Prevention of Fraud in Electronic Payment Gateway using Secret Code

Miss.Shilpa D. Dhobe,Asst. Prof. Khemutai K. Tighare, Asst. Prof. Sujata S. Dake

[1]*Wainganga College of Engineering and Management Dongargao Nagpur,Maharashtra, India*
[2]*Assistant Professor Department of Computer Science and Engineering,*
Wainganga College of Engineering and Management Dongargaon Nagpur, Maharashtra, India.
[3]*Assistant Professor Department of Computer Science and Engineering,*
Wainganga College of Engineering and Managemen Dongargaon Nagpur,, Maharashtra, India.

ABSTRACT

Now a days the volume of electronic transactions has raised significantly, mainly due to the popularization of electronic commerce (e-commerce), such as online retailers (e.g., Amazon.com, eBay, AliExpress.com). The use of credit cards has increased and it becomes the popular mode of payment for both online and offline purchases. Fraud is one of the major ethical issues in electronic payment Gateway. Fraud essentially involves using deception to dishonestly make a personal gain for oneself and/or create a loss for another. We also observe a significant increase in the number of fraud cases, resulting in billions of dollars losses each year worldwide. Therefore it is important and necessary to prevent and use techniques that can assist in fraud detection and prevention. Preventing fraud in real-time is not easy so it is not surprising that many fraud systems have serious limitations. Encryption is the process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized cannot. In this system credit card numbers for online transactions, other personal and financial information all need to be encrypted. System reduces fraud by using Secret Code. This secret code stored in encryption format so unauthorized user cannot use this secret code. The goal of this paper is to provide a comprehensive review of preventing fraud in Electronic Payment Gateway.

***Key Words*: E-commerce, Electronic Payment Gateway, Credit Card, Secret Code.**

1. INTRODUCTION

E-commerce is evolving rapidly and now it is reality. Efficient and effective electronic payment services are already established and accepted by businesses and consumers. Advances in e-commerce, expansion of modern technologies and global communication provide a large number of business opportunities, as well as new threats for the banking and financial services. The advancement in the electronic commerce technology, the use of credit cards has increased and it becomes the popular mode of payment for both online and offline purchases. E-commerce provides the capability of buying and selling products, services and information on the Internet by using electronic payment systems. In electronic payment systems the exchange of value is represented by the exchange of data. Credit card transactions have become a standard for Internet and Web based payments. There are millions of credit card transactions processed each day.

Credit card is a plastic-card issued by a bank or nonbanking financial company (NBFC) ready to lend money (give credit) to its customer. It is a suitable alternative for cash payment. It is used to execute transactions which are compiled through electronic devices like a card swapping machine, computer with internet facility, etc.

1.1Credit Card Operation:

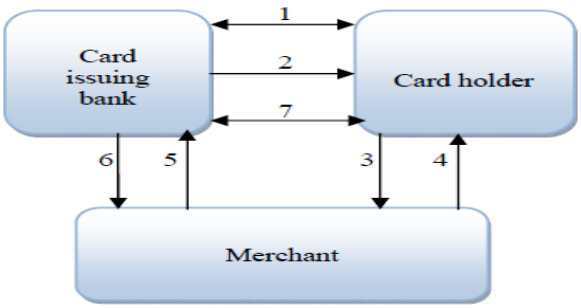

Figure 2Credit Card Operation

The credit card operation consists of the steps as follows:

1. Contract for credit card: there is a contract between cardholder and the cared issuing bank regarding limit etc.

2. Card issue: Once the contract is finished, the bank issues the credit card to their customer.

3. Purchasing goods: A Cardholder purchases goods/services and offers the credit card.

4. Deliver goods: A merchant establishment delivers goods once taking a valid credit card and noting the number and taking signatures.

5. Raising of bill: The merchant establishment raises the bill for the purchase and sends it to the credit card issuing bank for payment.

6. Payment for bill: The issuing bank pays the amount to the merchant establishment.

7. Payment of Credit card: The issuing bank raises bill on the credit cardholder and sends it for payment. The credit cardholder then pay the amount to the issuing bank.

Credit card fraud is defined as a transaction when an individual uses another individuals. credit card or corresponding data for payment of goods or services while the owner of the card and the card issuer are not aware of that. There are many types of fraud in electronic payment systems. Fraud can occur in a number of ways including:

- Counterfeit fraud,
- Merchant fraud,
- Card-not-present fraud,
- ATM fraud,
- Internet fraud,
- Lost or stolen cards,
- Identity theft,
- Skimming or copying of electronic data contained on magnetic stripe, and
- MOTO (mail order telephone order) fraud.

Fraud prevention describes measures to stop fraud occurring in the first place. When prevention fails then fraud detection comes into play.

Bhatla et al [1] said that the rate at which Internet credit card fraud occurs is 12 to 15 times higher than face-to face transactions. The 12th annual online fraud report by CyberSource [2] shows that, for most of the current decade, merchant online fraud losses continued to increase, reaching a peak of $4 billion in 2008. According to Siddhartha Bhattacharyya et al. [3] with the growth in credit card transactions, as a share of the payment system, there has also been an increase in credit card fraud.

1.2 Types of Fraud:

I. Application Fraud:

This kind of fraud happens once someone falsifies an application to acquire a credit card. Application fraud is committed in 3 ways:

Assumed identity, wherever an individual illicitly obtains personal info of another person and opens accounts in his or her name, using partly legitimate info.

Financial fraud, wherever an individual provides false info regarding his or her financial standing to acquire credit. Not-received items (NRIs) additionally known as postal intercepts occur once a card is purloined from the postal service before it reaches its owner's destination.

II. Lost/ Stolen Cards:

A card is lost/stolen once a legitimate account holder receives a card and loses it or somebody steals the card for criminal functions. This sort of fraud is in essence the best way for a fraudster to get hold of alternative individual's credit cards without investment in technology. It is also maybe the toughest kind of ancient credit card fraud to tackle.

III. Account Takeover:

This type of fraud happens once a fraudster illicitly obtains a valid customers' personal info. The fraudster takes control of (takeover) a legitimate account by either providing the customers a/c.no or the cardnumber. The fraudster then contacts the card issuer, masquerading as the real cardholder, to ask that mail be redirected to a new address. The person who commit the fraud reports card lost and asks for a replacement to be sent.

IV. Identity theft: Identity theft/fraud refer to crime in which fraudster illegally obtains and uses another person personal information in some way that involves deception or fraud to gain something of value. Identity theft/fraud is the most serious crime for the person whose information is stolen as well as the financial institution.

V. Phishing : Phishing is a well-known technique for obtaining confidential information from an user by posing as a trusted authoring. Phishing is an attempt by fraudster to „fish" for your baking details through emails with attachment or hyperlinks. The e-mail appears to be send from legitimate organization to trick people in order to reveal sensitive information. On clicking the attachment or the hyperlink the computer system get infected with malware. During the next online transaction the malware will activate and steal private and personal financial information, including credit card numbers, PIN number which is used by fraudster to steal money from the account. Malware or „Malicious Software" is software which includes computer viruses, worms, Trojan Horses, spyware and other malicious software.

VI. Spoofing or Website cloning: This is an act of creating a hoax web site or to say duplication of a website for criminal use. The fraudsters use legitimate companies name, logos, graphics and even code. This usually take form of know chat room or trade sites where in people

would innocently giving out personal information to criminals or make a fake purchase of a product the does not exist. Site cloning is the process where fraudsters close whole site or simply the pages from which the customer made a purchase. There is no option left with the customers to believe that they are not dealing with the company that they wished to purchase goods or services from because the pages that they are viewing are somehow.

VII. Skimming: Another kind of fraud being committed is skimming which is fast emerging as the most popular form of credit card fraud. Mostly, fraud cases of Counterfeit fraud involve skimming. It is a method where the actual data on a card's magnetic stripe is electronically copied onto another. Fraudster(s) does this even as the customer is waiting for the transaction to be validated through the card terminal. Card holder doesn't t know about this activity and it is very difficult for customer(s) to identify. In some of the cases, details obtained by skimming are used to carry out fraudulent card not-present (CNP) transactions by fraudsters.

2. LITERATURE REVIEW

2.1 Background History

2.1.1 Online Fraud

Credit is a method of selling goods or services without the buyer having cash in hand. A credit card is only an automatic way of offering credit to a consumer. Today, every credit card carries an identifying number that speeds shopping transactions. According to Encyclopedia Britannica (no date), "the use of credit cards originated in the United States during the 1920s, when individual firms, such as oil companies and hotel chains, began issuing them to customers."

Online fraud is committed via web, phone shopping or cardholder not- present. Only the card's details are needed, and a manual signature and card imprint are not required at the time of purchase. In the credit card business, fraud occurs when a lender is fooled by a borrower offering him/her purchases, believing that the borrower credit card account will provide payment for this purchase. Ideally, no payment will be made. If the payment is made, the credit card issuer will reclaim the amount paid.

2.1.2 Payment Gateway

A payment gateway, also known as the processor or credit card processor, connects the merchant's website and shopping cart, the acquiring bank (merchant's bank), and the issuing bank (cardholder's bank). The payment gateway handles all communication messages between these entities. By handling the two key parts of credit card processing, authorization and payment settlement, the payment gateway is the key link in an online transaction.

During authorization, credit card information from the merchant's website is sent to the payment gateway by the shopping cart, which verifies the card information and then sends a request to the cardholder's bank for the card to be charged. If the card information is valid and the customer's credit is sufficient, then the credit card company sends an approval to the payment gateway, which in turn communicates with the shopping cart and confirms the authorization for the purchase. The payment gateway then initiates a payment settlement (funds transfer) to allow the transfer of funds from the customer's credit card account to the merchant's bank account.

3. RELATED WORK

The technology for detecting credit card frauds is advancing at a rapid pace. This has attracted much researchers attention recently due to increase in credit card fraud. Some of the popular techniques employed by Issuing and Acquiring banks these days are; rule based systems, neural networks, data mining, grid based hidden Markov Model, etc.

V. Dheepa and R. Dhanapal developed [4] credit card fraud detection using Support Vector Machines. Support Vector Machines are employed and efficient feature extraction method also adopted. If any discrepancies occur in the behaviours transaction pattern then it is predicted as suspicious and taken for further consideration to find the frauds.

3.1 Finger Print Recognition

Priyadharshini, and G.Adiline Macriga [11] Credit Card Fraud Detection using Finger Print Recognition. The main objective of this proposed method is to achieve resilience by adding two new, real time, data mining based layers to complement the two existing non data mining layers proposed system utilizes real time data mining-based security layers (CD and SD) for identity crime detection. The first new layer is Communal Detection (CD):

the white list-oriented approach on a fixed set of attributes. To complement and strengthen CD, the second new layer is Spike Detection (SD): the attribute-oriented approach on a variable-size set of attributes.

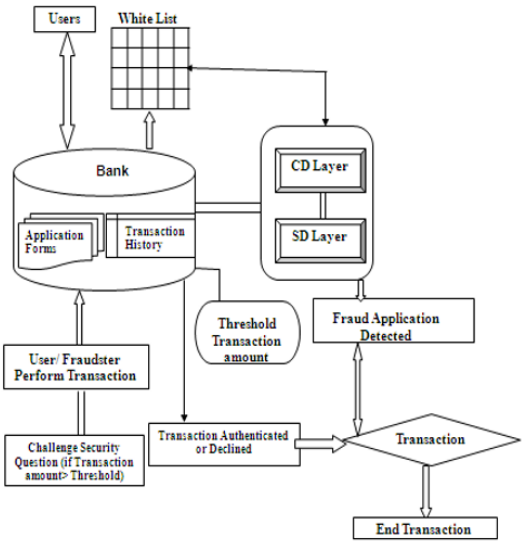

Fig.3 Architecture Diagram for Fraud Detection using Finger Print Recognition

The CD and SD layers are continuously updated. Data are traditionally based on a binary representation in which discrete information is assumed (even in continuous data, range representations are possible) and so the operations involve "modifying" bits without concern for any underlying semantics. In dealing with text data, representing the linguistic knowledge is an important issue in which traditional binary coding is insufficient, and so new representation schemes should be investigated.

3.2 Hidden Morkov Model

Twinkle Patel, Ms. Ompriya Kale[6] developed credit card fraud detection using Hidden Morkov Model. HMM is used along with HOTP to make HMM more secured as we have seen above HMM [5] needs training and during training some transactions are involved and fraud is not detected during training but it is detected after training so HOTP is used for secured approach in HMM so make initial transaction secure by sending one time password i.e. security code to clients mobile if the security code entered by client is correct then only transaction is done successfully else transaction is not allowed to progress. But once the HMM is trained and ready for detection client does not need to enter any security code unless HMM detects the transaction is above threshold value. If the transaction is above threshold value security code is send to mobile and client need to enter that security code then only transaction is done successfully else transaction is not allowed to progress [6].

Detection System using HMM

As shown in Fig. 3 there are two phases of HMM. In training phase card holder transaction amount is converted in observation symbols i.e. low medium or high and form sequences from them. After the sequence is formed threshold is calculated from the sequence of amount.

In the detection phase client enters amount and form an initial sequence of symbol. Let O1, O2, O3…….OR be such sequence of length R up to time t. This sequence is the input to HMM and from that we compute the threshold of acceptance α1. Let OR+1 be a symbol of new transaction at time t+1.now with new transaction we generate a new sequence O2, O3,…….OR ,OR+1. We input these sequence in HMM and calculate the new threshold of acceptance if amount is less than threshold than amount is added in new sequence else the it is detected as anomaly.

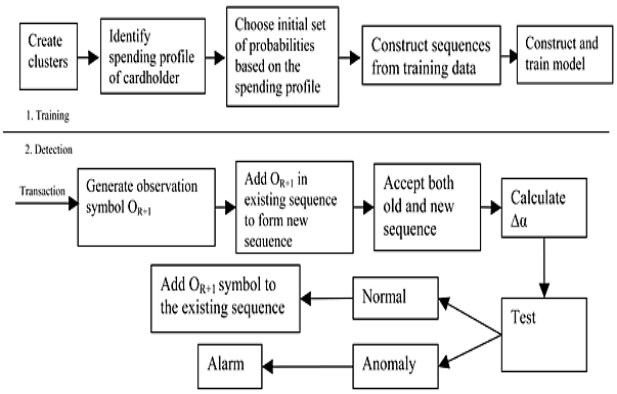

Figure 4 Process flow of Credit Card Fraud

3.3 Genetic algorithms and other algorithms.

Algorithms are often recommended as predictive methods as a means of detecting fraud. One algorithm that has been suggested by Bentley et al. (2000) is based on genetic programming in order to establish logic rules capable of classifying credit card transactions into suspicious and non-suspicious classes. Basically, this method follows the scoring process. In the experiment described in their study, the database was made of 4,000 transactions with 62 fields. As for the similarity tree, training and testing samples were employed. Different types of rules were tested with the different fields. The best rule is the one with the highest predictability. Their method has proven results for real home insurance data

and could be one efficient method against credit card fraud. Chan et al. (1999) also developed an algorithm to predict suspect behavior. The originality of their research is that the model is evaluated and rated by a cost model, whereas other studies use evaluation based on their prediction rate/the true positive rate and the error rate/the false negative rate. Wheeler & Aitken (2000) developed the idea of combining algorithms to maximize the power of prediction. They conclude from their investigation that neighborhood-based and probabilistic algorithms have been shown to be appropriate techniques for classification, and may be further enhanced using additional diagnostic algorithms for decision-making in borderlines cases, and for calculating confidence and relative risk measures.

3.4 Outlier Detection

An outlier is an observation that deviates so much from other observations as to arouse suspicion that it was generated by a different mechanism. Unsupervised learning approach is employed to this model.

Usually, the result of unsupervised learning is a new explanation or representation of the observation data, which will then lead to improved future responses or decisions. Unsupervised methods do not need the prior knowledge of fraudulent and non-fraudulent transactions in historical database, but instead detect changes in behavior or unusual transactions.

These methods model a baseline distribution that represents normal behavior and then detect observations that show greatest departure from this norm. Outliers are a basic form of non-standard observation that can be used for fraud detection. In supervised methods, models are trained to discriminate between fraudulent and non-fraudulent behavior so that new observations can be assigned to classes. Supervised methods require accurate identification of fraudulent transactions in historical databases and can only be used to detect frauds of a type that have previously occurred.

An advantage of using unsupervised methods over supervised methods is that previously undiscovered types of fraud may be detected. Supervised methods are only trained to discriminate between legitimate transactions and previously Known fraud.

Proposed System

4.1 Analysis

Now day's internet becomes most popular mode of payment for online transaction. With the developments in the Information Technology and improvements in the communication channels, fraud is spreading all over the world with results of huge financial losses. Therefore we need security for any transaction. In this system provide security when fraudulent user processing.

The existing system reduces fraud of card holder's spending behavior consideration like low spending behavior, medium spending behavior, high spending behavior, analyze these behavior and detect fraud. But this proposed system not analyze the past behavior or any past transaction it depends only current processing transaction.

4.1.1 Problem Definition

Reducing fraud is main objective of this system. There are many existing systems available for detect or reduces fraud. But this existing system occurred some problem and limitation. Hidden Markov Model based system detects the fraud only after some transaction so it is not secured for initial some transaction. Behavior based fraud detection model means that the data use in the model are form the transactional behavior of cardholder directly or derived from them. So, the proposed system needs to improve detection technique to effectively reduces fraud when current transaction processing.

For performing our proposed system, that is for reducing fraud in electronic payment gateway. So we proposed to develop reducing fraud for cloned payment gateway and secured customer data in bank service. For this purpose used secret code encryption technique. The detailed mechanism and requirement study by identifying challenges is given below.

- **Clone Payment Gateway Detection:**

There is need to establish trust around the environment in which e-commerce transactions is operating to attract people to explore the medium for their transaction. This is due to factors such as distance between customers and merchants, identifying genuine customers and merchants, protection of customer's privacy and financial details, protection of transaction process to prevent hijacking, and the like. Some online activities could be for positive motives or for negative motives. Thus, there is need for clear distinction between these two motives in other to ascertain trust in e-commerce environment. Different types of models have being designed to enhance

customer and merchant trust from cloning of website or payment page to ensuring the authenticity of the credit card used

- **Security Information:**

In the internal fraud employee or owner access customer's detail. The steals the customer's personal information to commit crime or pass on the information about cardholder to fraudster for money. To overcome these fraud we required security of users information from any unauthorized users.

In Security information generate the information detail of customer send on email and its store's in database. These information contain in privacy and stored in encrypted format so unauthorised user cannot access this database for any transaction.

4.2 System Design

4.2.1 Basic Idea

Internet fraud is to give out fraud information to potential victims for execution of certain kind of fraudulent trading or fraud action aimed at the financial and the related institutions, by means of one or more online services, including chat rooms, E-mail and BBS, etc. Online bank fraud is an illegal way of stealing money from different bank accounts by using internet technique which mainly refers to the two kinds of fraudulent methods website cloning and internal fraud.

Cloning is the process of replication or alteration of a block of codes. Dedicated hackers and criminals always seek new ways to commit fraud. Two of such ways are webpage cloning and use of fake virtual stores. When a cloned credit card /webpage is properly done, it is difficult to detect.

The security of e-commerce is a continuing process that requires the acceptance of strong security policies and the use of proven security software. Thus the existing system use of CMRR component will add to the existing knowledgebase of Information technology. Furthermore, the huge problem of credit card fraud is being mitigated but a more severe problem is credit card cloning and web page cloning. Thus, a CMRR is shown and proven to identify cloned payment page in ecommerce transaction and prompt customers not to send credit card details.

For performing our proposed system, that is for reducing fraud in electronic payment gateway. So we proposed to develop reducing fraud for cloned payment gateway and secured customer data in bank service. For this purpose used secret code encryption technique.

3.2.2 System Architecture

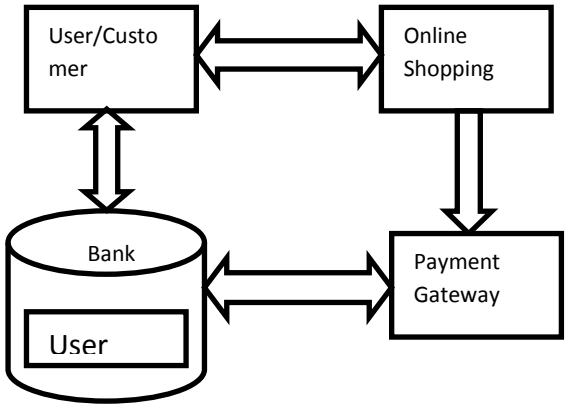

Fig. 5 Architecture of for Reduce Fraud in Electronic Payment Gateway

Fig. 5 shows the architecture of the proposed system, in this system user can be login particular site to purchase goods and services, and then choose item. Then next step after purchasing go to payment gateway, by this transfer of information payment gateway and bank service which is having user information of particular user.

In these proposed system all user information stored in encrypted format for secured from any unauthorized user. Main purpose of the proposed system generates secret code for the payment gateway without entering correct secret code we cannot proceed transactions.

Modules of Proposed System:

Proposed system can be divided into the following modules,

1. Online Shopping:

It comprises with many steps, first is the user registration, second is login, next is shopping and view cart. After the registration of any user login into site to purchase goods or services, then choose an item and next

step is go to view cart options, in these option display all items which is purchased by the user with their price and quantity. In the view cart page having one option i.e. edit cart for editing the quantity of the any items.

2. Bank Service:

Bank plays an important role as an intermediary, go between, in the financial system for customer. Banks are largely responsible for the payment system. In bank service store all information regarding credit card details, debit card details etc. this information useful for payment gateway.

Also this information of user send their email-id for any transaction. This information stored in encrypted format for security or not accessing for unauthorized user.

3. Payment Gateway:

A payment gateway facilitates a payment transaction by the transfer of information between a payment portal (such as a website, mobile phone) and the front end processor or acquiring bank.

Payment Gateway is the last module of the proposed system before go to these option generate one secret code for detecting authorized payment gateway, when we enter correct secret code then transaction successful.

4. RESULT ANALYSIS

Figure shows result analysis graph of the proposed system with different existing system such as CMRR (Centralized Merchant Registration Retrieval) and Finger Printing Method using different parameter i.e. Detection Rate(Precision) and Accuracy.

Sr.No.	Technique	Accuracy	Detection Rate
1.	CMRR(Centralized Merchant Registration Retrieval)	85%	86%
2.	Finger Printing Method	90%	92%
3.	Proposed System using Secret Code	96%	98%

Table 4.1 Graph Details in Tabulation Format

The Internet potential for electronic commerce was expected to boom with the spread of the Internet but, the lack of consumer confidence in electronic payments as regards security of payment mechanisms explained the slow growth of online purchase. Thus, in this system, a centralized merchant registration retrieval (CMRR) component of e-commerce model is used to serve as an advisory tool that identify cloned payment page in e-commerce transaction.

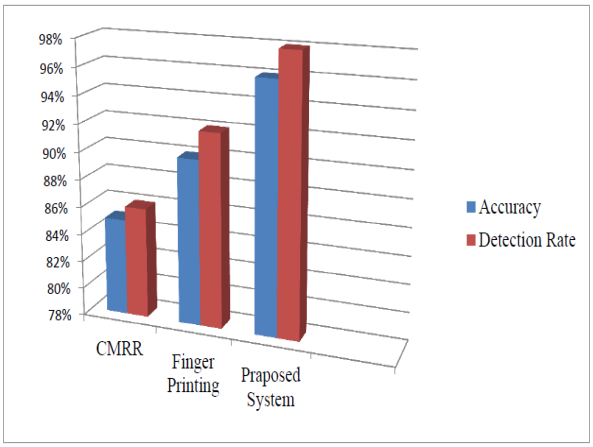

Fig. 4.1 Result Analysis Graph

An online evaluation of the use of CMRR in identifying cloned payment page and acting as an advisory to customer were carried out through the use of questionnaire. Data analysis of generated questionnaire showed that CMRR can enhance customer's confidence and trust in the purchase of online goods and services via identifying cloned payment page[12].

The evaluation of the use of CMRR component in identifying cloned payment page in e-commerce transaction was carried out using SPSS to analyze administered questionnaires. It was observed that CMRR has the capability to identify cloned payment page by comparing the URL of the payment page at the time of customer check out with the URL address of the merchant entered during local merchant registration. Thus, the CMRR sends advisory message to the customer and a transaction log to the retailer alerting both parties of URL mismatch. Therefore, the CMRR ensures that the customer's account details are not sent to fraudulent payment page. This is another attribute of CMRR that makes the component distinctive and essential in e-commerce model.

Duplicate and near-duplicate web pages are the chief concerns for web search engines. In reality, they incur enormous space to store the indexes, ultimately slowing

down and increasing the cost of serving results. A variety of techniques have been developed to identify pairs of web pages that are "similar" to each other. The problem of finding near-duplicate web pages has been a subject of research in the database and web-search communities for some years. In order to identify the near duplicate web pages, we make use of sentence level features along with fingerprinting method.

When a large number of web documents are in consideration for the detection of web pages, then at first, we use K-mode clustering and subsequently sentence feature and fingerprint comparison is used. Using these steps, we exactly identify the near duplicate web pages in an efficient manner. The experimentation is carried out on the web page collections and the results ensured the efficiency of the proposed approach in detecting the near duplicate web pages [15].

Duplicate documents are frequently found in huge databases of digital documents such as the government declassification effort or in digital libraries. The occurrence of near duplicates increase the space required to store the index, decreases serving results, and irritate the users. Capable duplicate document detection is important not only to allow querying for similar documents, but also to filter out unnecessary information in the huge document databases. The removal of the near duplicate pages provides reduced storage costs and improved quality of search indexes in addition to considerable bandwidth management. In the proposed approach, we are using sentence level extraction and simhash algorithm to detect near duplicates. Our proposed approach reduces the storage space greatly and allows quicker comparison and search.

Proposed system using secret code, in this used symmetric encryption technique for security purpose. There is no need to any hardware and past transaction history for reducing or detecting fraud. Table 4.1 shows tabulation format for result analysis graph. The proposed system is better than the existing system of cloned website detection because there detection rate and precision value is high. This system detect or reducing at a time two fraud technique of the electronic payment gateway that is Internal Fraud and Site Cloning.

5. CONCLUSION

In recent times credit cards becomes the most popular means of payment and if credit card transactions increase, so too do frauds. Credit card fraud has become more and more widespread in recent years. In this paper the problem of fraud in electronic payment systems is addressed. Every time user requests a transaction from their bank, the merchant server must be verified to eliminate any chance of fraud. The fraudster may create a fake merchant server that asks the user for their banking credentials. There have been many cases of users falling for a fraudster's web application and entering their credentials.

Security is a major concern of web users, particularly when using banking applications. usage of credit cards or online payment become more and more common in every field of the daily life So we need security for any transaction from fraudulent user. In this proposed system reduce the fraud in online credit-card transactions in real time by generating Secret Code to prevent fraud.

REFERENCES

[1] Vishal Jain, Gagandeep Singh Narula & Mayank Singh, "Implementation of DataMining in Online Shopping System Using TANAGRA Tool", International Journal of Computer Science and Engineering (IJCSE), Vol 2, Issue 1, 47-58, Feb 2013.
[2] Shaffy Goyal, Namisha Modi, "A Review on Various Classification Algorithms for Online Shopping Data", International Journal of Computer Application, Vol 6, March-April 2016
[3] Bharati M. Ramageri, Dr.B. L. Desai, "Role of Data Mining in Retail Sector",International Journal on Computer Science and Engineering, Vol. 5, Jan 2013
[4] V. Dheepa, R. Dhanapal, "Behavior Based Credit Card Fraud Detection using Support Vector Machines", ICTACT Journal on Soft Computing, Vol 2, July 2012
[5] Mr. P. Matheswaran, Mrs. E. Siva Sankari, Mr. P. Rajesh, "Fraud Detection in Credit Card Using Data Mining Techniques", International Journal for Research in Science Engineering and Technology, Vol 2, 11-18, Feb 2015
[6] Priya Ravindra Shimpi, Prof. Vijayalaxmi Kadroli, "Survey on Credit Card Fraud Detection Techniques", International Journal of Engineering and Computer Science", Vol-4, Nov 2015, Page No. 15010-15015.
[7] Deepak Pawar, Swapnil Rabse, Sameer Paradkar, Naina Kaushik, "Detection of Fraud In Online Credit Card Transactions", International Journal of Technical Research And Application, Vol 4, Issue, March-April-2016, PP 321-323
[8] V. Bhusari, S. Patil, "Study of Hidden Markov Model in Credit Card Fraudulent Detection", International Journal of Computer Application, Vol-2, April 2011
[9] Ashlesha Bhingarde, Avnish Bangar, Krutika Gupta, Snigdha Karambe, "Credit Card Fraud Detection using Hidden Markov Model", International Journal of Advanced Research in Computer and Communication Engineering, Vol 4, March 2015

[10] Twinkle Patel, Ms. Ompriya Kale, "A Secured Approach to Credit Card FraudDetection using Hidden Markov Model", International Journal of Advanced Research In Computer Engineering & Technology (IJARCET), Vol 3, May 2014

[11] 1V.Priyadharshini, G.Adiline Macriga, "An Efficient Data Mining for Credit Card Fraud Detection using Finger Print Recognition ", International Journal of Advanced Computer Research, Vol-2, December-2012

[12] S.S. Bhamare, "Near Duplicate Web Page Detection for Efficient Web Crawling: A Survey", International Journal of Advanced Scientific Research and Management, Volume 4 Issue 5, May 2019

[13] J. Prasanna Kumar and P. Govindarajulu, "Near-Duplicate Web Page Detection: An Efficient Approach Using Clustering, Sentence Feature and Fingerprinting", International Journal of Computational Intelligence Systems, Vol 6, No. 1 January 2013

[14] Yashvi Jain, Namrata Tiwari, Shripriya Dubey, Sarika Jain, "A Comparative Analysis of Various Credit Card Fraud Detection Techniques", International Journal of Recent Technology and Engineering(IJRTE), Volume -7 Issue-5S2, January 2019 .

[15] T.S.Vigneshwaran, M.Yokesh, "A study on causes and prevention of fraud in banking industry", International Journal of Pure and Applied Mathematics, Volume 120 No. 5 2018.

[16] A. Aruna, Devansh Sharma, Manikanta Elluru, Subha Sarkar, "Securing Online Transactions with Cryptography And Secured Authentication Methods", International Journal of Recent Technology and Engineering (IJRTE), Volume-8, Issue-1, May 2019.