International Journal of Advanced Research

in Electrical, Electronics and Instrumentation Engineering

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.317

Secure Electronic Fund Transfer Using AES

M.Sunil Kumar, J.P Sesha Sai, K.Krishna Chaitanya, Sk.Rownakh Zameer

UG Students, Dept. of CIC, Vasireddy Venkatadri Institute of Technology, Guntur, Andhra Pradesh, 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. The system architecture includes a client-server model, where the clients are responsible for initiating and executing transactions, while the server manages the transaction requests and interacts with the MySQL database. The Java programming language was used to develop the client and server components, facilitating platform independence and ease of deployment. 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 developed system serves as a practical example of how Java, MySQL, and AES can be combined to create a robust and secure online transaction platform. The project's findings can benefit individuals, businesses, and financial institutions by providing them with a secure framework for conducting online transactions and protecting sensitive information.

KEYWORDS: AES(Advanced Encryption Standard),MY SQL, JAVA, ENCRYPTION, DECRYPTION, etc.

I.INTRODUCTION

Computer security (Also known as cyber security or IT Security) is information security as applied to computers and networks. The field covers all the processes and mechanisms by which computer-based equipment, information and services are protected from unintended or unauthorized access, change or destruction. Computer security also includes protection from unplanned events and natural disasters. Otherwise, in the computer industry, the term security -- or the phrase computer security -- refers to techniques for ensuring that data stored in a computer cannot be read or compromised by any individuals without authorization. Most computer security measures involve data encryption and passwords. Data encryption is the translation of data into a form that is unintelligible without a deciphering mechanism. A password is a secret word or phrase that gives a user access to a particular program or system.Whenever we are making a transaction through online the major thing we should think about the security.At that point to secure the sensitive transaction data during transmission and storage, the AES algorithm was implemented. The AES algorithm operates on 128-bit blocks and supports key lengths of 128, 192, and 256 bits.

II.LITERATURE SURVEY

A.Yadva(2013) Designed and analyzed Random number generator is a key component for strengthening and securing the confidentiality of electronic communications. Random number generators can be divided as either pseudo random number generators or true random number generators. A pseudo random number generator produces a stream of numbers that appears to be random but actually follow predefined sequence. A true random number generator produces a stream of unpredictable numbers that have no defined pattern. There has been growing interest to design true random number generator in past few years. 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.

A.Hedayati(2012) This paper is a conceptual review of the major crimes leading to ID fraud and losses of millions of dollars for business and people in the world every year. The 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.Moreover, the various techniques that thieves use to attack individuals and organizations are discussed.

V.L.Reddy,T.Anusha(2015)discussed Combine use of steganography and visual cryptography for online payment system.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.

III.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.

This system integrates with a MySQL database management system to efficiently store and manage transaction-related information and user credentials. Secure practices are implemented to protect against SQL injection attacks and unauthorized access to the database. The system is designed to optimize performance and scalability, ensuring smooth and reliable transaction processing even during peak periods. Efficient algorithms and database optimization techniques are employed to enhance system responsiveness.

It 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.
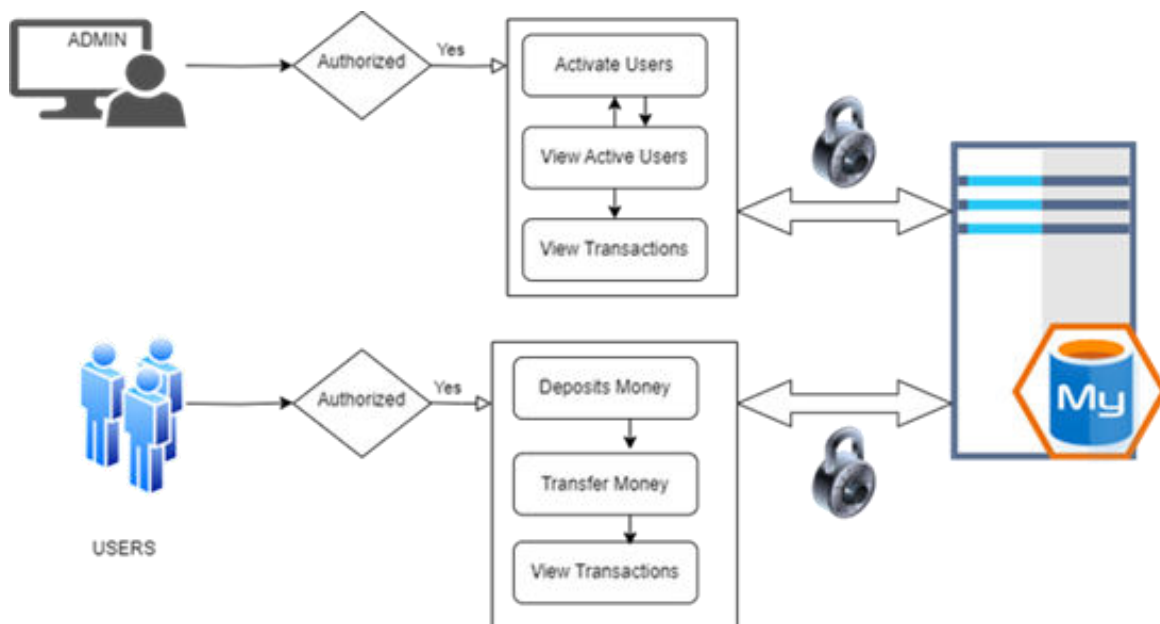
IV.SYSTEM DESIGN

Fig. 1 System Architecture

V. RESULT AND DISCUSSION

In the fig 2, it shows the output interface of the project which can be used to log in into our bank account .
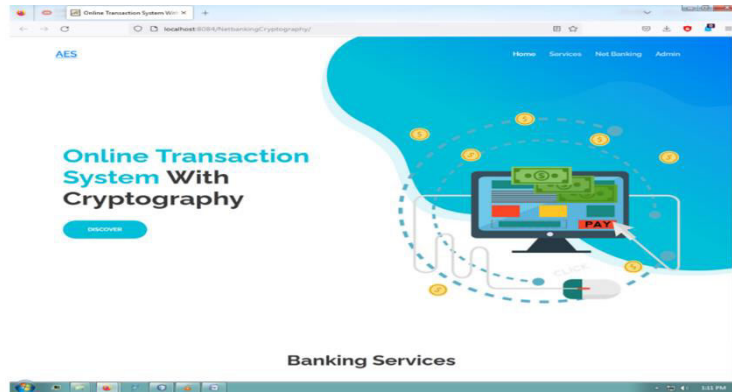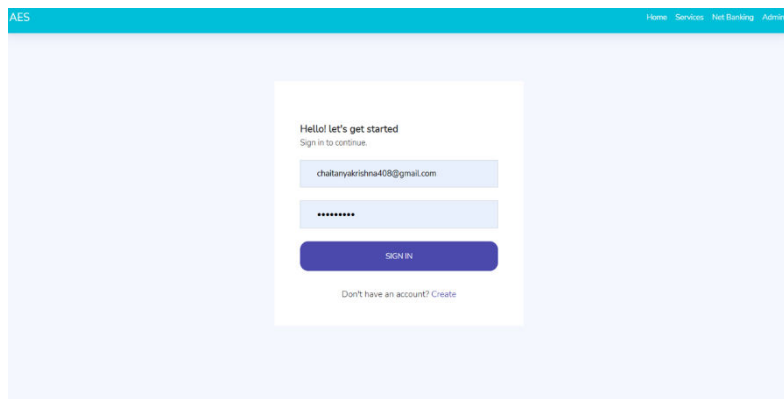

Fig. 2 Interface of project

Fig. 3 login page

In the fig 3, it shows the log in page to access the account by entering the correct credentials.
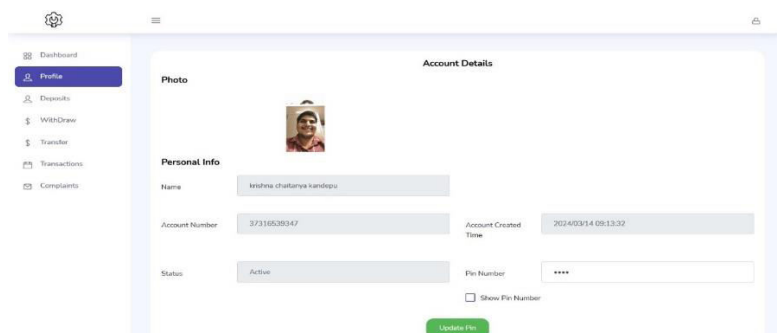

Fig. 4 profile page of user

In Fig 4 the profile page gives the details like account number,username,account status etc.,.


Fig. 5 Transaction details

In Fig 5 it shows the all transactions which are done by the user,status of the transaction,time etc.,.

VI.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.The project's objectives were to ensure the confidentiality, integrity,and authenticity of online transactions,safeguard sensitive data,and mitigate the risks associated with unauthorized access and fraudulent activities.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.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.

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: Rovaniemen 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.

[6] B. R. Williams, A. A. Chuvakin, and D. Milroy, PCI compliance: understand and implement effective PCI data security standard compliance, third edition. Waltham: Syngress, 2012.

[7] C. Hadnagy and P. Wilson, Social engineering: the art of human hacking. Hoboken, N.J: Wiley, 2011.

[8] Bhusari, V., and S. Patil. "Study of Hidden Markov Model in Credit Card Fraudulent Detection." International Journal of Computer Applications, (0975 –8887), Volume 20–No.5, April 2011.
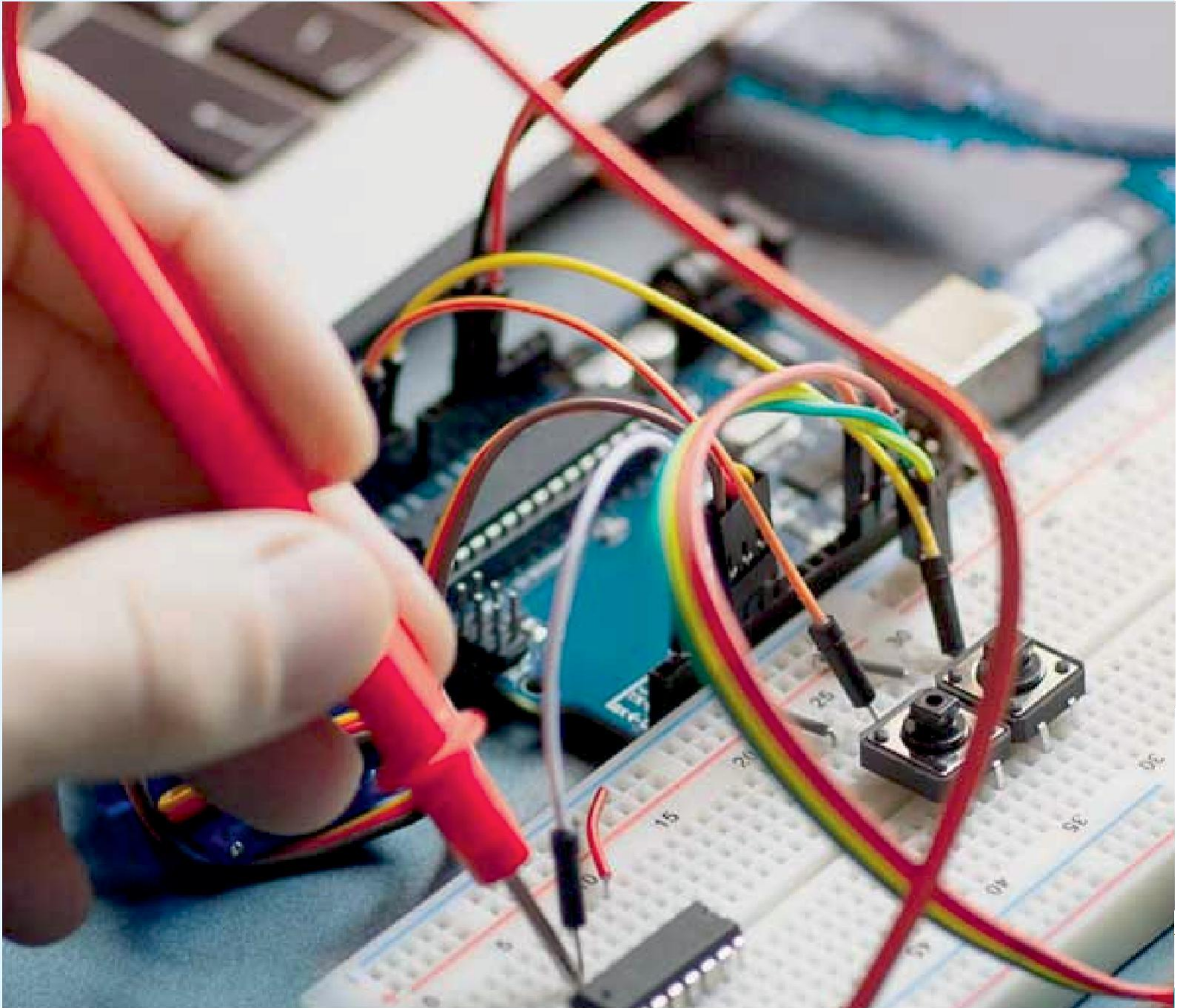
International Journal of Advanced Research

in Electrical, Electronics and Instrumentation Engineering

9940 572 462 6381 907 438 ijareeie@gmail.com