e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 7, Issue 4, April 2024

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 7.521

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly Peer Reviewed & Referred Journal |

| Volume 7, Issue 4, April 2024 |

| DOI:10.15680/IJMRSET.2024.0704027 |

Secure Online Transaction System with Cryptography

S.N. Sivasaran, Dr. R. Nagarajan Msc., M.Phil., Ph.D.

B.Sc. Computer Science, Sri Ramakrishna College of Arts and Science, Coimbatore, India

Assistant professor, Department of Computer Science, Sri Ramakrishna College of Arts and Science, Coimbatore, India

ABSTRACT: In today's digital age, secure online transactions are crucial for maintaining the confidentiality, integrity, and authenticity of sensitive data. This project presents a Secure Online Transaction System developed in Java, utilizing MySQL as the database management system, and employing the AES (Advanced Encryption Standard) algorithm for encryption purposes. The objective of this project was to design and implement a robust system that ensures secure online transactions, safeguarding against unauthorized access, data breaches, and fraudulent activities. To achieve this, the project leveraged the AES algorithm, a widely adopted symmetric encryption algorithm known for its high level of security and performance. To secure the sensitive transaction data during transmission and storage, the AES algorithm was implemented. It provides robust encryption and decryption functions, ensuring that the data remains confidential and tamper-proof. The keys used in the AES algorithm were securely generated and managed within the system. The implemented Secure Online Transaction System with Cryptography successfully provides a secure environment for users to conduct online transactions.

KEYWORDS: Online Transaction, Cryptography, Advanced Encryption Standard (AES), encryption, decryption.

I. INTRODUCTION

In an era dominated by digital transactions and online commerce, ensuring the security and confidentiality of sensitive information exchanged over the internet has become paramount. Traditional methods of securing online transactions often fall short in the face of sophisticated cyber threats, necessitating the implementation of robust cryptographic techniques.

A Secure Online Transaction System with Cryptography represents a cutting-edge solution designed to safeguard the integrity, confidentiality, and authenticity of data transmitted during online transactions. By leveraging cryptographic principles, this system aims to thwart malicious attacks such as eavesdropping, tampering, and unauthorized access, thereby fostering trust and confidence among users engaging in online transactions.

This introduction will explore the fundamental concepts of cryptography and its relevance in the context of online transactions. We will delve into the key components and mechanisms that underpin a secure online transaction system, highlighting how cryptographic techniques are employed to fortify various aspects of the transaction process. Additionally, we will examine the benefits of such a system in terms of enhancing security, protecting sensitive information, and mitigating the risks associated with cyber threats.

Overall, a Secure Online Transaction System with Cryptography serves as a cornerstone in the realm of e-commerce and digital finance, providing a robust framework for conducting transactions securely over the internet. By understanding the principles and functionalities of cryptographic techniques within this system, businesses and consumers alike can navigate the online landscape with greater confidence and peace of mind.

II. LITERATURE REVIEW

Random number generator is a key component for strengthening and securing the confidentiality of electronic communications. A true random number generator produces a stream of unpredictable numbers that have no defined pattern. Several Field Programmable Gate Array (FPGA) and Application Specific Integrated Circuit (ASIC) based approaches have been used to generate random data that requires analog circuit. RNGs having analog circuits demand for more power and area. These factors weaken hardware analog circuit-based RNG systems relative to hardware completely digital-based RNGs systems. This thesis is focused on the design of completely digital true random number generator ASIC. [1]

This paper provides a review of the unique effective techniques for sustainable development of prevention methods that have been offered to people and business. In addition, the paper reviews literature and summarizes the most effective ways for people and business to protect them against ID theft because victims may face a lengthy process of cleaning up the damage, such as their reputation, credit rating, and jobs. Identity (ID) theft is unauthorized obtaining of others confidential information in order to misuse it. ID theft is one of the major problems that impose billions of dollars annually on people and businesses across the globe. In 2008 only, 9.9 millions of Americans were victimized which show 22% increase compared to 2007. This report examines different types of frauds that are the major outcomes of ID theft. The frauds as the results of ID theft comprise ID fraud, financial fraud, tax fraud, medical fraud, resume fraud, mortgage fraud, and organized crimes such as money laundering, terrorism, and illegal immigration. [2]

A rapid growth in the E - Commerce market is seen in recent time in the whole extent of the world. With ever increasing popularity of online shopping, Debit/Credit card fraud and personal information security are major concerns for clients, Merchandiser and depository financial institution specifically in the case of CNP (Card Not Present). This paper presents a novel approach for providing limited information that is necessary for fund transfer during online shopping thereby safeguarding customer data and increasing customer confidence and preventing identity stealing. This method uses combined application of Steganography and visual cryptography for this purpose. [3]

The most accepted payment mode is credit card for both online and offline in today's world, it provides cashless shopping at every shop in all countries. It will be the most convenient way to do online shopping, paying bills etc. Hence, risks of fraud transaction using credit card has also been increasing. In the existing credit card fraud detection business processing system, fraudulent transaction will be detected after transaction is done. It is difficult to find out fraudulent and regarding loses will be barred by issuing authorities. Hidden Markov Model is the statistical tools for engineer and scientists to solve various problems. In this paper, it is shown that credit card fraud can be detected using Hidden Markov Model during transactions. Hidden Markov Model helps to obtain a high fraud coverage combined with a low false alarm rate. [4]

Identity theft is a very scary and real threat to everyone. In an attempt to give people peace of mind a new algorithm of mitigating risk is presented, the Secure Online Transaction Algorithm (SOTA). The proposed SOTA seeks to use two-factor authentication with the random codes. This form of user authentication has become widely accepted and many companies have started to implement this security feature. This can be utilized to identify users and establish secure way of purchasing items online. The proposed SOTA uses mobile devices to log into card accounts via an application to view the randomly generated code. This is then inputted on an online retailer's website when prompted in order to authenticate the individual making the purchase. This minimizes the possibility that an illegitimate user can use someone else's information to make fraudulent purchases. [5]

III. SYSTEM REQUIREMENTS

Hardware Requirements

System	: Pentium i3 Processor
Hard Disk	: 500 GB.
Monitor	: 15" LED
Keyboard	: Keyboard, Mouse
Ram	: 4 GB

Software Requirements

Operating system:	Windows 10.
Coding Language:	JAVA
Tool:	Netbeans 13
Database:	MYSQL

IV. SYSTEM ANALYSIS

Existing System

The existing online transaction systems often suffer from several vulnerabilities that pose risks to users' sensitive data. One of the primary concerns is the lack of robust encryption mechanisms, leading to potential data breaches during transmission and storage. Without encryption, data can be intercepted and compromised, jeopardizing the confidentiality of transaction details and user information. The existing system is also another weakness which lies in the authentication mechanisms employed by the earlier systems. Many systems rely solely on passwords for user authentication, which can be easily exploited through password guessing, brute-force attacks, or social engineering techniques. Such vulnerabilities increase the likelihood of unauthorized access to user accounts, enabling fraudulent activities and compromising the integrity of transactions.

Drawbacks:

- The existing system lacks robust encryption mechanisms, leaving sensitive transaction data vulnerable to interception and unauthorized access.
- This deficiency increases the risk of data breaches and compromises the confidentiality of user information.
- Many earlier systems rely solely on passwords for user authentication, which can be easily compromised. Password guessing, brute-force attacks, and social engineering techniques can lead to unauthorized access and fraudulent activities, compromising the integrity of transactions.
- Attackers can intercept and manipulate data exchanged between the client and server, leading to unauthorized modifications and potential financial losses.

Proposed System

The proposed system aims to address the limitations of the existing online transaction systems by introducing enhanced security measures and leveraging cryptography techniques. This system ensures secure online transactions with improved data confidentiality, integrity, and authentication. The proposed system incorporates the AES (Advanced Encryption Standard) algorithm, a widely recognized and secure symmetric encryption algorithm. AES ensures the confidentiality of transaction data during transmission and storage, protecting it from unauthorized access and data breaches.

The proposed system offers a secure environment for users to conduct online transactions. It instills confidence by protecting sensitive data, enhancing the integrity of transactions, and mitigating the risks associated with unauthorized access and fraudulent activities. The proposed system’s implementation and evaluation involve rigorous testing and validation procedures to ensure its effectiveness, performance, and resistance to potential attacks. The findings from this project contribute to the development of secure online transaction systems and cryptography research, paving the way for future advancements in online transaction security.

Advantages

- The proposed system utilizes robust encryption techniques, such as the AES algorithm, ensuring the confidentiality of transaction data.
- The integration of secure authentication mechanisms enhances the system’s defense against unauthorized access.
- This ensures that only authorized users can initiate and execute transactions, reducing the risk of fraudulent activities.
- The proposed system prioritizes user experience, offering a user-friendly interface that simplifies the transaction process.
- This enhances user engagement and satisfaction, promoting the adoption of secure online transactions.

V. SYSTEM IMPLEMENTATION

Admin Module:

This module facilitates the processing of online transactions securely. It handles functionalities such as transaction initiation, verification, and authorization. It ensures the confidentiality and integrity of transaction data throughout the process. In this module, Admin will activate the users’ accounts by viewing all the details given by the users. After verifying the details only admin activate the account. After activation a unique account number will be generated for each user accounts. Admin can view the rejected and active users details. Admin can view all the transactions made by the users. Admin can also view the complaints made by the users.

Activate Users:

This sub-module allows the administrator to activate user accounts after reviewing their applications. It validates user information and grants access to the system.

Create Account details for users:

This sub-module enables the administrator to create and manage account details for users. It involves assigning unique identifiers, setting up user profiles, and ensuring accurate information.

Reject Applications:

This sub-module allows the administrator to reject user applications that do not meet the system's criteria or have insufficient information. It provides feedback to the rejected applicants.

View Rejected applications:

This sub-module enables the administrator to view a list of rejected user applications for reference or further review.

View Active Users:

This sub-module allows the administrator to view a list of active users currently using the system. It provides an overview of user accounts and their status.

View Transactions:

This sub-module provides the administrator with access to view transaction details, including the sender, recipient, transaction amount, and timestamp.

View Complaints:

This sub-module allows the administrator to view and address 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. User's first register all the details requested in the account activation form after filling the form user have to submit. User will get a unique account number after activating the account. Users can perform the deposits, withdraw, transfer money to another accounts. User can view all the transactions and also if any complaint needs the register then users can raise the complaints. All the details shown to users are End to End Encryptions.

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.

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.

Withdraw Money:

This sub-module enables users to withdraw money from their account. It validates the transaction, deducts the requested amount from the account balance, and generates a receipt for record-keeping.

Transfer Money:

This sub-module facilitates money transfers between user accounts. It verifies the sender's account balance, deducts the transferred amount, updates the recipient's account balance, and generates transaction records.

AES Algorithm Module:

This module is responsible for encrypting and decrypting transaction data using robust encryption algorithms such as AES. It ensures that sensitive information remains confidential during transmission and storage, protecting it from unauthorized access.

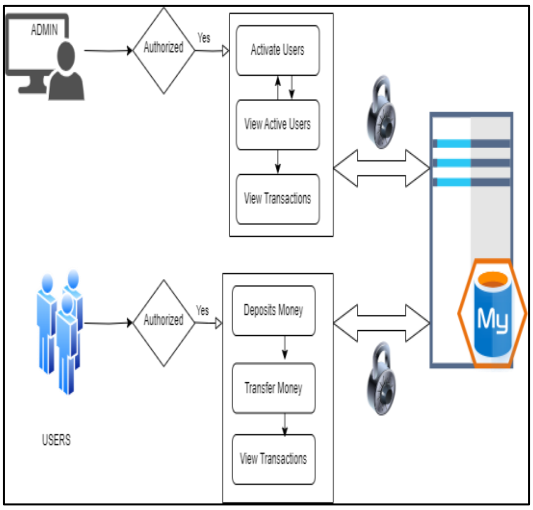
Encryption:

This sub-module implements the AES (Advanced Encryption Standard) algorithm to encrypt sensitive data. It takes the plaintext data and encryption key as input and generates encrypted ciphertext, ensuring data confidentiality during transmission and storage.

Decryption:

This sub-module performs the decryption process using the AES algorithm. It takes the encrypted ciphertext and the decryption key as input and produces the original plaintext data, allowing authorized users to access and interpret the information securely.

VI. SYSTEM ARCHITECTURE



VII. CONCLUSION

The Secure Online Transaction System with Cryptography project has successfully addressed the limitations of existing online transaction systems by introducing enhanced security measures and leveraging cryptography techniques. Through the implementation of robust encryption mechanisms, such as the AES algorithm, the project has significantly enhanced the data confidentiality of online transactions. By encrypting transaction data during transmission and storage, the system provides a secure environment, reducing the risk of data breaches and protecting sensitive information. Secure practices are implemented to protect against SQL injection attacks and unauthorized access to the database. Overall, the Secure Online Transaction System with Cryptography project has successfully developed a secure environment for online transactions. The project's outcomes contribute to the field of online transaction security by showcasing the effective implementation of cryptography techniques and advanced security measures. The proposed system provides users with enhanced data confidentiality, integrity, and authentication, promoting trust and confidence in online transactions. In conclusion, the Secure Online Transaction System with Cryptography project has successfully addressed the security challenges in online transactions, providing a robust and secure platform for users to conduct transactions with confidence.

VIII. FUTURE ENHANCEMENTS

Multi-factor Authentication: Introduce additional layers of authentication, such as biometric authentication or one-time passwords (OTP), to further strengthen user authentication and reduce the risk of unauthorized access. Blockchain Integration: Explore the integration of blockchain technology to enhance transparency, immutability, and decentralization in transaction processing, providing an additional layer of security and trust for online transactions. Biometric Payments: Enable biometric authentication for payment authorization, allowing users to securely authorize transactions using biometric identifiers such as fingerprint or facial recognition, enhancing convenience and security.

Mobile Wallet Integration: Integrate mobile wallet functionality to enable users to securely store payment credentials and conduct transactions seamlessly from mobile devices, catering to the growing trend of mobile commerce.

REFERENCES

1. Design and Analysis of Digital True Random Number Generator.
2. An Analysis of Identity Theft: Motives, Related Frauds, Techniques and Prevention.
3. Combine use of steganography and visual cryptography for online payment system
4. Study of Hidden Markov Model in Credit Card Fraudulent Detection
5. Secure Online Transaction Algorithm: Securing Online Transaction Using Two-Factor Authentication

INTERNATIONAL JOURNAL OF

MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com