International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 3 Mar. 2021, pp: 497-506 www.ijaem.net ISSN: 2395-5252

Genetic Algorithm Using Secure Online Payment System for E-Commerce Websites

G.Sandhya Rani[1], Dr.P.Pedda Sadhu Naik[2]
PG Scholar M.Tech (CSE),Dr.Samuel George Institute of Engineering & Technology1
Professor&HOD of CSE Dept, Dr.Samuel George Institute of Engineering & Technology2

Submitted: 01-03-2021 Revised: 09-03-2021 Accepted: 12-03-2021

ABSTRACT: In recent time there is rapid growth in e-commerce market. Major concerns for customers in online shopping are phishing attacks. Phishing is a method of stealing personal confidential information such as username, passwords and credit card details from victims, redirecting user to fake websites. It is a social engineering technique used to deceive customers. Phishing attacks target ecommerce checkout pages; hackers are infecting checkout pages on legitimate ecommerce sites and redirecting customers to phishing checkout pages on malicious third-party sites. To address this problem, a new method is proposed to make secure online payment system. It represents a new approach which will authenticate both user and merchant for secure fund transfer. This method increases customer's confidence and ensures secured transaction.

Keywords: Phishing attacks, e-commerce, Genetic algorithm.

I. INTRODUCTION

Over the years number of users on internet has exponentially increased, this growth has given a big boost to online shopping. Online shopping is basically a way to check, feel and order the tons of product available for sell by the online retailers. We just need to select the product on the online retailer's website, it will generate the digital purchase order, after this we have to provide the credit, debit card or net banking details and the product you have selected will be delivered to you. Identity theft and phishing are the major pitfall of online shopping. Phishing is an unethical way to steal the end users personal as well as banking data. Some technical professionals are used to hack this data from online retailers so that they can misuse this data. Identity theft is an act of stealing and assuming another person's identity in order to commit fraud or other crimes like using this data for purchasing or opening new bank account.

Phishing Attacks Target E-commerce Checkout Pages, Hackers are infecting checkout pages on legitimate ecommerce sites and redirecting customers to phishing checkout pages on malicious third-party sites. A fake checkout page works like when a customer is ready to pay for selected products, they open a site's "checkout" page. But instead of landing on the site's own checkout page, they end up on a third-party site's checkout page. Without knowing this customer may enter all his payment details, as a result payment is made to fake merchant and customer loses his money as well as the ecommerce site owner will lose the sale. To address this fake checkout page phishing attack, we proposed a secure online payment system for E-Commerce Websites using genetic algorithm. This method increases customer's confidence and prevents transfer of funds to fake merchants.

1.1. Motivation

Online shopping has been receiving ever-increasing attention. Phishing attacks have become a major concern for customers. These phishing attacks at checkout pages in online shopping causee-commerce site owner lose his sale as well as customer loses his money. Our proposed system adds an extra layer of security to the existing system and provides more security by authenticating both customer as well as merchant. It helps in avoiding phishing attacks and ensures secure transactions between customer and merchant.

1.2. Problem Definition

In recent time there is rapid growth in E-Commerce market. Major concerns for customers in online shopping are phishing attacks. Phishing is a method of stealing personal confidential information such as username, passwords and credit card details from victims, redirecting user to fake websites. It is a social engineering technique used to deceive users. Phishing Attacks Target Ecommerce Checkout Pages, Hackers are infecting checkout pages on legitimate ecommerce

sites and redirecting customers to phishing checkout pages on malicious third-party sites. A fake checkout page works like when a customer is ready to pay for selected products, they open a site's "checkout" page. But instead of landing on the site's own checkout page, they end up on a third-party site's checkout page. Without knowing this customer may enter all his payment details, as a result payment is made to fake merchant and customer loses his money as well as the ecommerce site owner will lose the sale. To address this fake checkout page phishing attack, we proposed a secure online payment system for E-Commerce Websites using genetic algorithm. This method increases customer's confidence and prevents transfer of funds to fake merchants. The main objectives of the proposed system are: Prevent phishing attacks, Safeguard customers' credentials, and protect the reputation of merchant, Ensure reliable transactions.

II. LITERATURE SURVEY

A rapid growth in E-Commerce market is seen in recent time throughout the world. With ever increasing popularity of online shopping, Debit or Credit card fraud and personal information security are major concerns for customers, merchants and banks specifically in the case of CNP (Card Not Present). This paper presents a new approach for providing limited information only that is necessary for fund transfer during online shopping thereby safeguarding customer data and increasing customer confidence and preventing identity theft. The method uses combined application of steganography and visual cryptography for this purpose[1].Authentication plays a critical role in securing any online banking system, and many banks and various services have long relied on username/password combos to verify users. Memorizing usernames and passwords for a lot of accounts becomes a cumbersome and inefficient task. Furthermore, legacy authentication methods have failed over and over, and they are not immune against a wide variety of attacks that can be launched against users, networks, or authentication servers. Over the years, data breach reports emphasize that attackers have created numerous high-tech techniques to steal users' credentials, which can pose a serious threat. In this paper, we propose an efficient and practical user authentication scheme using personal devices that utilize different cryptographic primitives, such as encryption, digital signature, and hashing. The technique benefits from the widespread usage of ubiquitous computing and various intelligent portable and wearable devices that can enable users to execute a secure authentication protocol. Our proposed scheme does not require an authentication server to maintain static username and password tables for identifying and verifying the legitimacy of the login users. It not only is secure against password-related attacks, but also can resist replay attacks, shoulder-surfing attacks, phishing attacks, and data breach incidents [2].Core banking is a set of services provided by a group of networked bank branches. Bank customers may access their funds and perform other simple transactions from any of the member branch offices. The major issue in core banking is the authenticity of the customer. Due to unavoidable hacking of the databases on the Internet, it is always quite difficult to trust the information on the Internet. To solve this problem of authentication, we are proposing an algorithm based on image processing and visual cryptography. This paper proposes a technique of processing the signature of a customer and then dividing it into shares. Total number of shares to be created is depending on the scheme chosen by the bank. When two shares are created, one is stored in the bank database and the other is kept by the customer. The customer has to present the share during all of his transactions. This share is stacked with the first share to get the original signature. The correlation method is used to take the decision on acceptance or rejection of the output and authenticate the customer [3].Since the introduction of internet banking to the banking sector, many users have discovered hard ways that their use of e-banking can place their financial data at risk. Therefore, security has become a frequent concern for both banks and users. A phishing attack refers to any modus operand to trick customers into thinking that their financial institution is requesting information from them, when in reality, the request is coming from the hacker. Phishing leads to online identity theft, because it involves an unauthorized individual or group stealing confidential data. Unfortunately, phishing attacks are among the most common criminal activities that have been conducted by hackers, since the introduction of internet banking. The objective of this research is to investigate how phishing hackers attempt to steal users' data and conduct financial fraud. In turn, it explains how bank users can secure their online transactions with security solutions[4].In recent years E-shopping gained a tremendous growth due to its benefits. Even though benefits of E-shopping are considerable, it creates some security threats such as debit, credit card fraud, phishing etc. In this paper we introduce an E-payment system that provides an unrivalled security using visual and quantum cryptography. Visual cryptography hides

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 3 Mar. 2021, pp: 497-506 www.ijaem.net ISSN: 2395-5252

the details of customer by generating shares whereas Quantum cryptography secures the transmission of one time password. Image steganography embeds the share with one time password which results in secure transmission of share to bank. Proposed approach guarantees unconditional security than traditional E-payment system by using two importantcryptographic techniques [5].

Credit card is a small plastic card issued by a bank, building society, etc., allowing the holder to purchase goods or services on credit. Debit card is a card allowing the holder to transfer money electronically from their bank account when making a purchase. The use of credit cards and debit cards are increasing day by day. People are relying more on both cards nowadays than in the previous days. As credit cards and debit cards becomes the most popular mode of payment for both online as well as regular purchase, cases of fraud associated with it are also rising. In real life, fraudulent transactions are scattered with genuine transactions and simple pattern matching techniques are not often sufficient to detect those frauds accurately. In this project the process of Cryptography has been followed, it is one of the most important security technologies which used to secure the data transmission and the data itself. As the time and challenge growth, the cryptography also grows up with variety of encryption techniques and algorithms. Among the algorithms, one of the most popular is the Triple Data Encryption Standard algorithm. Triple Data Encryption Standard is a type of computerized cryptography where block cipher algorithms are applied three times to each data block. The key size is increased in Triple DES to ensure additional security through encryption capabilities. The major advantage of TDES is, it is three times slower than regular DES but can be billions of times more secure if used properly. Since it is based on the DES algorithm, it is very easy to modify existing software to use Triple DES[6].

III. EXISTING SYSTEM

In the existing system, customer selects the product and enters his details to proceed for payment. After entering the payment details customer gets an OTP to proceed the transaction and as a result funds are transferred to merchant. But here the problem arises when the customer is redirected to fake merchant page, where he enters all his details to proceed transaction but funds are transferred to fake merchant. Therefore, customer loses his money as well as merchant loses his sale. Here merchant to whom the funds need to be transferred is not authenticated.

Figure 3.1 Existing system architecture

IV. PROPOSED SYSTEM

In the proposed solution, we are authenticating the client as well as merchant. The information of customer which is given to the bank side is also protected by this proposed system. This system helps to clients to prevent phishing attacks by safeguarding customer data and increasing customer confidence to ensure secured transactions and also provides the authentication of both customer and merchant.In this way it is said to be a secure system.

In this proposed solution, customer places the order and checkout to proceed for payment. He enters bank account number and IFSC code in order to proceed the transaction, bank will verify both the details of customer and merchant. If both customer and merchant are authorized then bank generates two shares of OTP using a genetic algorithm. Bank sends one share of OTP to merchant and the other share to customer through email. Merchant sends his share of OTP that is received from bank to customer. Therefore, customer combines both the shares and clicks submit. Bank will verify the combined OTP and if it is valid then asks customer to enter his credit, debit card or net banking details. If details are valid then funds are successfully transferred to merchant account. If the merchant is fake then bank will never send the OTP to merchant. As a result, the transaction fails and customer money will be safe.

Considering the advantages of the system Such as, protecting customer identity and authenticating both merchant and server, it is definitely said that it is better secure system. The process carried is done step by step. So the system is scenario oriented and flow based.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 3 Mar. 2021, pp: 497-506 www.ijaem.net ISSN: 2395-5252

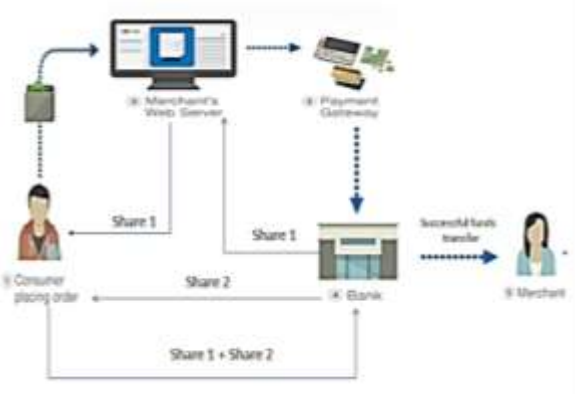


Figure 3.2. Proposed System Architecture

4.1 OTP Generation

Genetic algorithm: Genetic algorithm is kind of adaptive search algorithms which make use of the mechanics of natural selection and genetics. GA is part of Evolutionary Algorithms; which are used to solve optimization problems with the help of biological mechanism like selection, crossover and mutation. The key idea of GA is to imitate the randomness of the nature where natural selection process and behavior of natural system make population of individuals able to adapt the surrounding. We can say the survival and reproduction of the individuals is supported by exclusion of less fitted individuals. The population is generated in such a way that the individual with the highest fitness value is most likely to be replicated and unfitted individual is discarded based on threshold set by an iterative application of set of stochastic genetic operators.

The three basic operators used in Genetic algorithms contain: selection, crossover and mutation. The GA goes through the following cycle: Evaluate, select, mate, and mutate until some stopping criteria are reached. Reproduction and crossover together give genetic algorithms most of their searching power.

A. Selection

It is quantitative criterion based on fitness value to choose the chromosomes from population which are going to reproduce.

B. Crossover

In crossover operation two chromosomes are taken and a new is generated by taking some attributes of first chromosome and the rest from second chromosome.

C. Mutation

Mutation is used to maintain genetic diversity from one generation of population to the next. It is similar to biological mutation. GAs involves string-based modifications to the elements of a candidate solution. These include bit-reversal in bit-string GAs. Thisoperator randomly flips some of the bits in a chromosome.

Proposed method:

In the proposed method GA will be used in key generation process. The crossover and mutation operation is used along with Pseudo random number generators to make the key very complex. The process of generating the key from the Genetic Population has the following steps:

Step1: A pseudo random binary sequence is generated.

Step2: The generated string is divided in to two halves.

Step3: On the selected string uniform crossover operation is performed to achieve good randomness among the key.

Step4: After crossover operation, mutation, the bits of the string are swapped again to permute the bit values.

Step5: The same process i.e. step 3&4 is iterated two times.

Step6: The final two keys are converted to alphanumeric based on ASCIIvalues.

Step7: One of the key is sent to the customer and the other key is sent to the merchant through an email.

Step8: Merchant sends his share of key to the customer.

Step9: Customer enters both the shares of keys in the provided field. If both the keys are valid then authenticated and further customer is asked to enter his payment details to proceed the transaction.

Here the crossover and mutation is done two times to create more complexity and randomness in the key.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 3 Mar. 2021, pp: 497-506 www.ijaem.net ISSN: 2395-5252

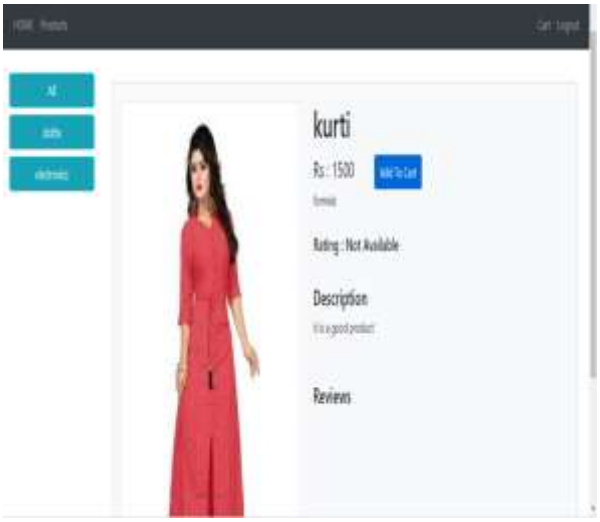
V. RESULTS

5.1 Home Page

5.2 E-commerce website user login page

5.3 Customer choosing products

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 3 Mar. 2021, pp: 497-506 www.ijaem.net ISSN: 2395-5252

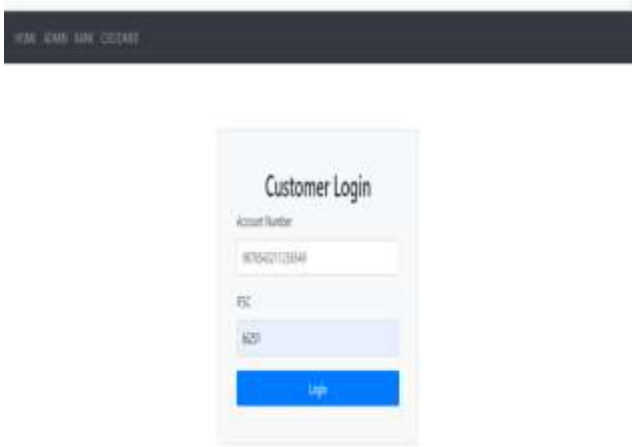


5.4 Customer selects a product and add it to cart

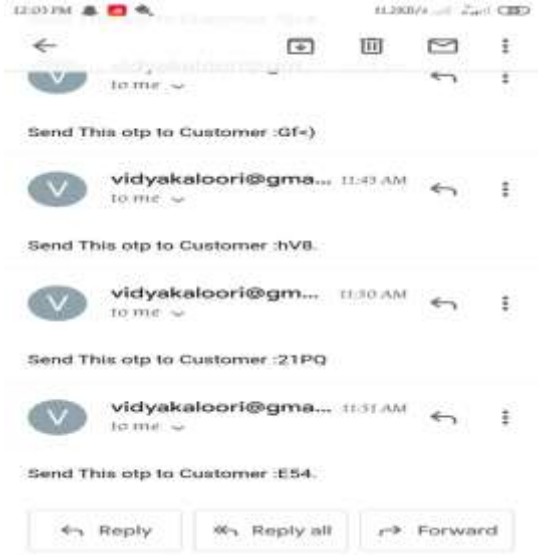
5.5 Checkout page

5.6 Customer choose a bank for payment

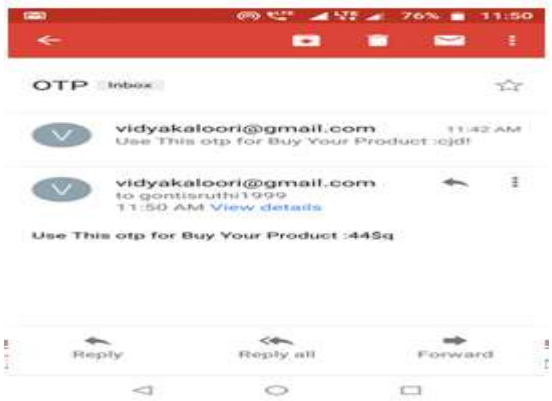
International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 3 Mar. 2021, pp: 497-506 www.ijaem.net ISSN: 2395-5252



5.7 Customer login with account number and IFSC code

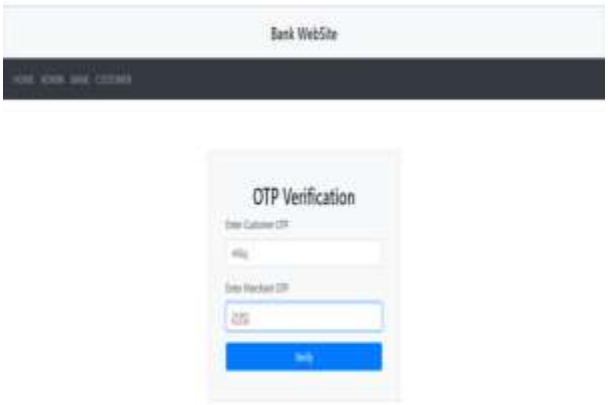


5.8 Customer OTPScreenshot



5.9 Merchant OTP

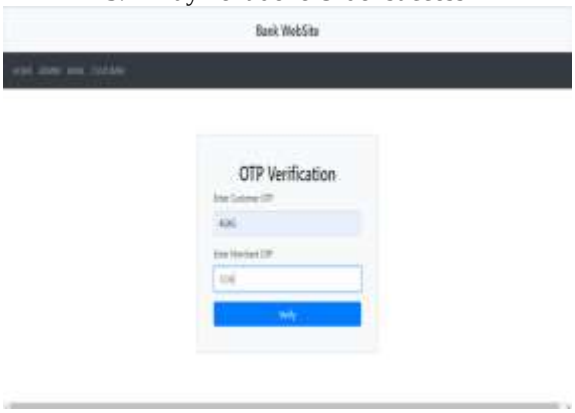
International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 3 Mar. 2021, pp: 497-506 www.ijaem.net ISSN: 2395-5252



5.10 Customer enters customer OTP and Merchant OTP

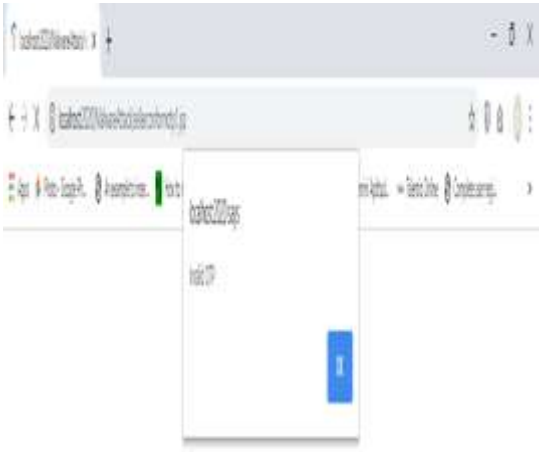
5.11 Customer Logins with his credentials

5.12 Payment done Order success



5.13 Entering Invalid Customer or Merchant OTP

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 3 Mar. 2021, pp: 497-506 www.ijaem.net ISSN: 2395-5252



5.14 Displays Invalid OTP message

VI. CONCLUSION

A payment system for online shopping is proposed by using genetic algorithm for the generation of OTP to provide secure fund transfer from the customer to the merchant and prevents fraud transactions. It secures the customer confidential information as well as protects the merchant from losing his sale. The system authenticates both customer as well as merchant. An extra layer of security is added to the existing system by authenticating customer, protecting customer identity and authenticating merchant. Implementation of Genetic Algorithm with pseudo random number generator, a very complex key, which is very difficult for cryptanalyst to attack. Therefore, the proposed method is concerned with the prevention of phishing attacks and provides security to customer and merchant. The proposed system can be used by all e-commerce websites to have more secured transactions as it adds an extra layer of security to the existing system by authenticating customer, protecting customer identity and authenticating merchant. As a future enhancement merchant OTP is automatically entered in the merchant OTP field to reduce the burden on merchant sending mail to each customer for each transaction. We can also use QR code method for transaction, this minimizes the details to be provided by the customer. We can also include URL matching mechanism to this proposed system. In this URL matching mechanism when customer redirects to payment page then that URL is verified with the original URL if matches then the payment proceeds otherwise that page need to be blocked and redirect back to cart page. This enhancement can add another layer of security to this proposed system.

REFERENCES:

[1]. SouvikRoy,P.Venkateswaran(2014). "Online payment system using steganography and visual cryptography". 2014 IEEE Students' Conference on Electrical, Electronics and Computer Science.

[2]. Abdulrahman Alhothaily, Chunqiang Hu, Alrawais (2017). "ASecure and Practical Authentication Scheme Using Personal Devices". IEEE.

[3]. ChetanaHegde,S. Manu,P.Deepa Shenoy, L.M.Patnaik.(2008)."Secure Authentication using Image Processing and Visual Cryptography for Banking Applications". 2008 16th International Conference on Advanced Computing and Communications.

[4]. P.A. Shemin,&Vipinkumar K. S. (2016). "E –Payment System Using Visual and Quantum Cryptography". International Conference on Emerging Trends in Engineering, Science and Technology (ICETEST - 2015).

[5]. TrihastutiYuniati, Rinaldi Munir (2018). "Secure E-Payment Method Based on Visual Cryptography". 2018 3rd International Conference on Information Technology, Information System and Electrical Engineering (ICITISEE).

[6]. S. Aishwarya , K.DEVIKA RANI DHIVYA. "Online Payment Fraud Prevention Using Cryptographic Algorithm TDES". International Journal of Computer Science and Mobile Computing, Vol.4 Issue.4, April-2015.

[7]. Alhuseen Omar Alsayed, Anwar Bilgrami."E-Banking Security: Internet

Hacking, Phishing Attacks, Analysis and Prevention of Fraudulent Activities".International Journal of Emerging Technology and Advanced Engineering, January 2017.

[8]. ShubhangiKhairnar and Reena Kharat."Online fraud transaction prevention system using extended visual cryptography and QR code".In Computing Communication Control and automation (ICCUBEA), 2016 International Conference on IEEE, 2016.

International Journal of Advances in Engineering and Management
ISSN: 2395-5252

IJAEM

Volume: 03 Issue: 03 DOI: 10.35629/5252

www.ijaem.net
Email id: ijaem.paper@gmail.com