Secure Online Transaction system with cryptography

SUNITHA S MUDDI
PG Student
Department of Master of Computer Application
The Oxford College of Engineering
Bommanahalli Bengaluru-560068
suithamuddi@gmail.com

MRIDULA SHUKLA
Associate professor
Department of Master of Computer Application
The Oxford College of Engineering
Bommanahalli Bengaluru-560068
mridulatewari005@gmail.com

ABSTRACT

In today's digital age, online business security is essential to protect the confidentiality, integrity and accuracy of sensitive information. This project introduces a secure online business developed in Java, using MySQL as the database management system and using the Advanced Encryption Standard (AES) algorithm for encryption. The aim of the project is to create and implement strong systems to ensure the security of online transactions, preventing unauthorized access, information leaks and fraud.

To achieve this goal, the AES algorithm, which is approved by the encryption algorithm known for its high security and performance, was used in the project. The system architecture follows the client-side model, where the client initiates and completes transactions, while the server manages transaction requests and interacts with the MySQL database.

Keywords: AES, MYSQL, cryptograph

I. INTRODUCTION

In today's digital environment, securing online transactions is essential to protect sensitive information from unauthorized access, leakage and fraud. The project introduced a secure online business carefully designed in Java, strengthened using the Advanced Encryption Standard (AES) algorithm, and using MySQL as the database management system. The aim of the program is to create a resilient platform that guarantees the confidentiality, integrity and accuracy of data transfer.

This project demonstrates the implementation of Java, MySQL and AES to improve business security. It offers cost-effective solutions for individuals, businesses and financial institutions looking to secure their online activities. By integrating encryption technology, the system ensures the confidentiality, integrity and authenticity of transactions on the Internet, thereby creating users' trust and confidence.

II. LITERATURE REVIEW

This study explores the use of Advanced Encryption Standard (AES) to secure online transactions. AES is an important encryption algorithm known for its strength and efficiency. This article examines the deployment of AES in various e-commerce businesses and its impact on business security. AES helps reduce the risk of data leakage and inaccessibility by encrypting sensitive data. This study also demonstrates the effectiveness of AES in terms of encryption and decryption speed, demonstrating its suitability for the current business environment. Research results show that AES improves the confidentiality and integrity of online transactions.

This whitepaper outlines the design methods, encryption methods, and security measures used to protect against cyber threats. The results show that the combined use of AES and RSA provides security, protects users' information, and increases the reliability of online banking services. This course focuses on using AES in e-commerce to secure online transactions. It highlights the challenges of protecting sensitive customer data and how AES solves these challenges.

III. EXISTING SYSTEM

Existing online businesses often have many security vulnerabilities, posing a significant risk to users' sensitive information. A major problem is weak encryption mechanisms that can cause data leakage during transmission and storage. Without encryption, data can be intercepted and leaked, compromising the confidentiality of transaction content and user data.

Another weakness of these systems is their reliance on regular authentication processes. Most systems use single passwords for user authentication, and these passwords can be easily exploited through password guessing, brute force attacks, or technology. These vulnerabilities allow unauthorized access to user accounts, facilitating fraud and affecting the integrity of the business.

In addition, early systems often lacked secure communication mechanisms. If protocols such as SSL or TLS are not used correctly, the risk of man-in-the-middle attacks increases. In this type of attack, the attacker intercepts and controls the information exchanged between the client and the server, which can lead to unauthorized changes to the content of the transaction, bankruptcy, and lack of trust in the system.

DISADVANTAGES OF EXISTING SYSTEM:

Inadequate encryption: The current system does not have a strong encryption mechanism.

Weak Authentication: Many legacy systems only use passwords for user authentication, and this can be easily compromised. Techniques such as password guessing, brute force attacks, and social engineering can lead to unauthorized access and fraud, compromising integrity.

Insufficient credentials: Existing systems often lack full credentials and are vulnerable to security attacks such as SQL injection and cross-site scripting (XSS). These vulnerabilities allow attackers to alter physical behavior, gain unauthorized access, and compromise the integrity of stored data.

Limited scalability and performance: Some legacy systems may lack scalability and experience performance issues, especially during business hours. This limitation can lead to slow response times, failed transactions, and an overall poor user experience.

Regulatory Challenges: Insufficient security measures in existing systems can make compliance with regulations such as the Payment Card Industry Data Security Standard (PCI DSS) or the General Data Protection Regulation (GDPR) difficult. Such negative actions may lead to legal and reputational damage.

Recognition of these deficiencies' points to the need for improved security measures. Integrated strong encryption, secure authentication mechanisms, secure communication protocols, data analysis, auditing and record keeping capabilities, timely incident response systems and user training programs will help overcome these problems. Solving these problems will lead to increased safety and security of online trading.

IV. PROPOSED SYSTEM

System Architecture:

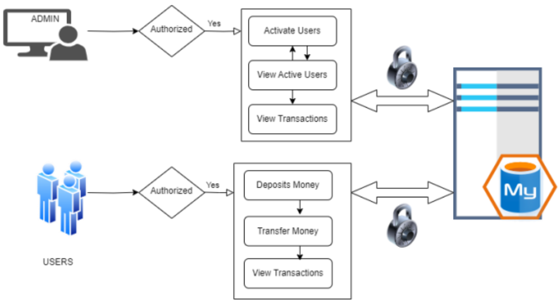


Fig 1 Architecture

The proposed system provides users with a secure environment to conduct business online, increases trust by protecting sensitive information, improves integrity, and reduces risks related to illegality and fraud. Implementation and evaluation of the system involves rigorous testing and practical procedures to ensure the system's effectiveness, efficiency and resistance to attacks. The research results of this project will contribute to the development of online security and cryptography research, paving the way for future advances in online security.

ADVANTAGES OF PROPOSED SYSTEM:

Strong authentication mechanism: The integration of security authentication method enhances the system against unauthorized access. This reduces the risk of fraud by ensuring only authorized users can initiate and transact.

Strong attack prevention: By using secure communication methods, the proposed system can protect against man-in-the-middle attacks. It creates encrypted and authenticated channels to prevent attackers from intercepting and manipulating data exchange.

V. MODULE DESCRIPTION

Admin Module:

This module supports the security of the online job and manages job startup, authentication and authorization. Ensure confidentiality and integrity of data transfer throughout the entire process. In this module, the administrator activates the user account by reviewing all the details provided by the user. After verifying the information, the administrator opens the account by creating a unique account for each user. Administrators can view details of rejected and active users, track all user transactions and resolve user complaints.

Users:

This submodule allows administrators to open user accounts after reviewing their applications. Verifies user information and provides access to the system.

This submodule allows administrators to create and manage user content, including assigning unique identifiers, setting user information, and ensuring accuracy.

Application rejected:

This change allows administrators to reject applications from users who do not meet the criteria or do not have sufficient information and to provide feedback to rejected applicants.

View rejected request:

This change allows administrators to view the list of users who have rejected applications for use or further review.

View active users:

This submodule allows administrators to view the list of current active users, providing details of user accounts and their status.

View results:

This submodule provides administrators with transaction information including sender, recipient, transaction amount, and timestamp.

See complaints:

This submodule allows administrators to view and manage user complaints.

Users Module:

This module provides a user-friendly interface for users to interact with the system. It includes functionalities such as displaying transaction details, managing user settings, and providing feedback to users regarding the status of their transactions.

Account Register:

This sub-module enables users to create an account by providing necessary personal information. It validates user inputs, checks for duplicate accounts, and generates unique account identifiers.

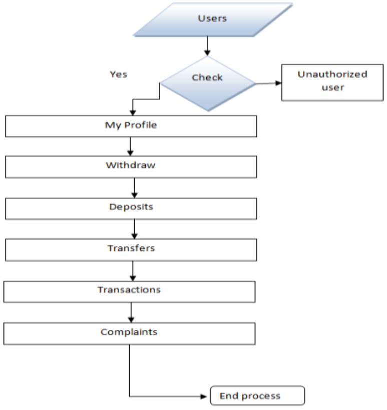


Fig 2 .Flow chart

Login with Credentials:

This sub-module allows users to log into the system securely using their credentials, such as username and password. It verifies the user's identity and grants access to their account.

Update Pin Number:

This sub-module allows users to update their PIN (Personal Identification Number) for added security. It ensures that only the authorized user can access the account.

Deposits Money:

This sub-module allows users to deposit money into their account. It verifies the transaction, updates the account balance, and generates a receipt for confirmation.

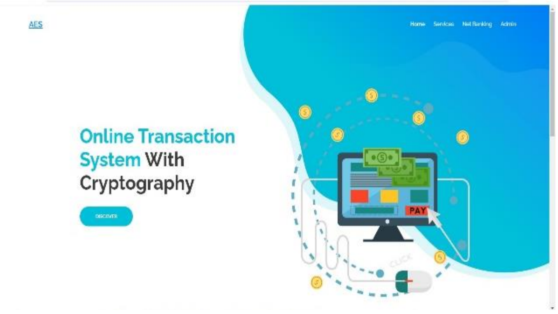
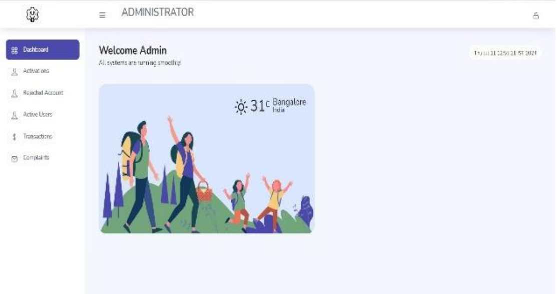


Fig 3: Home Page



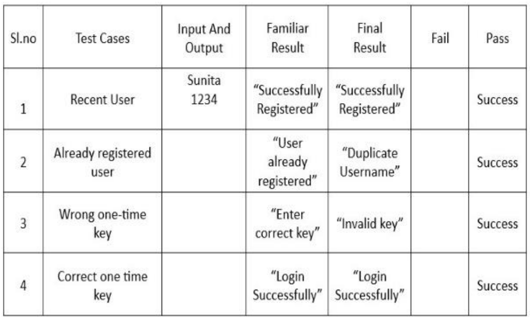
All systems are running smoothly!

Fig 4: Admin Page

VI.RESULT

The Secure Online Transaction System with Cryptography project lays a solid foundation for secure online transactions, but there are several areas for future work and improvement to enhance its capabilities. The following are potential avenues for future research and development:

Advanced Cryptographic Algorithms: While the project has implemented the AES algorithm for encryption, exploring and integrating other advanced cryptographic algorithms can provide additional security options. Researching and evaluating algorithms such as RSA, Elliptic Curve Cryptography (ECC), or post-quantum cryptography can strengthen the system's cryptographic capabilities.



Sl.no	Test Cases	Input And Output	Familiar Result	Final Result	Fail	Pass
1	Recent User	Sunita 1234	"Successfully Registered"	"Successfully Registered"		Success
2	Already registered user		"User already registered"	"Duplicate Username"		Success
3	Wrong one-time key		"Enter correct key"	"Invalid key"		Success
4	Correct one time key		"Login Successfully"	"Login Successfully"		Success

Table : Test cases

VII.CONCLUSION

Improve user education and awareness: Improving training on user assessment is important to promote online business security. Providing users with sound advice, guidance, and resources to detect and avoid scams, phishing attacks, and other online threats can help users make informed decisions and protect themselves.

Usability and user development: User research and feedback to gather information on usability and user experience can lead to further improvements. Incorporating user-cantered design principles and conducting usability tests can lead to better understanding and efficiency.

Integration with new technologies: Explore the integration of new technologies into the business, such as Internet of Things (IoT) devices or artificial intelligence Online shopping can open up new possibilities in terms of security and efficiency. Evaluating security implications and ensuring compatibility with existing systems are important considerations.

REFERENCES

1. A. Yadva, “Design and Analysis of Digital True Random Number Generator,” in Background of Random Number Generator, Virginia: Richmond, 2013.

2. E. Harrell, “Victims of Identity Theft 2014,” U.S. Department of Justice, Office of Justice Programs, North Carolina, 2015, pp.1-25.

3. G.C. Anup, “Credit Card Security,” Finland: Rovaniemi University, 2013.

4. A. Hedayati, "An Analysis of Identity Theft: Motives, Related Frauds, Techniques and Prevention." Journal of Law and Conflict Resolution Vol. 4(1), pp. 1-12, January 2012.

5. V. L. Reddy and T. Anusha. Combine use of steganography and visual cryptography for online payment system. International Journal of Computer Applications 124(6), 2015.