IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 5, May 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205014 |

Cyber Security Analysis for Banking and E-Commerce Web Server Management System

R. Mathan, B. Gowthaman, N. Naveen, P. Abishek, Ms.A. Ananthi

UG Student, Dept. of CSE., Sir Issac Newton College of Engineering and Technology, Nagapattinam, Tamil Nadu, India

UG Student, Dept. of CSE., Sir Issac Newton College of Engineering and Technology, Nagapattinam, Tamil Nadu, India

UG Student, Dept. of CSE., Sir Issac Newton College of Engineering and Technology, Nagapattinam, Tamil Nadu, India

UG Student, Dept. of CSE., Sir Issac Newton College of Engineering and Technology, Nagapattinam, Tamil Nadu, India

Assistant Professor, Dept. of CSE., Sir Issac Newton College of Engineering and Technology, Nagapattinam, Tamil Nadu, India

ABSTRACT: Now a day online shopping plays a vital role in our day to day life, and also it became a part of our life. At present 95% of the people uses smart phone to purchase through online. In this digital word, people are becoming even more smatter of doing money transactions through online payments. They use credit cards to pay their bills while shopping but in online shopping once purchase a product using credit card, it seeks only the OTP number instead of asking any other details. To purchase a product through online, bank details, address, phone number will be registered in a database. Next time, to purchase a product it will send the OTP to the registered mobile number and it will be delivered to the corresponding person to confirm. The hackers will be able collect the credit card details in some other public areas like petrol bunk, malls etc. while using this already. Even though the system has developed with security, the hackers may hack the credit card details and trying to purchase the product. The OTP will send it to the registered number the hacker will make some spam call to the mobile number, get the OTP and the money will be granted. This project was aims to designed and implemented to prevent the cyber theft in online shopping. Once the products are ready to purchase it will send the OTP along with the message carries the purchased items in the mail. Once the user check the mail if he/she is ordered the product then they are expected to place the OTP otherwise there will be a link along with the OTP if they press the link it will send an alert message to locate the nearby police station during the purchase. Using this preventive method can prevent the cyber theft while using online shopping. This system will be accessible to all the users those who have a valid registered mobile with secure transactions to find out the purchased product. The main objective of this project is to create a secure online purchase to provide more security.

I. INTRODUCTION

Credit card fraud in cybercrime refers to the use of technology with the help of internet to commit fraudulent activities to steal credit card information. This can include online purchases, data breaches, phishing scams etc. This project involves a link protection scheme to maintain security while purchasing the products through online. This empowers the clients to perform the essential sitting so as to manage an account exchanges at their office or at homes through PC or portable PC. The clients can get to the banks site for review their account subtle elements and perform the exchanges on record according to their necessities. With Internet Banking, the block

and mortar structure of the customary managing an account gets changed over into a tick and gateway model, accordingly giving an idea of virtual keeping money a genuine shape. In this way today's keeping money is no more restricted to branches. Also e-saving money encourages managing an account exchanges by clients round the clock internationally.

The essential point of this product is to give an enhanced configuration procedure, which imagines the future extension, and adjustment, which is vital for a centre division like keeping money. This requires the outline to be expandable and

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205014 |

modifiable thus a particular methodology is utilized as a part of building up the product. The user has account in bank can turn into an individual from internet managing an account. All exchanges are done online by moving from transactions in the same bank.

II. LITERATURE REVIEW

"**Enhancing security and privacy in biometrics-based authentication systems**": N. K. Ratha, J. H. Connell, R. M. Bolle Year : 2023

Reliable user authentication is becoming an increasingly important task in the Web-enabled world. The consequences of an insecure authentication system in a corporate or enterprise environment can be catastrophic, and may include loss of confidential information, denial of service, and compromised data integrity. The value of reliable user authentication is not limited to just computer or network access. Many other applications in everyday life also require user authentication, such as banking, ecommerce, and physical access control to computer resources, and could benefit from enhanced security. It is important that such biometrics-based authentication systems be designed to withstand attacks when employed in security-critical applications, especially in unattended remote applications such as ecommerce. In this paper we outline the inherent strengths of biometrics-based authentication, identify the weak links in systems employing biometrics-based authentication, and present new solutions for eliminating some of these weak links. Although, for illustration purposes, fingerprint authentication is used throughout, our analysis extends to other biometrics-based methods.

III. EXITING SYSTEM

The existing model of online shopping model, if the user places an order of products through online mart like Amazon, flip cart, etc. then the user needs to purchase the product with the details like address, name, and phone number whether they want credit card payment or UPI transactions or cash on delivery. The cash on delivery process does not have any problem. When the user use credit card payment method the OTP will occur to card holder number. While the hackers hacked the data they will contact the card holder using spam call and collect the OTP by asking questions like:

- From ABC bank that the user's loan must be verified and ask them to share the OTP for other verification process.
- In shopping mall the users may received a prize pool for the purchased items to conform the product and to share the OTP.
- Once the OTP has been shared and the cash will be debited for the purchasing product by the hackers. The user notifies the amount once the amount is withdrawn and it is not able to take action in this situation. This is the big problem in this filed.

3.1DISADVANTAGES:

There is no security in amount transactions

- No action is taken after the amount is debited
- There is no protection for the amount transactions
- Details about the product will not be shown and economic justification is not obvious
- OTP transactions is not be secured in shopping

IV. PROPOSED SYSTEM

Unlike the existing system that is relying on online shopping, this proposed system depends upon the security. Once the hackers hack the card then they will order a product to the delivery address. Hence it is a credit card based transactions they have to enter the OTP for further process. Once the OTP is received by the credit card holder the hacker will spam the person and get the OTP. This project helps to prevent this type of money transactions. Once the product is ready to order with the OTP will be alert in the g-mail account registered in bank account. Once the user get alert such as purchased product with corresponding amount as well as the security link then the OTP will be displayed. When the users get the notifications of the amount details, they will not send any further information or details. Otherwise if they share their details, then immediately the users money from their account will be deducted and credited to the hackers account. This situation can be avoided or handled by introducing that a link will be displayed to send an alert message to the cybercrime to file a complaint for taking further action from cybercrime departments.

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205014 |

4.1ADVANTAGES:

- The amount will be safe
- Action will be suddenly taken by the police

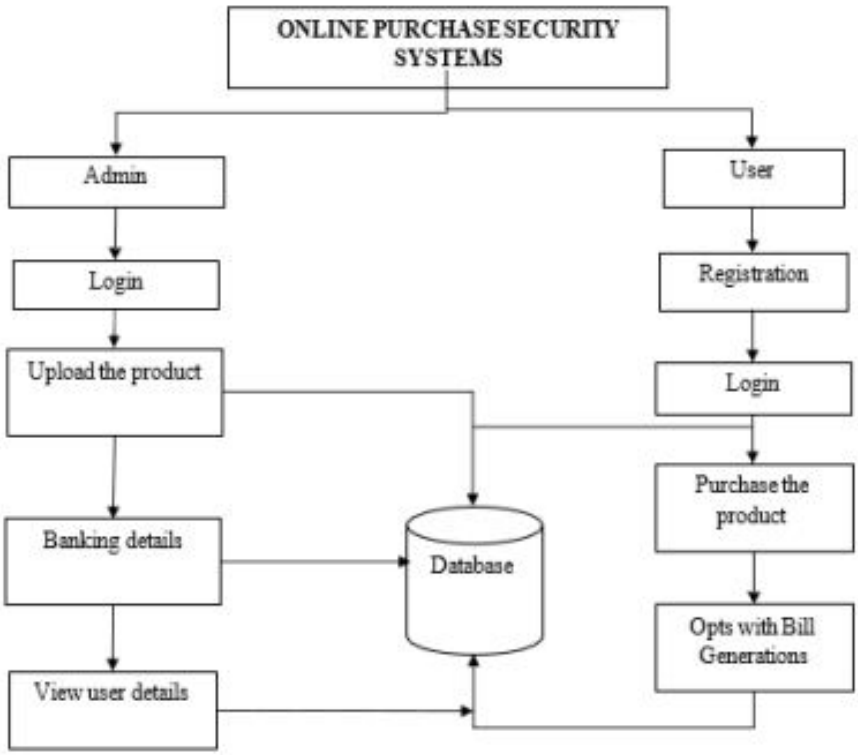

FIG:DATA FLOW DIAGRAM

- The product bill will be shown at the ordering
- Hackers can be reduced in this fraud detection
- Credit card transactions will be fraud free
- User friendly
- Secure bill history

ALGORITHM:

Algorithm 1 – RSA

RSA is asymmetric key Encryption technique and it is also known as public key encryption. It is one of the most secured algorithms and is growing at an exponential rate in many fields related to security. While designing an e-commerce application security is one of the major concern as many of the personal data of customers like payment details, goods detail etc. are presents on e- commerce application. To encrypt the product id, RSA algorithm will be used. The following steps are involved for the encryption and decryption of messages.
Suppose product id is 5

Step – 1: Let 2 prime number be r=7, s=3 Step – 2: Calculate n=r*s = 21
Step – 3: Phi = (r-1)*(s-1) = 12
Step – 4: Select e = 3 (e is a random number) Step – 5: Compute gcd(e,phi) = gcd(3,12) = 3
Step – 6: Compute d such that ed=3(mod phi) and d=e-1 mod phi d=1

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205014 |

Step – 7: Public key = (n,e)=(21,3) Step – 8: Private key = (n,d) = (33,1)
This above scenario is mathematical simulation based on RSA algorithm. Here, encryption and decryption used. RSA algorithm involves on the basis of PGP method.

TF-IDF Algorithm:

TF-IDF algorithm split into two terms TF, which means how many words are in the current news.

TF *(word)=number of repeated words appear in the document/total number of words in the document* where IDF refers to how necessary any terms are in all news. IDF gave a score to words.

IDF (*word*) = log (*total amount of documents*)/*number of document where the word appea*

Algorithm – TF Input:
Step – 1: D: Fake News
Step – 2: T: the unique term in all Fake News Output: weight matrix

Procedure:
Step – 1: For each ti €T do Step – 2: For each News € do
Step – 3: Wij = number of appearances of term ti in news di Step – 4: End for of news
Step –5: End for of term

Algorithm - Diffie Hellman
Diffie Hellman uses public key cryptography technique. Instead of generating encrypted data, this algorithm generates a secret key which would be common to both sender and the receiver. Some cryptography algorithm uses small length number key which can be identified easily by brute force attack. So, this algorithm use around 246 bits - 4096 bits to maintain more secure communication between merchant and customer in e-commerce application

Diffie Hellman key generation - secure e-commerce Application from third party attack.

Step – 1: Customer and merchant agree on two numbers “p” and “g” Step – 2: Customer select a secret number “c”
Step – 3: Merchant select a secret number “d”
Step – 4: Customer computes public number x = gc mod p Step – 5: Merchant computes public number y = gd mod p
Step –6: Customer and Merchant exchange their public numbers
A. Customers knows p, g, c, x, y
B. Merchant knows p, g, d, x, y Step –7: Customer computes kc = yc mod p Step – 8: Merchant computes kd = xd mod p
Step – 9: By the law of algebra, Customer “kc” and Merchant “kd” are equal kc=kd=k Customer and Merchant knows the secret value “k”[3]

V. CONCLUSION

This project is based on web privacy. Every day online purchase need to perform many activities related to users which needs huge infrastructure with more end user etc. Almost everybody faces issues with online shopping, primarily because the user needs to make a purchase decision without actually looking at the product based billing getting OTP. Then the user may need verfications billing that should be able to get the money back or the product pay amount. In this system, the user can easily perform the money transaction with security. In fake shopping sites analysis fake user, fake tractions spam calls, where it is almost impossible to get the money back, but it can able to builtup security analysis even more stronger . There are two main modules such as admin and user modules. In admin module, the admin can maintain the user details and modify the details. In user module, the user can perform the secure product through online. IN future this project can be extended to deploy AI based system to detect this frad.

REFERENCE

[1]. de Oliveira N. R., Pisa P. S., Lopez M. A., de Medeiros D. S. V., and Mattos D. M. F., (2021).”Identifying fake news on social networks based on natural language processing: Trends and challenges",Information, vol. 12, no. 1, pp. 38.
[2]. Vijay J. A., Basha H. A. and Nehru J. A. (2021). “A dynamic approach for detecting the fake news using random

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205014 |

forest classifier and NLP", in Computational Methods and Data Engineering. Springer, pp. 331-341.
[3]. Nikiforos M. N., Vergis S., A. Stylidou A., Augoustis A., Kermanidis, K. L and Maragoudakis, M. (2020). "Fake news detection regarding the Hong Kong events from tweets", in Proc. Int. Conf. Artif. Intell. Appl. Innov. Greece: Springer, pp. 177-186.
[4]. Kumar S., Asthana, R. Upadhyay S., Upreti, N. and Akbar M., "Fake news detection using deep learning models: A novel approach", (2020). Trans. Emerg. Telecommun. Technol., vol. 31, no. 2, p. e3767.
[5]. Sansonetti G., Gasparetti F., D'Aniello G., and Micarelli A. (2020. "Unreliable users detectionn in social media: Deep learning techniques for automatic detection", IEEE Access, vol. 8, pp. 213

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details