Hashing ensures that data transmitted between the user's device and the bank's server remains unchanged during transit.

Key Management:

- Proper key management practices are crucial for securely generating, storing, and exchanging encryption keys.
- Key rotation, key escrow, and key revocation mechanisms are implemented to enhance security.

2.Functionality:

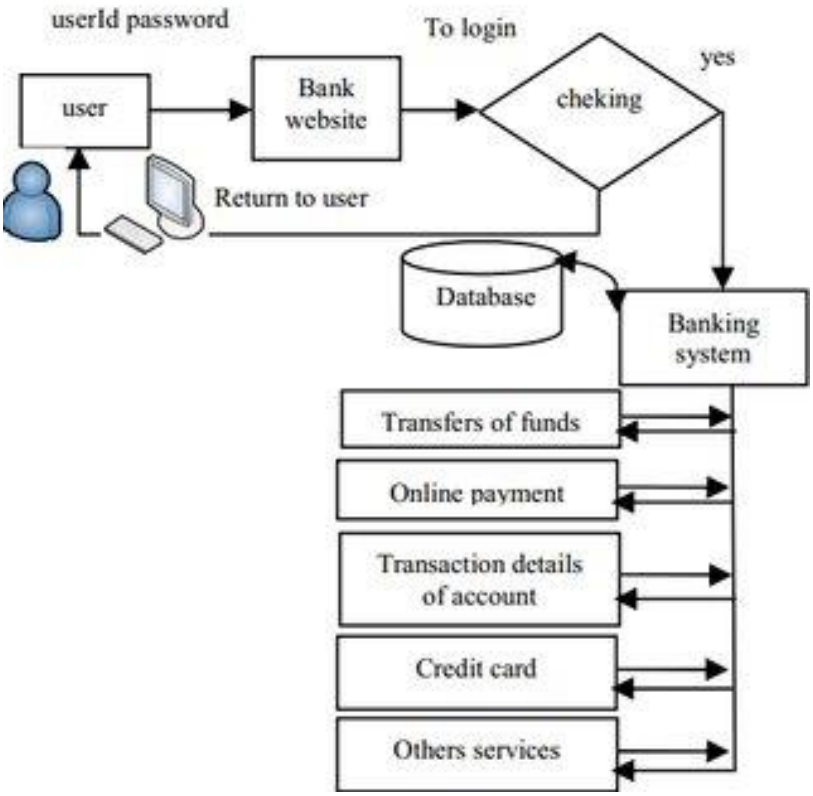
The PKI facilitates secure communication between the client and the server by managing digital certificates. Certificate Authorities (CAs) issue digital certificates, which are used to verify the identity of parties involved in the transaction. Digital certificates ensure that communication channels are secure and trustworthy.

Encryption algorithms like Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA) are employed to encrypt sensitive data during transmission and storage. AES is used for symmetric encryption, ensuring that data is securely stored and transmitted between the user's device and the bank's server. RSA is utilized for asymmetric encryption, enabling secure key exchange and digital signatures, thereby protecting data integrity and confidentiality.

Effective key management practices ensure the secure generation, distribution, and storage of encryption keys. Key rotation mechanisms regularly update encryption keys, minimizing the risk of key compromise. Key escrow services securely store encryption keys, enabling recovery in case of key loss or compromise.

3. Architectural Design:

The architectural design of an online banking system encompasses several key components aimed at ensuring the security, reliability, and compliance of the platform. At its core, the system comprises client-side and server-side architectures, each playing a distinct role in facilitating user interactions and processing transactions securely.



On the client side, a user-friendly interface provides customers with access to their accounts and enables them to perform various banking activities. To bolster security, client-side encryption libraries are integrated, empowering users to encrypt sensitive data such as login credentials and transaction details before transmitting them to the server. This ensures that data remains protected even during transit over potentially insecure networks.

A crucial aspect of the architectural design revolves around cryptography and security mechanisms. Public Key Infrastructure (PKI) manages digital certificates and facilitates secure key exchange, while encryption layers employ both symmetric and asymmetric encryption algorithms to safeguard data at rest and in transit. A robust key management system ensures the secure generation, distribution, rotation, and storage of encryption keys, bolstering data confidentiality and integrity.

UI DESIGN:

1.Layout design:

Flexible layout: The architectural blueprint of an online banking system is a sophisticated blend of client-side and server-side components, meticulously crafted to ensure security, reliability, and compliance with regulatory standards. At the forefront lies the client-side interface, offering users intuitive access to their accounts and enabling a spectrum of banking activities. To fortify data security, client-side encryption libraries empower users to encrypt

sensitive information, such as login credentials and transaction details, before transmission, bolstering confidentiality during transit across potentially vulnerable networks. Cryptographic techniques and security protocols form the cornerstone of the system's defense strategy. Public Key Infrastructure (PKI) orchestrates digital certificates and facilitates secure key exchange, while encryption layers deploy both symmetric and asymmetric algorithms to shield data at rest and in transit. A meticulous key management system oversees the lifecycle of encryption keys, ensuring their secure generation, distribution, rotation, and storage to fortify data confidentiality and integrity.

User friendly: In the design of an online banking system, creating a user-friendly experience is paramount alongside ensuring robust security measures. The user interface, where customers interact with the platform, is designed to be intuitive and accessible. Users can easily access their accounts and carry out various banking tasks hassle-free.To enhance security without compromising usability, encryption tools are seamlessly integrated into the user interface. Customers can encrypt sensitive data such as login credentials and transaction details with just a click, ensuring their information remains confidential during transmission over the internet.

Color selection: In the design of an online banking system, creating a user-friendly experience is paramount alongside ensuring robust security measures. The user interface, where customers interact with the platform, is designed to be intuitive and accessible. Users can easily access their accounts and carry out various banking tasks hassle-free.To enhance security without compromising usability, encryption tools are seamlessly integrated into the user interface. Customers can encrypt sensitive data such as login credentials and transaction details with just a click, ensuring their information remains confidential during transmission over the internet. Behind the scenes, a sophisticated server-side infrastructure handles user requests and manages data securely. While users focus on their banking needs, the system employs advanced security

mechanisms like firewalls and intrusion detection systems to safeguard against unauthorized access and cyber threats.

2.feasible elements used:

Element positioning: In the design of an online banking system, the paramount goal is to create a user-friendly experience while ensuring robust security measures. The user interface serves as the primary point of interaction for customers with the platform. It's carefully crafted to be intuitive and accessible, allowing users to effortlessly access their accounts and carry out various banking tasks. To bolster security without compromising usability, encryption tools are seamlessly integrated into the user interface. Customers can encrypt sensitive data such as login credentials and transaction details with ease, ensuring their information remains confidential during transmission over the internet. Cryptography plays a pivotal role in protecting user data. Public Key Infrastructure (PKI) ensures secure key exchange, while encryption algorithms safeguard data both in transit and at rest. Despite the complexity of these security measures, the system maintains a user-friendly approach, shielding users from the technical intricacies behind the scenes.

Accessibility: In the design of an online banking system, accessibility is as paramount as security and user-friendliness. The user interface serves as the primary point of interaction for customers, and it's crucial that it is designed to be inclusive and usable by individuals of all abilities. To achieve this, the interface is crafted with attention to accessibility standards, ensuring that users with disabilities can navigate and use the platform effectively. For visually impaired users, the system is designed to be screen reader-friendly, with descriptive alt text for images and proper labeling of form fields. Additionally, the interface employs high contrast and scalable fonts to accommodate users with low vision. Keyboard navigation is also prioritized, allowing users who cannot use a mouse to navigate through the platform easily. In terms of cognitive accessibility, the interface is kept simple and intuitive, with clear instructions and minimal distractions. Complex jargon is avoided, and information is presented in a straightforward manner to cater to users with cognitive disabilities.

3.Elements Function:

Here are the key elements and their functions for the topic of designing an online banking system with a focus on accessibility:

User Interface (UI):

Function: Serves as the primary point of interaction for customers.

Features: Designed to be inclusive and usable by individuals of all abilities.

Accessibility Considerations: High contrast, scalable fonts, keyboard navigation, descriptive alt text for images, and proper labeling of form fields.

Screen Reader Compatibility:

Function: Ensures that visually impaired users can navigate the platform effectively.

Features: Descriptive alt text for images, proper labeling of form fields, and compatibility with screen reader software.

Accessibility Considerations: Screen reader-friendly interface, clear and descriptive text, and adherence to accessibility standards.

Keyboard Navigation:

Function: Allows users who cannot use a mouse to navigate through the platform easily.

Features: Ability to navigate through all interactive elements using only the keyboard.

Accessibility Considerations: Prioritization of keyboard shortcuts and navigation flow for users with mobility impairments.

Cognitive Accessibility:

Function: Ensures that the interface is understandable and usable by users with cognitive disabilities.

Features: Simple and intuitive design, clear instructions, minimal distractions, and avoidance of complex jargon.

Accessibility Considerations: Presentation of information in a straightforward manner, avoidance of clutter, and adherence to readability guidelines.

Compatibility with Assistive Technologies:

Function: Ensures that the platform is usable with a wide range of assistive technologies.

Features: Compatibility with screen readers, magnifiers, voice recognition software, and other assistive devices.

Accessibility Considerations: Testing with various assistive technologies to ensure compatibility and usability.

Customizable Features:

Function: Allows users to adjust settings according to their specific accessibility needs.

Features: Customizable button sizes, color schemes, font sizes, and spacing options.

Accessibility Considerations: Empowerment of users to personalize their experience based on their individual needs and preferences.

Inclusive Design Principles:

Function: Guides the overall design process to prioritize accessibility and inclusivity.

Features: Incorporation of accessibility considerations from the early stages of design and development.

Accessibility Considerations: Collaboration with diverse user groups, adherence to accessibility standards and guidelines, and ongoing testing and refinement.

LOGIN TEMPLATE:

1.login process/sign up process:

CONCLUSION:

In conclusion, the emphasis on accessibility in the design of online banking systems is not just a matter of compliance; it's a fundamental commitment to inclusivity and equal access to financial services for all individuals. By prioritizing accessibility features such as screen reader compatibility, keyboard navigation, and cognitive accessibility, online banking platforms can empower users with disabilities to manage their finances independently and confidently.The integration of customizable features and adherence to inclusive design principles further enriches the user experience, allowing individuals to tailor their interactions based on their specific needs and preferences. Collaboration with diverse user groups and continuous refinement through testing ensures that accessibility remains at the forefront of the design process, fostering a culture of inclusivity and responsiveness to user needs.

Ultimately, an accessible online banking system is not just about providing equal access; it's about recognizing the inherent value of diversity and creating a platform that reflects the needs and experiences of all users. By embracing accessibility as a core principle, online banking systems can truly fulfill their mission of providing financial services that are accessible, equitable, and empowering for everyone.

Accessible design goes beyond compliance; it reflects a commitment to diversity, equity, and social responsibility. Through collaboration with diverse user groups, continuous testing, and refinement, online banking systems can evolve to meet the evolving needs of their users, including those with disabilities.Moreover, the benefits of accessibility extend beyond users with disabilities. An accessible design often leads to improved usability for all users, including older adults, individuals with temporary impairments, and those using mobile devices or low-bandwidth connections. Therefore, investing in accessibility not only expands the reach of financial services but also enhances the overall usability and effectiveness of online banking platforms.

Future Enhancements

1. **Enhanced Biometric Authentication:**
    1. **Multi-modal Biometrics:** Combining multiple biometric factors (e.g., fingerprint and facial recognition) to improve accuracy and security.
    2. **Liveness Detection:** Implementing advanced techniques to ensure the biometric data is from a live person and not a spoof.
2. **Improved Two-Factor Authentication:**
    1. **Physical Security Keys:** Using hardware tokens like YubiKeys for 2FA, which are more resistant to phishing.

2. **Push Notifications:** Utilizing app-based notifications instead of SMS for 2FA to mitigate SIM swapping risks.

3. **Password Alternatives:**
    1. **Password less Authentication:** Adopting methods like email-based links or biometrics to eliminate the need for passwords.
    2. **Behavioral Biometrics:** Using patterns in user behavior (e.g., typing speed, mouse movements) to authenticate users.

4. **Advanced Encryption Techniques:**
    1. **Post-Quantum Cryptography:** Developing algorithms that are resistant to potential future quantum computing attacks.
    2. **Homomorphic Encryption:** Allowing data to be processed without decrypting it, enhancing security in data processing.