IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.105 ⁜ Vol. 9, Issue 6, June 2022

DOI: 10.17148/IARJSET.2022.9695

Advanced banking transaction using secured key generation

Vaibhavalaxmi S Hebsur[1], Thanuja J C[2]

[1]Dept. of MCA, Bangalore Institute of Technology, Bengaluru, India.

[2]Dept. of MCA, Assistant Professor, Bangalore Institute of Technology, Bengaluru, India.

Abstract: Advanced banking transaction using secured key generation is an online web application developed for secure banking transactions. The executive framework of the project is where the customer makes transactions without having any third party involved in the verification process of the transaction where a secret key and binary keys are generated. The secret key is sent to the customer's email whereas the binary key is sent to the customer's bank module. As in the case of understanding the process of the project it involves a shopping portal.

In this project, the admin handles the users, products, and transactions. To understand the process the project is organized in such a way that we can make transactions for purchasing products such as electronic devices, books, and shoes. This application is a fully computerized method for managing all the data. At the moment, All the transactions are made in the POS (point of sale) Method. It includes a lot of manual cycles and is tedious to use; it also keeps a nearby information base. To beat issues in the current System, A new " Advanced banking transaction with security analysis" is recommended to address shortcomings in the current system.

INTRODUCTION

Theft of credit cards and online data storage, which is one of the most prevalent issues in modern technology, are the two most frequent types of crime. Criminals occasionally opt to attack sales data systems in order to steal data from clients. With improved secured code, the New POS System was more affordable, but user information was more difficult to access in this way. Threats can quickly steal the card information using this technique.

This project tends to disconnect users and traffickers from the network as a result of these things because there is no security once the system is offline. This project outlines a secure e-commerce micro-payment transaction by creating a binary key and a secret key using cryptographic techniques. We always utilize an encrypted technique to conduct transactions in order to protect the security of the data. We must keep all offline payment information confidential in order to safeguard user data. Validation shouldn't involve any outside parties.

LITERATURE SURVEY

Improved E-Banking System With Advanced Encryption Standards And Security Models:

This world has become a global village as a result of new emerging technologies and large-scale corporations. Online services are offered by many commercial entities to international clientele. In order to meet the demands of the aforementioned commercial entities, banks from all over the world have facilitated transactions on an international scale through E-banking. Both bank customers and the banks themselves can benefit greatly from e-banking. Better service quality increases client satisfaction and gives banks a competitive edge over rival institutions. Online banking requires a high level of security in order to offer a stable, reliable, and secure environment that ensures secure data transmission and the identities of both the bank and the customer. Lack of security may cause people to have a less trusting or sceptical attitude about internet banking. Although users are drawn to online banking because of its ease, they appear to be primarily worried about identity theft and phishing. The literature review has analysed a number of research papers on e-banking security models and assessed the pros and cons of each. E-banking security measures include usernames, passwords, E-banking dongles, fractal pictures, biometric scanning, and high encryption standards. The security beyond the aforementioned techniques is the study's main concern. Three degrees of security are provided in this paper for online banking. Utilizing an internet dongle with integrated fingerprint scanning technology at the client and data transmission levels for banking servers.

Security in Next Generation Mobile Payment Systems: A Comprehensive Survey:

In many markets, cash payments still reign supreme, making up more than 90% of transactions in virtually every developing nation. In the modern era, using a cell phone is fairly commonplace. For many users, mobile phones have beyond the realm of simple communication devices and are now inseparable friends. Due to their widespread usage and accessibility, every subsequent person strongly relies on them. Every person wants to use their cell phone to manage their

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.105 ⁜ Vol. 9, Issue 6, June 2022

DOI: 10.17148/IARJSET.2022.9695

daily transactions and associated concerns. Threats are advancing along with the growth and development of mobile-specific security. We present an overview of various mobile phone security models in this study.

A model to authenticate requests for online banking transactions:

Online banking systems are becoming increasingly appealing targets for assaults as more customers use online banking. Financial institutions must determine how attackers compromise accounts and create safeguards to prevent it in order to keep the clients' trust and confidence in the security of their online banking services. This work outlines a modified architecture to authenticate clients for online banking transactions using the Identity Based mediated RSA (IB-mRSA) technique in conjunction with the one-time ID concept in order to increase security, fend off swallow's sorties, and shield against reply attacks. The newly developed system takes advantage of a technique for dividing private keys between the client and the server of the Certification Authority.

Existing System:

The POS (point of sale) System was cost-effective with enhanced secured code, but user information was more inaccessible through this manner. Threats can steal the card details by this method in a short period of time. Because there is no security after the system is offline.

Proposed System:

This project has a tendency to disconnect users and traffickers from the network as a result of these things. So to avoid this theft this application provides a transaction process without involving any third party and by generating a secret key and binary key which is only accessible by the customer. Here the binary key is sent to the bank module which is handled by the customer itself the and secret key is sent to user's registered email Id as part of verification for the transaction.

ALGORITHM

Md5

The MD5 hashing method (message-digest algorithm) is a one-way cryptographic operation that accepts as an input a message of any length and generates a fixed-length digest value that may be used to confirm the accuracy of the original message. When the MD5 hash function was first developed, one of its primary applications was as a secure cryptographic hash method for examining digital signatures. With the exception of preserving data integrity and spotting unintentional data contamination, MD5 has been judged no longer useful.

The process generates a 128-bit "message digest" or "fingerprint" of the data and can process messages of any length. It is proposed that building any message with a specific goal message digest or creating two messages with the same message digest are computationally impractical. The MD5 approach is intended for digital signature applications when a large file needs to be safely "compressed" before being encrypted with a private (secret) key under a public-key cryptosystem like RSA.

RESULT AND DISCUSSION

In this project "Advanced banking transaction using secured keys" the admin Manages the product details like inserting, deleting, and updating the products. He has the privilege to give authentication for the users so that the users can proceed. Admin manages the orders. He has the authority to view order details, customer details, and Transaction details where bank details are hidden from admin. Here the customer can view and update his data. He can view the product, purchase the products and make online transactions using the cryptographic technique without involving a third party where an OTP, a secret key, and a binary is generated. Here OTP is generated to verify the user before proceeding with the transaction and to make transactions securely the customer should enter a secret key and a binary key, he need not have to add bank or card details. Here to get the binary key admin need to login into the bank module and it's only accessible by the customer. By generating new keys for every transaction we can make a secure transaction.

CONCLUSION

In this project, we implemented online payment, which is a simple solution for preventing data from being collected by a micropayment system that operates online. The security analysis indicates that it is not only devoid of trite assumptions, but it is also the first approach to respond to questions for an existent system in which no client device information attacks are utilized to penetrate the system. In this project configuration, we're using the secret key and binary key elements to construct the secret, and we're encrypting the key with the block cipher AES technique using an attribute-based standard encryption method. Finally, we have some concerns about problems that have been identified and are being worked on in the future. We're specifically looking into the prospect of allowing online digital money to be used for a range of transactions while maintaining a similar level of security.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.105 ⁜ Vol. 9, Issue 6, June 2022

DOI: 10.17148/IARJSET.2022.9695

REFERENCES

1. Ulrich Ruhrmair, Marten van Dijk, "Attack Models and Security Evaluations", IEEE Symposium on Security and Privacy, 2013
2. Sharaaf N. A., Haamid M.N., Samarawickrama S.S., Gunawardhane C.N., Kuragala K.R.S.C.B, Dhishan Dhammearatchi, "Improved E-B anking System With Advanced Encryption Standards And Security Models", NTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 5, ISSUE 10, OCTOBER 2016
3. WAQAS AHMED1 , AAMIR RASOOL1 , ABDUL REHMAN JAVED 1 , (Member, IEEE), NEERAJ KUMAR 2,3, (Senior Member, IEEE), THIPPA REDDY GADEKALLU 4 , ZUNERA JALIL 1 , (Member, IEEE), AND NATALIA KRYVINSKA, "Security in Next Generation Mobile Payment Systems: A Comprehensive Survey", Received July 4, 2021, accepted August 11, 2021, date of publication August 16, 2021, date of current version August 26, 2021
4. Saad M. Darwish , Ahmed M. Hassan, "A model to authenticate requests for online banking transactions", Alexandria Engineering Journal (2020)
5. Robert W Sebesta," Programming the World Wide Web", 8th Edition, Pearson education, 2015.
6. Luke welling & Laura Thomson, PHP and MySQL Web Development 4th Edition, 2012
7. Steven Holzner, PHP Complete Reference, Mc Graw Hill, 2010
8. Ian Somerville, Software Engineering, 9th, Pearson Ed, 2015
9. Roger S. Pressman, Software Engineering: A Practitioners Approach, 7th, McGraw, 2007
10. Php,"w3school", [online] Available https://www.w3schools.com/php/
11. HTML, "developer.mozilla.org", [online]Available https://developer.mozilla.org/en-US/docs/Web/HTML
12. SQL, "javaTpoint", [online] Available https://www.javatpoint.com/sql-tutorial

