Avoiding Cybercrime Pandemic in Cashless Society using HMM

Abdulrahman Abdulganiyu
Department of
Math's/Computer Science
Ibrahim Badamasi Babangida
University
Lapai, Niger State, Nigeria

Aliyu Y. Badeggi
Department of
Math's/Computer Science
Ibrahim Badamasi Babangida
University
Lapai, Niger State, Nigeria

Usman M. Gana
Department of
Math's/Computer Science
Ibrahim Badamasi Babangida
University
Lapai, Niger State, Nigeria

ABSTRACT

Internet fraudulent activities are increasing dramatically in the availability of technology resources like telecommunication networks, mobile communications, and E-commerce. Fraud is a major problem in electronic payment systems. With this increased availability has come a new form of criminal activity that takes advantage of electronic payment system, namely cybercrime, mobile-crime, SIM-crime and computer fraud. Currently, these new forms of crime are burgeoning and pose a new and challenges to researchers,merchant, customers and the law enforcement agencies. In this paper we discus types of electronic payment, we propose an effective method of detecting and preventing unauthorized cybercriminals from gaining access to several devices and technologies used in electronics payment by using Hidden Markov Model, also we take care not to prevent genuine transaction not to be rejected.

Keywords

SIM-crime, E-payment,E-cash,Cyber criminals, Enabling technologies, Cashless society.

1. INTRODUCTION

Ever since Diners Club introduced the first general-purpose charge card in the early 1950s, pundits have been predicting the emergence of a “cashless society” [2].About sixty one years later the Central Bank of Nigeria began a campaign in a new policy on cash-based transactions which stipulates a ‘cash handling charge’ on daily cash withdrawals or cash deposits that exceed certain amount.

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. It is easy, cheap and fast to transfer data, but the main challenge is security [7,16]. The economy of most nations in the world is accessible through the aid of electronic via the internet, machine (POS) and mobile communication network (GSM). Since the Electronic market is opened to everybody it also includes conversation with legalize vendor and unknown criminals. False pretence, finds fertile opportunity in this situation. Some perpetrators of this crime usually referred to in Nigeria as “yahoo boys” are taking advantage of e-payment system to defraud unsuspected victims who are mostly merchants and customers who is purchasing product through the online system, job seekers and sometimes people who got sms alert to update or trying to update their financial profile online without knowing the truth site of their banks. These criminals fraudulently represent themselves involving in scholarships for students schooling abroad, they represent themselves as having products to sell or that they are involved in a loan scheme project. They may even pose to have financial institution where money can be loaned out to prospective businessmen. In this regard, so many persons will be duped. Merchants who take orders from merchandise on credit could also be facing lost from cybercrime [12].

Electronic payment systems may be classified into two groups: “account-based” or credit-debit systems and “token-based” or electronic currency systems. Both groups have important characteristics such as trust, security, reliability, ease of use, efficiency, flexibility, convertibility, interoperability, etc. However, in this paper the focus is on the knowledge of devices and the technology use in electronic payment system with the security of the system and possible prevention and detection of fraud.

2. RELATED WORK

In “Credit Card Fraud Detection Using HMM” paper, they have proposed an application of HMM in credit card fraud detection. The different steps in credit card transaction processing are represented as the underlying stochastic process of an HMM. They have used the ranges of transaction amount as the observation symbols, whereas the types of item have been considered to be states of the HMM. They have suggested a method for finding the spending profile of cardholders, as well as application of this knowledge in deciding the value of observation symbols and initial estimate of the model parameters. It has also been explained how the HMM can detect whether an incoming transaction is fraudulent or not. Experimental results show the performance and effectiveness of our system and demonstrate the usefulness of learning the spending profile of the cardholders. Comparative studies reveal that the Accuracy of the system is close to 80 percent over a wide variation in the input data. The system is also scalable for handling large volumes of transactions [2].

In “credit card fraud detection with a neural network” paper, using data from a credit card issuer, a neural network based fraud detection system was trained on a large sample of labeled credit card account transactions and tested on a holdout data set that consisted of all account activity over a subsequent two-month period of time. The neural network was trained on examples of fraud due to lost cards, stolen cards, application fraud, counterfeit fraud, mail-order fraud and NRI (non-received issue) fraud. The network detected significantly more fraud accounts (an order of magnitude more) with significantly fewer false positives (reduced by a factor of 20*)* over rule based fraud detection procedures. They discuss the performance of the network on this data set in terms of detection accuracy and earliness of fraud detection. The system has been installed on an IBM 3090 at Mellon Bank and is currently in use for fraud detection on that bank's cmlit card portfolio [4].

In "Offline Internet Banking Fraud Detection" paper .Object of this paper is to demonstrate one successful fraud detection model which is established in Greece. Apart from the offline internet banking fraud detection system itself, which is described briefly, there scope is to present its contribution in fast and reliable detection of any "strange" transaction including fraudulent ones[14].

In "Security Analysis for Internet Banking Models" paper they stated that Internet banking fraud can be performed internally by genuine staff or externally by customers or suppliers. This paper presents a security analysis of the proposed Internet banking model compared with that of the current existing models used in fraudulent Internet payments detection and prevention. Several modern models in preventing and detecting fraud are evolving and being applied to many banking systems. However, they have no effective detection mechanism to identify legitimate users and trace their unlawful activities. Also they are not secure enough to prevent fraudulent users from performing fraudulent transactions over the Internet. The proposed model facilitates Internet banking Fraud Detection and Prevention (FDP) by applying two new secure mechanisms, Dynamic Key Generation (DKG) and Group Key (GK) [6].

In "Study on Fraud Risk Prevention of Online Banks" paper .The paper is aimed, in the first hand, at giving a discussion on the fraud risks of online banking, introducing the current application situation of information sharing mechanism in respect of internet fraud outside China as well as the development of such concept in China. Then, a system is designed for sharing internet fraud information. The paper finally proposing that all the online banks should put more joint efforts in perfecting this mechanism for sake of international co-operation[7].

In "Fraudulent Internet Banking Payments Prevention using Dynamic Key" In this paper, they have proposed an efficient new scheme which can prevent fraud by applying different security algorithms, generating and updating limited-use secret keys. It uses advanced authentication technologies and is well adapted to any possible future technology. Moreover, it does not rely on fixed values where hacking one secret will not compromise the whole system's security. The generation of each set of keys is based on dynamically generated preference keys. The higher number the transactions performed, the less chance the system has of being compromised. The practical usefulness of the technique has been demonstrated by applying it to Internet banking payment systems. The results show that our technique enhances their security considerably. It has been shown that the proposed technique is secure against key compromise. For future work, we aim to analyze the security of the system that applies the proposed technique. Moreover, we aim to apply the proposed technique to other kinds of internet applications, especially mobile commerce [6].

In the paper "Parallel Granular Neural Networks for Fast Credit Card Fraud Detection". A parallel granular neural network (GNN) is developed to speed up data mining and knowledge discovery process for credit card fraud detection. The entire system is paraUelized on the Silicon Graphics Origin 2000, which is a shared memory multiprocessor system consisting of 24-CPU, 4G main memory, and 200GB hard-drive. In simulations, the parallel fuzzy neural network running on a 24-processor system is trained in parallel using training data sets, and then the trained parallel fuzzy neural network discovers fuzzy rules for future prediction[15].

3. TYPES OF E-PAYMENTS SYSTEM

With the advent of computers and electronic communications a large number of alternative electronic payment options have emerged. Some of the e-payment options are:

A. E-cash

E-cash (also known as e-currency, e-money, electronic cash, electronic currency, digital money, digital cash, digital currency, cyber currency) is a computer generated Internet based system which allows funds to be transferred to third party and items to be purchased by credit card, ATM card or by money order, providing secure online transaction processing. Typically, this involves the use of the internet network and digital stored value systems. Electronic funds transfer (EFT), direct deposit, digital gold currency and virtual currencies are all examples of electronic money.

B. Electronic wallets

E-wallet is highly convenient, easy-to-use, secure e- payment system.E-wallet offers secure, convenient, and portable tool for online shopping. They store personal and financial information such as credit cards, passwords, PINs, and much more. E-wallets allow you to keep track of your billing and shipping information so that it can be entered with one click at participating merchants' sites. E-wallets can also store e-checks,e-cash and your credit-card information for multiple cards.Example of an e-wallet on the market is Microsoft wallet.

C. Smart card

Smart card is about the size of a credit card, made of a plastic with an embedded microprocessor chip that holds important financial and personal information. The microprocessor chip is loaded with the relevant information and periodically recharged. In addition to these pieces of information, systems have been developed to store cash onto the chip. The money on the card is saved in an encrypted form and is protected by a password to ensure the security of the smart card solution. In order to pay via smart card it is necessary to introduce the card into a hardware terminal. The device requires a special key from the issuing bank to start a money transfer in either direction. Smart cards can be disposable or rechargeable. A popular example of a disposable smart card is the one issued by telephone companies which can be used in phone booths. After using the pre-specified amount, the card can be discarded.

Smart cards have been extensively used in the telecommunications industry for years. Smart-card technology can be used to hold information on health care, transportation, identification, retail, loyalty programs and banking, to name a few. Smart cards enable information for different purposes.

D. Credit card

Credit card is the modern system of payment, which has to a large extent replaced the traditional forms of payment by cash, cheques, etc. Visa and master cards are association of banks, which deal in credit cards. Bank credit cards are a type of consumer loans, revolving in nature, i.e., automatically renewing itself, within specific limits. The utility of credit card is derived from its ability to buy goods and services without actually paying for them immediately. Credit cards were introduced much earlier than debit cards. There are two types of credit cards on the market today:

(a) **Credit cards issued by credit card companies**(e.g., MasterCard, Visa) and major banks (e.g. Is First bank, GTB Bank, UBA, etc.) Credit cards are issued based on the customer's income level, credit history, and total wealth. The customer uses these cards to buy goods and services or get cash from the participating financial institutions. The customer is supposed to pay his or her debts during the payment period; otherwise interest will accumulate. Two limitations of credit cards are their unsuitability for very small or very large payments. It is not cost-justified to use a credit card for small payments. Also, due to security issues, these cards have a limit and cannot be used for excessively large transactions.

(b) **Credit cards issued by department stores**(e.gBoyner), oil companies (e.g. Shell) businesses extremely benefit from these company cards and they are cheaper to operate. They are widely issued to and used by a broad range of customers. Businesses offer incentives to attract customers to open an account and get one of these cards.

E. Debit card

The difference between credit cards and debit cards is that in order to pay with adebit card you need to know your personal identification number (PIN) and need ahardware device that is able to read the information that is stored in the magneticstrip on the back [3].Debit cards task similar to checks in that the charges will be taken from thecustomer's checking account. The benefit for the customer is the easiness of useand convenience. These cards also keep the customer under his or her budgetbecause they do not allow the customer to go beyond his or her resources. Theadvantage to the merchant is the speed at which the merchant collects thesecharges.

F. Mobile payment

Mobile payment(m-payment)ispayment made with the use of mobile device to initiate, authorize and confirm an exchange of financial transaction in return for goods and services. With mobile money, users can create e-wallets on their mobile phones for storing funds. If you activate your bank accountto accept mobile money e-payment solutions, such users will be able to pay with their phone.

Accepting payment with mobile money is similar to POS terminals. After shopping, you provide the shopper with cost of the purchase and your merchant ID, the shopper enters these details on their mobile money interface, enter their PIN to authorize payment and in seconds the value of the purchase will be electronically transferred to your account and you will receive alert for confirmation on your device.

G. E-checks

This facility is the internet version of FEDI systems which have allowed these functions to be performed over VAN'S. The electronics cheques provide internet websites with the ability to perform the following functions, Present the bill to the payer, allow payer to initiate payments of the invoice, provide remittance information and allow the payer to initiate automatic payment authorizations for a pre-specified amount or range of amounts.

4. E-PAYMENT CHANNELS AND ENABLING TECHNOLOGIES

Defined as 'physical points' where a payment transaction is originated or initiated and e-payment can be executed through a variety of channels:

A. Internet based

This is a platform where can be launch payment for goods and services electronically. Internet is an international network that allow browser. The internet helps to look at it as a system with two main components. The first of those components is hardware [7]. That includes everything from the cables that carry terabits of information every second to the computer sitting in front of you. There are other types of hardware that supports the Internet include routers, servers, cell phone towers, satellites, radios, smartphones and other devices. All these devices together create the network of networks. The Internet is a malleable system it changes in little ways as elements join and leave networks around the world. Some of those elements may stay fairly static and make up the backbone of the Internet. Others are more peripheral.

B. Kiosks

Interactive kiosk is a computer terminal featuring specialized hardware and software designed within a public exhibit that provides access to information and applications for communication, e-commerce, entertainment, and education. Early interactive kiosks sometimes resembled telephone booths, but can also be used while sitting on a bench or chair. Interactive kiosks are typically placed in high foot traffic settings such as hotel lobbies or airports. Integration of technology allows kiosks to perform a wide range of functions, evolving into self-service kiosks. For example, kiosks may enable users to enter a public utility bill account number in order to perform an online transaction, or collect cash in exchange for merchandise. Customized components such as coin hoppers, bill acceptors, card readers and thermal printers enable kiosks to meet the owner's specialized needs.

C. Contactless or proximity sensors

Proximity sensor is an electromagnetic field or a beam of electromagnetic radiation (infrared, for instance), and looks for changes in the field or return signal. The object being sensed is often referred to as the proximity sensor's target. Different proximity sensor targets demand different sensors. For example, a capacitive photoelectric sensor might be suitable for a plastic target; an inductive proximity sensor always requires a metal target.The maximum distance that this sensor can detect is defined "nominal range". Some sensors have adjustments of the nominal range or means to report a graduated detection distance.Proximity sensors can have a high reliability and long functional life because of the absence of mechanical parts and lack of physical contact between sensor and the sensed object.

D. Mobile e.g. mobile phones, GSM, PDA

Mobile phone (also known as a cellular phone, cell phone and a hand phone) is a device that can make and receive telephone calls over a radio link whilst moving around a wide geographic area. It does so by connecting to a cellular network provided by a mobile phone operator, allowing access to the public telephone network. By contrast, a cordless telephone is used only within the short range of a single, private base station.In addition to telephony, modern mobile phones also support a wide variety of other services such as text messaging, MMS, email, Internet access, short-range wireless communications (infrared, Bluetooth), business applications, gaming and photography. Mobile phones that offer these and more general computing capabilities are referred to as smartphones.

E. Automated POS payments

A Point of Sale terminal(PoS) terminal is a portable device that enables shoppers pay for goods and services with electronic payment cards like ATM/Debit cards and credit cards. If a merchant installs a PoS terminal for payment, customers will be able to use e-payment cards like InterSwitch Verve, MasterCard, Visa, eTranzact, etc. to pay for goods and services on checkout.The PoS terminal is connected to your bank. After shopping, the shopper presents his e-payment card to your teller, who slots it into the POS terminal or swipes it on the POS terminal depending on the configuration of the terminal. The customer checks the bill and authorizes payment by entering his PIN. If all is well, funds will be electronically transferred from the shoppers account to your merchant account at your bank. With their **e-payment** cards, your customers can spend up to ₦500000 on goods bought from your shop with no need to carry cash. In addition, depending on your PoS terminal, you may also be able to offer money transfer services as well as sell recharge cards as most PoS machines can also print recharge cards for telecommunication companies like GLO, MTN, ETISALAT and AIRTEL

F. Automatic teller machines (ATM)

An automated teller machine (also known as an ATM or Cash Machine), is a computerized device that provides the customers of a financial institution with the ability to perform financial transactions without the need for a human clerk or bank teller.

G. Network, including GPRS and 3G

General Packet Radio Service (GPRS) is a mobile data service available to GSM users. GPRS provides packet-switched data for GSM networks. GPRS enables services such as Wireless Application Protocol (WAP) access, Multimedia Messaging Service (MMS), and for Internet communication services such as email and World Wide Web access in mobile phones.

H. SIMs(Subscriber Identification Module)

The subscriber identity module (SIM) used in GSM mobile phones is a smart card i.e., it is a small chip with processing power (intelligence) and memory. The information in the SIM can be protected using cryptographic algorithms and keys. This makes SIM applications relatively more secure than client applications that reside on the mobile phone. Also, whenever the customer acquires a new handset only the SIM card needs to be moved (Card Technology, 2007) [15]. If the application is placed on the phone, a new handset has to be personalized again.

5. SECURITIES ON E-PAYMENT SYSTEM INFRASTRUCTURE

Security is the biggest issue in the field of e-payment system because without secure payment information exchange and safe electronic financial transactions over e-payment system, no one would trust e-payment transaction [5, 16]. In order to ensurethe integrity and security of each electronic transaction and other e-payment Systemutilize some or all of the following security measures and technologiesdirectly related to e-payment system:

A. Authentication

This is the process of verification of the authenticity of a person and/or atransaction. There are many tools available to confirm the authenticity of auser. For instance, passwords and ID numbers are used to allow a user tolog onto a particular site.

B. Confidentiality

The confidential information must be secured from an unauthorized person, process or device. Customers would have trust on the website of a merchant if the privacy of authorize owners of credit card use on their sites are secured.

C. Public Key Cryptography

Public key cryptography uses two keys, one public and one private, toencrypt and decrypt data, respectively. Cryptography is the process ofprotecting the integrity and accuracy of information by encrypting data intoan unreadable format, called cipher text. Only those who possess a privatekey can decrypt the message into plain text.

D. Digital Signature

Rather than a written signature that can be used by an individual toauthenticate the identity of the sender of a message or of the signer of adocument; a digital signature is an electronic one. E-check technology alsoallows digital signatures to be applied to document blocks, rather than tothe entire document. This lets part of a document to be separated from theoriginal, without compromising the integrity of the digital signature.

A digital signature includes any type of electronic message encrypted with aprivate key that is able to identify the origin of the message. The followingsare some functions of digital signature.

E. Certificate Authorities

Certificate authorities are similar to a notary public, a commonly trustedthird party. In the e-commerce world, certificate authorities are thecorresponding of passport offices in the government that concern digitalcertificates and validate the holder’s identity and authority.

F. Secure Sockets Layer (SSL)

Secure Sockets Layer transmits private documents viathe Internet. SSL uses a cryptographic system thatuses two keys to encrypt data - a public key known toeveryone and a private or secret key known only tothe recipient of the message. It operates between thetransport and the application layers in the networkstack and uses both public and private keycryptography

6. PROBLEM STATEMENT

E-payment is increasingly used in almost every business. Most of our e-payment systems devices and technologies are not fully secure, and reliable.Security is fundamental vulnerabilities inthe existing e-payment system infrastructures, and serious risks thatthese vulnerabilities will be exploited with possibly very severeeffects.

The defiant manner in which hackers operate reflects the weakness of the devices, and technology capacities of the E-payment system. There are manytypes of fraud in electronic payment systems. Fraud can occur in a number of ways including

A. Counterfeit fraud:

This is an activity whereby some criminals have managed to make fake card of legitimate credit cards by copying or “skimming” the data contained in a card’s magnetic stripe. Using this “skimmed” information, criminals manufacture phony or counterfeit cards and use them for fraudulent purposes.

B. Credit card fraud:

Credit card fraud is divided into two types: credit-card (offline) fraud and card-not-present (online) fraud. Offline fraud is committed by using a stolen physical card at storefront or call center. Online fraud is committed via web, phone shopping or cardholder-not-present. In online fraud only the card’s details are needed, and a manual signature and card imprint are not required at the time of purchase.

C. ATM fraud:

These are methods used by criminals to capture data from the magnetic stripe on the back of an ATM card. These devices used are smaller than a deck of cards and are often fastened in close proximity to, or over the top of the ATM’s factory-installed card reader.

D. Phishing:

Phishing is a criminal activity whereby fraudsters attempt to acquire sensitive information, such as credit card numbers, addresses, social security numbers, drivers ’license numbers, usernames and passwords by appearing as a trustworthy organization in an electronic communication. Phishing is typically carried out by email, phone calls or instant messaging, and often directs users to provide the sensitive information at a website monitored by the criminals.

E. Lost or stolen cards:

This is a method use by criminals to validate stolencredit card numbers. The criminals submit the credit card number and the cardholders’personal data on a website that has real-time transaction processing. Typically, smallmonetary purchases are made in order to not attract the attention of a merchant and topreserve the credit limit on the card. Once validated, the card number and related detailswill be sold to or exchanged with other criminals who will use the information to makelarger purchases.

F. Shoulder Surfing:

Shoulder Surfing is the act of direct observation, watching what number that person taps onto the keypad. The criminal usually positions himself in close but not direct proximity to the ATM to covertly watch as the ATM user enters their PIN or in the process of using public internet cafe. Sometimes miniature video cameras that are easily obtained might be installed discretely on the fascia or somewhere close to the PIN Pad,and keyboard to record the PIN entry information.

G. Skimming:

This is done by dishonest employee ofa legitimate merchant, by manually copying down numbers, or using a magnetic stripereader device. There are devices used by criminals to capture the data stored in the magnetic strip of the card. Reading and deciphering the information on the magnetic stripes of the card can be accomplished through the application of small card readers in close proximity to, or on top of, the actual card reader input slot, so it is able to read and record the information stored on the magnetic track of the card. The device is then removed, allowing the downloading of the recorded data. Skimming often takes place in restaurants or bars where the skimmer haspossession of the victim's credit card out of their immediate view

7. FRAUD DETECTION TECHNIQUES

HMM model:

A hidden Markov model (HMM) is a statistical model inwhich a system being modeled is assumed to be a Markovprocess with unobserved state. In our case purchases ismodeled to different state. A HMM can be considered as thebest dynamic Bayesian network. The major difference betweenregular Markov model and Hidden Markov Model is that the stateis visible to the observer in case of regular MarkovModel while state is not directly observablein case of HMM. The statetransition probabilities are the parameters in RegularMarkov Model. Each state has a probability distribution overthe possible output tokens. In our case output tokensare low, medium, high. Therefore the sequence of tokensgenerated by an HMM gives some information about thesequence of states. Even if the model parameters are knownexactly, the model is still 'hidden'. Hidden Markov models areused for their application pattern recognition such as speech,handwriting, gesture recognition, part-of-speech tagging,musical score following, partial discharges andbioinformatics[6,13].A hidden Markov model can be considered a generalizationof a mixture model where the hidden variables (or latentvariables), which control the mixture component to beselected for each observation, are related through a Markovprocess rather than independent of each other[15].

8. THE ARCHITECTURE OF PROPOSED SYSTEM

Architecture of Proposed system consists of following component

A. Authorized Users:

He is the authorized client who is has registered internetbanking account in his bank .He can do onlinepayment.

Unauthorized users:

They are the criminals who are not having Internetbanking account. Who makes use of authorized usersInternet banking account to do Transaction. Hence He isFraudulent User. He obtains the password of ParticularCustomer By doing attacks that are mentioned in 5 above

B. Bank Server:

Bank Sever is responsibleto add customers for internet banking account. All theprocessing of internet banking done are Managed from the server;Change account status (Block to Unblock and vice versa) are done by management of Bank.

Bank Database:

Storesinformation about customers such as (Name,Contact Number, Email id, Account Number).It Storesthe previous Transaction information of Customer made,it records Sequence of Transaction and it is model throughHidden Markov Model. For about 10th Transaction arerecorded sequence and from 11th Transaction HMM algorithmis running to find Fraudulent Transaction.

C. Data Gatherer (prev. E-payment history):

Data gatherer are temporally stored till data gatherer obtains it completely and then it is erased from the local memory of the mobile. This exchange of data is done securely with the help of some encryption techniques applied before the exchange of data. This is done to protect the privacy of the customer. In this way the patterns will be detected while keeping in the mind the privacy of the customer.

The authentication checker collects the data from the data gatherer or directly from user client server. It collects the data based on the policy provided by the authentication decider. When a payment request comes to authentication decider it forward the request to the authentication checker and the details associated with it authentication checker then send the query to the user client server and/or data gatherer.

D. E-payment service provider:

The provider offers online services for accepting electronic payments by a variety of payment methods including credit card, bank-based payments such as direct debit, bank transfer, and real-time bank transfer based on online banking.It records the Customer Transaction Pattern Using HMM algorithm. This is used to detect pattern and to find Fraudulent Transaction. In case of Violation Bank server sends the synchronize password to the email which is registered in the Bank Database for Particular Customer to reset his account.

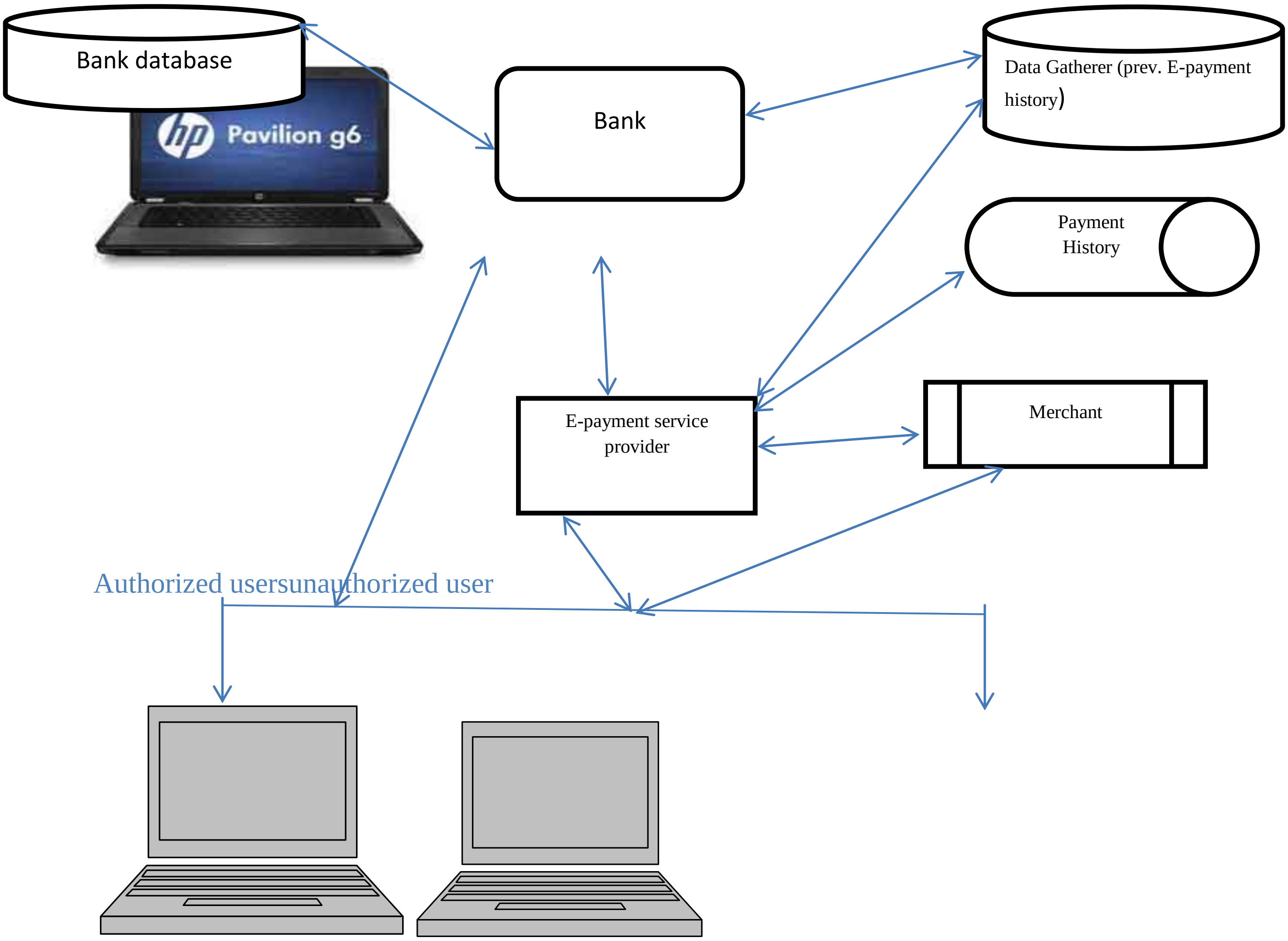
Bank database
Pavilion g6
Bank
Data Gatherer (prev. E-payment history)
Payment History
E-payment service provider
Merchant
Authorized usersunauthorized user

Fig 1: Architecture of Proposed System.

9. Use Case Diagram

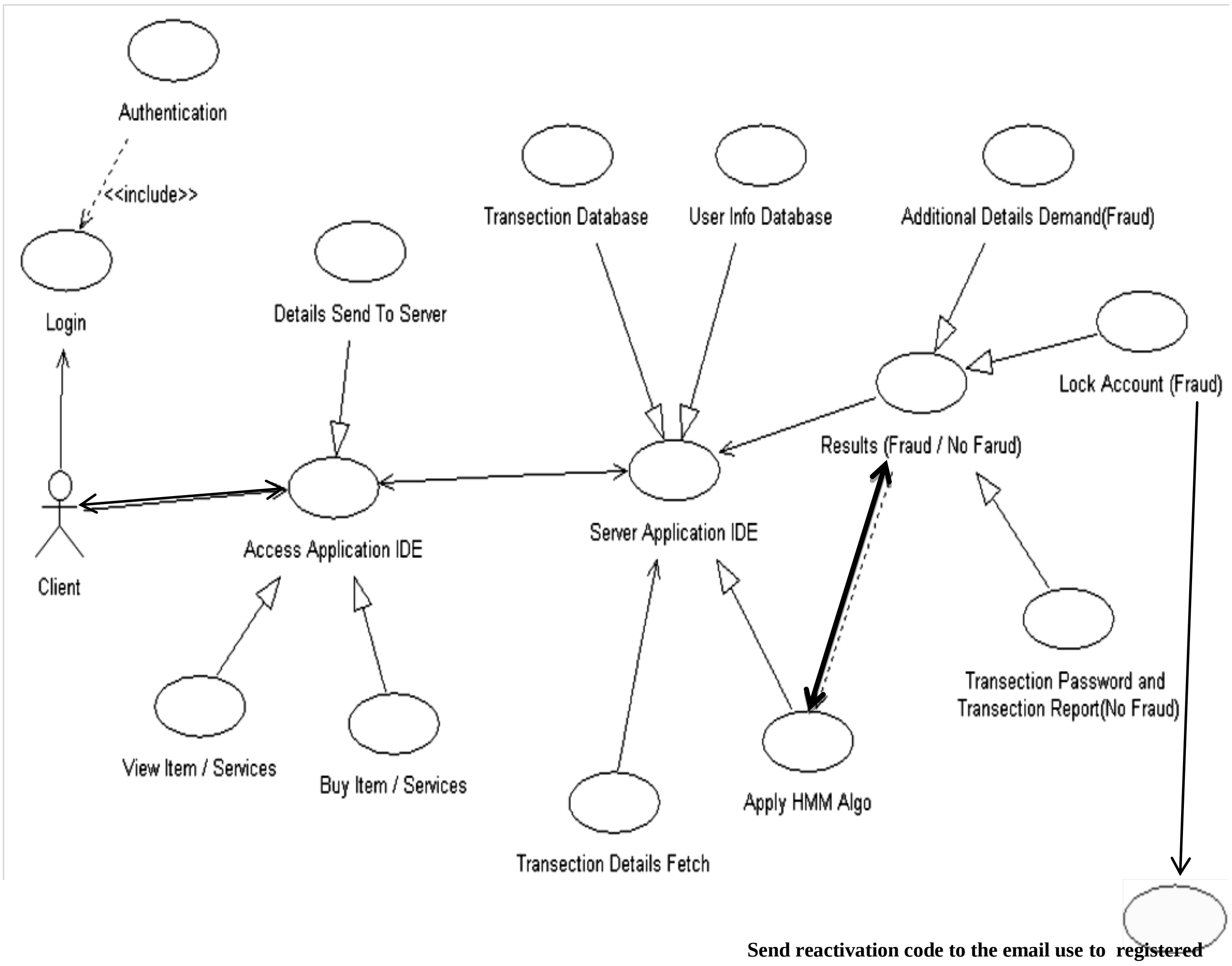

Fig. 2: Case Diagram of Proposed System

10. CONCLUSION

The propose an effective method of detecting and preventing unauthorized cybercriminals from gaining access to several devices and technologies used in electronics payment by using Hidden Markov Model, also we take care not to prevent genuine transaction not to be rejected. In electronic payment Frauddetection system will run at the E-payment service provider server and it's Functionto detect and reject fraud an online payment transaction. The proposed Fraud Detection System is also scalable for handling vast volumes of transactions data processing. The HMM based credit card fraud detection system is not having complex process to perform fraud check like the existing system. Proposed Fraud detection system gives genuine and fast result than existing system. The Hidden Markov Model makes the processing of detection very easy and tries to remove the complexity.Prediction system for Fraud detection and prevention carried out using Hidden MarkovModel which uses Baum-welch algorithm. Initially Afterdetecting a fraud it sends a Onetime password to a browser on the client side. We model the sequence of operations inonline payment transaction processing using a Hidden MarkovModel (HMM) and show how it can be used for the detectionand prevention of frauds. An HMM is initially trained with the normalbehavior of an account holder. If an incoming online bankingtransaction is not accepted by the trained HMM withsufficiently high probability, it is considered to be fraudulent.At the same time, we ensure that genuine transactions are notrejected.

11. REFERENCES

[1] A.J. Graaff A.P. Engelbrecht "The Artificial Immune System for Fraud Detection in the Telecommunications Environment"; (2011). (1-4)

[2] AbhinavSrivastava, AmlanKundu, ShamikSural, Arun K. Majumdar. "Credit Card Fraud Detection using Hidden Markov Model". IEEE Transactions on dependable and secure computing,Volume 5; (2008) (37-48).

[3] AihuaShen, Rencheng Tong, Yaochen Deng "Application of Classification Models on Credit Card Fraud Detection". (2007).

[4] Anshul Singh, Devesh Narayan "A Survey on Hidden Markov Model for Credit Card Fraud Detection".

International Journal of Engineering and Advanced Technology (IJEAT), (2012). Volume-1, Issue-3; (49-52).

[5] B.SanjayaGandhi ,R.LaluNaik, S.Gopi Krishna, K.lakshminadh "Markova Scheme for Credit Card Fraud Detection". International Conference on Advanced Computing, Communication and Networks; (2011). (144-147).

[6] Osama Dandash,Phu Dung Le and BalaSrinivasan "Security Analysis for Internet Banking Models". Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing IEEE DOI 10.1109/SNPD.2007.

[7] Qinghua Zhang "Study on Fraud Risk Prevention of Online Banks". 2009 International Conference on Networks Security, Wireless Communications and Trusted Computing.

[8] Bidgoli, B. M., Kashy, D., Kortemeyer, G. & Punch, W. F "Predicting student performance: An Application of data mining methods with the educational web-based system LON-CAPA". In Proceedings of ASEE/IEEE frontiers in education conference. . (2003).

[9] Bolton, R. J., Hand, D. J (2002). "Statistical fraud detection: A review". Statistical Science (1994).28(3); (235—255).

[10] Clifton Phua, Vincent Lee, Kate Smith, and Ross Gayler "A comprehensive survey of data mining-based fraud detection research". In Artificial Intelligence Review. (2005).

[11] Cortes, C. &Vapnik, V "Support vector networks, Machine Learning". . (1995). Vol. 20; (273–297).

[12] De Castro, L., &Timmis, J "Artificial immune systems: a new computational approach". London, UK: Springer-Verlag. . (2002).

[13] Dipti D. Patil, V.M. Wadhai, J.A. Gokhale "Evaluation of Decision Tree Pruning Algorithms for Complexity and Classification Accuracy". International Journal of Computer Applications, (2010). Volume 11– No.2; (23-30).

[14] MasoumehZareapoor,Seeja.K.R,M.Afshar.Alam"Analysis of Credit Card Fraud Detection Techniques: based on Certain Design Criteria". International Journal of Computer Applications, August 2012. Volume 52– No.3 (0975 – 8887).

[15] Sunil S Mhamane, L.M.R.J Lobo" Use of Hidden Markov Model as Internet Banking Fraud Detection". *International Journal of Computer Applications May 2012. Volume 45– No.21, (0975 – 8887).*

[16] *SandeepPratap Singh, Shiv Shankar P.Shukla,NitinRakesh and VipinTyagi"PROBLEM REDUCTION IN ONLINE PAYMENT SYSTEM USING HYBRID MODEL".* International Journal of Managing Information Technology (IJMIT) Vol.3, No.3, August 2011.

[17] Adnan M. Al-Khatib"Electronic Payment Fraud Detection Techniques". *World of Computer Science and Information Technology Journal (WCSIT) 2012, ISSN: 2221-0741 Vol. 2, No. 4, 137-141.*

[18] *DEJAN SIMIC"REDUCING FRAUD IN ELECTRONIC PAYMENT SYSTEMS". The 7th Balkan Conference on Operational Research, May 2005, Romania.*