ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 10, Issue 1, January 2023

# Development of Secured E-Payment System Using Support Vector Machine (SVM) and Hidden Markov Model (HMM)

**C.M Igbe, A .O Agbakwuru (PhD), Madu Fortunatus U, Oladimeji Biodun S. (PhD) ,Madu Loyce Kelechi**

Professor, Department of Computer Science, Imo State University, Owerri, Nigeria
Department of Computer Science, Imo State University, Owerri, Nigeria
Department of Computer Science, Federal Polytechnic Nekede, Owerri, Nigeria
Department of Computer Science, Federal Polytechnic Nekede, Owerri, Nigeria
Department of Computer Science, Federal Polytechnic Nekede, Owerri, Nigeria

**ABSTRACT**: This paper demonstrated the concept and use of a high-level model for electronic-payment application software with the integration of Support Vector Machine (SVM) and Hidden Markov Model (HMM) as payment security gateway. The motivation of this work is as a result of several e-payment frauds associated with most Nigerian financial sector or platform. This paper identifies various e-payment frauds in Nigeria financials sector as reported by Financial Institutions Training Centre (FITC) , and also discusses the challenges of the current system for e-payment and develop a model to detects, terminate fraudulent transactions and also control genuine transaction done under duress. One of the objectives of this work is to create a database of customers with model that studies the spending behavior of cardholder, verifies transactions credibility and terminates fraudulent transactions, and most importantly control possible fraudulent transactions done under duress. The methodology used is structured systems analysis and design methodology (SSADM) and Object-oriented analysis and design (OOAD). The web browser required includes Mozilla Firefox. MySQL and SQL is used for creation of database while jQuery and HTML/CSS, PHP, JavaScript supports front end development. The paper however, recommends that Central Bank of Nigeria (CBN) should review this model with all financial institutions for adoption and modification of the current system for an enhanced secured e-payment system.

**KEYWORDS: E-payment, Support Vector Machine (SVM) and Hidden Markov Model (HMM)**

## 1. INTRODUCTION

An e-payment system is a way of making transactions or paying for goods and services through an electronic medium, without the use of checks or cash. It is also called an electronic payment system or online payment system [10]. An e-commerce payment system (or an electronic payment system) facilitates the acceptance of electronic payment for online transactions [7]. They have become increasingly popular due to the widespread use of the internet-based transactions, buying, selling and banking. Despite the widespread use of e-payment system, so many countries such as Nigeria have some problems to overcome in regard to e-payment security. E-commerce **fraud** is seen as a type of false, illegal, or illegitimate commercial transaction conducted through the internet. The fraudster typically impersonates a legitimate user, making purchases without valid authorization to do so, and is growing on daily bases. When a merchant chooses a payment system which is not highly secure; there is a risk of sensitive data breach which may cause identity theft. A weak payment system may severely drag on the stability and developmental capacity of a national economy. Such failures can result in inefficient use of financial resources, inequitable risk-sharing among agents, actual losses for participants, and loss of confidence in the financial system [12].

## II. REPORT ON FRAUDS AND FORGERIES IN NIGERIAN BANKS

According to Financial Institutions Training Centre (FITC) report on frauds and forgeries in Nigerian banks fourth quarter, 2021. FITC received sixty-four (64) returns on cases of fraud and forgery from twenty-two (22) deposit money

institutions in the fourth quarter of 2021.Twenty-one (21) returns were received in October 2021, Twenty-one (21) returns were received in November 2021, and another Twenty-two (22) returns were received in December 2021.
Financial Institutions Training Centre (FITC) Nigeria was established in 1981 as a not for profit special purpose professional services organization that is limited by guarantee of its members, who are also members of Nigerian Bankers' Committee, as comprised of the Central Bank of Nigeria, the Nigeria Deposit Insurance Corporation, all licensed Banks and Discount Houses in Nigeria.
According to an assessment of these returns, a total of twenty-six thousand, five hundred and sixty-six (26,566) incidents of Frauds and Forgeries were recorded in the fourth quarter of 2021, compared to twenty thousand, one hundred and ninety-five (20,195) recorded cases in the third quarter of 2021, representing a 31.55 percent increase between the periods. Of the types of fraud observed during the periods, computer/web fraud, mobile banking fraud, and ATM withdrawals fraud had the highest occurrences. According to a magnitude-based ranking of fraud categories, fraudulent withdrawals placed top at N2.19 billion (39.80 percent), followed by Computer/Web Fraud at 1.02 billion (18.47 percent). This was followed by ATM Withdrawal fraud and mobile fraud, with N807.2 million (14.63 percent) and N603.2 million (10.93 percent), respectively. During the fourth quarter of 2021, fraudulent activities were carried out using a range of channels, including ATMs, Web and Mobile Banking Platforms, Bank branches, and POS (Point of Sale) terminals. Cards and cash had the highest frequency for instruments used to carry out fraudulent activities in Q4 2021.

### Statement of the Problem

1. The current system lacks capacity to study the spending behavior of card holder.
2. Lack capacity to handle genuine transaction done under duress.
3. Lack capacity to move 80 per cent of current balance to suspense account via input of alternative password.
4. Poorly generated personal identification number (PIN)
5. Lacks capacity to swap password.

### Objectives of the Study

1. To create awareness about various frauds of electronic payments.
2. To make electronic payments safe and secure using support vector machine and Hidden Markov Model as the security architecture.
3. To identify a possible fraudulent transaction through spending behavior of card holder and terminate transactions if confirmed fraudulent.
4. To identify and handle genuine transaction done under duress.
5. To develop relational database management system for customers.

## III. LITERATURE REVIEW

The existence value of e-commerce is to allow consumers to shop online and pay online through the Internet, [11]. The increased volume of electronic transactions has also resulted in an increase in fraudulent activities. A weak payment system may severely drag on the stability and developmental capacity of a national economy. The technical efficiency of the payment system is important for the development of the economy [2].

These are multiple methods of payment fraud such as:

I. Phishing according to [8], is any emails or websites that require personal or private information such as credit card, bank account or login credentials are prone to phishing. If the source is trusted, such as a partner with a bank, the website is trustworthy. However, if the source is unfamiliar, it could indicate an attempt at stealing information.

II. Identity theft: Identity theft exists outside of the digital realm as well, but it's a common type of fraud online. A cybercriminal who steals personal information and uses it under false pretense is engaging in identity theft. Hackers penetrate firewalls through old security systems or by hijacking login credentials via public Wi-Fi.

III. Eavesdropping is the act of secretly or stealthily listening to the private conversation or communications of others without their consent in order to gather information.

IV. In the context of information security, and especially network security, Jindal,et al [6] state that a spoofing attack is a situation in which a person or program successfully identifies as another by falsifying data, to gain an illegitimate advantage.

V. Pagejacking: Hackers can reroute traffic from your ecommerce site by hijacking part of it and directing visitors to a different website. The unwanted site may contain potentially malicious material that hackers use to infiltrate a network security system. Ecommerce business owners must be aware of any suspicious online activity in this capacity.

VI. Skimming is the theft of personal information which has been used in an otherwise normal transaction. The thief can procure a victim's card number using basic methods such as photocopying receipts or more advanced methods such as using a small electronic device (skimmer) to swipe and store hundreds of victims' card numbers

### 1) Credit Card Fraud

A credit card is a type of credit facility, provided by banks that allow customers to borrow funds within a pre-approved credit limit. It enables customers to make purchase transactions on goods and services [13].

Credit card fraud can occur when unauthorized users gain access to an individual's credit card information in order to make purchases, other transactions, or open new accounts. A few examples of credit card fraud include account takeover fraud, new account fraud, cloned cards, and cards-not-present schemes. Credit card fraud is usually caused either by card owner’s negligence with his data or by a breach in a website’s security [13]..Here are some examples:

1. A consumer reveals his credit card number to unfamiliar individuals.
2. A card is lost or stolen and someone else uses it.
3. Mail is stolen from the intended recipient and used by criminals
4. Business employees copy cards or card numbers of its owner.
5. Making a counterfeit credit card.

### Hidden Markov Model (HMM)

The technical efficiency of payment system is important for the development of Nigeria economy; it is on this basis that the concept of Support Vector Machine (SVM) and Hidden Markov Model (HMM) is adopted for the security architecture. However, Hidden Markov Model (HMM) according to Satish and Gururaj [13] is a statistical Markov model in which the system being modeled is assumed to be a Markov process with unobservable ("hidden") states. HMM assumes that there is another process whose behavior "depends" on. A Markov chain is a stochastic model describing a sequence of possible events in which the probability of each event depends only on the state attained in the previous event.
HMM is the model to be implemented to detect frauds just based on the cardholder’s spending behavior. HMM model studies the spending behavior of the card holder which will be used to evaluate next transaction in other to predict its validity with the support of Supervised Machine Learning (SVM) model.

### 2) Supervised Machine Learning (SVM)

3) In machine learning, support vector machines (SVMs, or support vector networks are supervised learning models with associated learning algorithms that analyze data for classification and regression analysis [13]. Given a set of training examples, each marked as belonging to one of two categories, an SVM training algorithm builds a model that assigns new examples to one category or the other, making it a non-probabilistic binary linear classifier, [13]. Supervised Machine Learning is based on supervision. It means in the supervised learning technique, we train the machines using the "labelled" dataset, and based on the training, the machine predicts the output. Support Vector

Machines (SVM) will also be used to build a model to detect fraudulent transactions and genuine transaction done under duress.

1n 2017, John O. Awoyemi; Adebayo O. Adetunmbi; Samuel A. and Oluwadare [5] did a research on Credit card fraud detection using machine learning techniques: A comparative analysis in which they investigate the performance of naïve bayes, k-nearest neighbor and logistic regression on highly skewed credit card fraud data.. A hybrid technique of under-sampling and oversampling is carried out on the skewed data. The three techniques are applied on the raw and preprocessed data. The work is implemented in Python. The performance of the techniques is evaluated based on accuracy, sensitivity, specificity, precision, Matthews's correlation coefficient and balanced classification rate.

Ayoub Mniai in 2022 [1] did a research on Credit Card Fraud Detection by Improved Support Vector Data Description which designs a hybrid model for credit card fraud detection. Our hybrid solution combines the Support Vector Data Description (SVDD) and the Particle Swarm Optimization (PSO). For instance, SVDD is known by a random choice of two parameters, c and σ, which contribute to its efficiency. The proposed model uses the PSO algorithm, known by its speed, to find an optimal solution to optimize these two parameters to obtain better accuracy. Simulation results of real datasets indicate SVDD-PSO's performance compared to other machine learning techniques.

## IV. METHODOLOGY

The methodology adopted is Structured Systems Analysis and Design Methodology (SSADM) and will serve as the systems approach to the analysis and design of this work. SSADM combines three methods, complementing each other within a systems development cycle such as Logical Data Modeling, Data Flow Modeling, and Entity Event Modeling.

a) Logical data modeling, allows process of data requirements of this work investigated, identified, modeled and documented.
b) Data flow modeling deals with identifying, modeling and documenting how data flows around this work.
c) Entity event modeling: The process deals with events that have an impact on each entity and its surrounding.

Secondly, Object-oriented analysis and design (OOAD) will be based on the technical approach for analyzing and designing of this application.

### Data Collection Methods

The methods used is as follows

a) Interviews: Asking questions of a large sampling of people by direct interviews.
b) Secondary data collection: consulting various data sources, such as: Journals, conference publications, Government Records (FITC/CBN/NDIC) and the internet

## V. ANALYSIS OF THE EXISTING SYSTEM

The existing system uses a public key cryptography as the security architecture, Public key cryptography in this system uses method of encrypting or signing data with two different keys and making one of the keys, the public key, available for anyone to use. The other key is known as the private key. Data encrypted with the public key can only be decrypted with the private key. The existing does study the behavior of card holder and cannot stop transactions under duress.

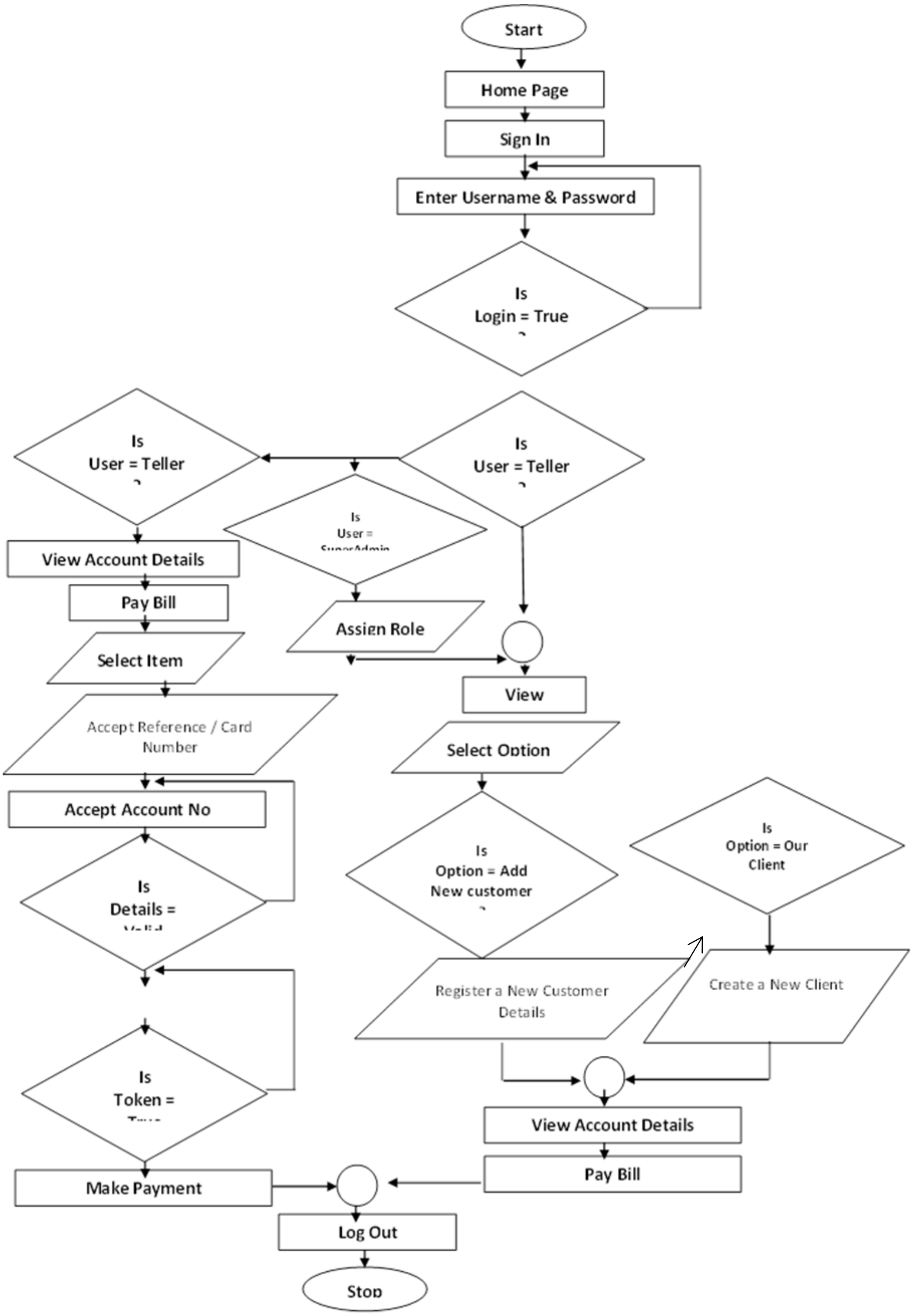

Figure A: Diagram of the existing system

### Weakness of the Existing system

The following are some of the problems with the existing system

1. The current system does not have the capacity to handle genuine transactions done under duress.
2. The current system does not have capacity to study the spending behavior of card holder
3. The current system cannot swap password.
4. In real time, the current system does not have the capacity to move current balance to suspense account.

### Analysis of the proposed system

The new system is more secured for e-payment transactions with the integration of Hidden Markov Model and Support Vector Machine as its security architecture. The new system therefore, has the following objectives:

i. To examine the causes of e-payment fraud associated with financial institution in Nigeria and develops a system that can be used to reliably secure online payment.
ii. To model the sequence of operations in credit card transaction processing using Support Vector Machine (SVM) and Hidden Markov Model (HMM)
iii. To provide a better technique of generating and providing personal identification number with creation of alternative password specifically for genuine transaction under duress.
iv. To recognize alternative password required for transactions under duress in which SVM uses to reduce 80 per cent of current balance and move it to suspense account without debit alert and also allows subsequent transactions by validating alternative password.

### How the proposed model works

Firstly, decide the type of bank account you want to open, fill up bank account opening form /Proposal Form, give references for opening your bank account, submit bank account opening form /documents and the bank officer will verify and process your bank account opening Form. Hidden Markov model (HMM) will detect frauds based on the cardholder's spending behaviors, it will prompt for BVN, the card details such as Card number, CVV number, card type, expiry date and amount to authenticate the transaction process. It then ascertain whether transaction is fraudulent or genuine. In HMM model, collections of training sets will be created to detect the spending habits of cardholder thereafter, it will be used to predict incoming transactions, if there is a suspected fraudulent, it calls up support vector machine (SVM) module that subject such transaction to further security checks by sending OTP associated with time to live (TTL) and then approve or terminate transactions based on responds of the user. However if transaction is approved, such transactions becomes part of cardholder spending behavior. In the case of genuine transaction under duress, an alternative password created during account opening will be recognized by SVM module in which 80 per cent of current balance is move to suspense account without debit alert and then automatically swap the alternative password to be the functional password while further transactions continue. However, this process is done only the first time the alternative password is used.

### Advantages of the proposed system

1. It provides a higher level of payment security for users by offering multiple encryptions and tokenization
2. It offer better conveniences to users to achieve a better user experience
3. It provides a **low risk of theft** by providing safe and secure payment transactions. Moreover, it gives all transaction records by the end of the day.
4. It has a fault tolerant due the combination of HMM and SVM

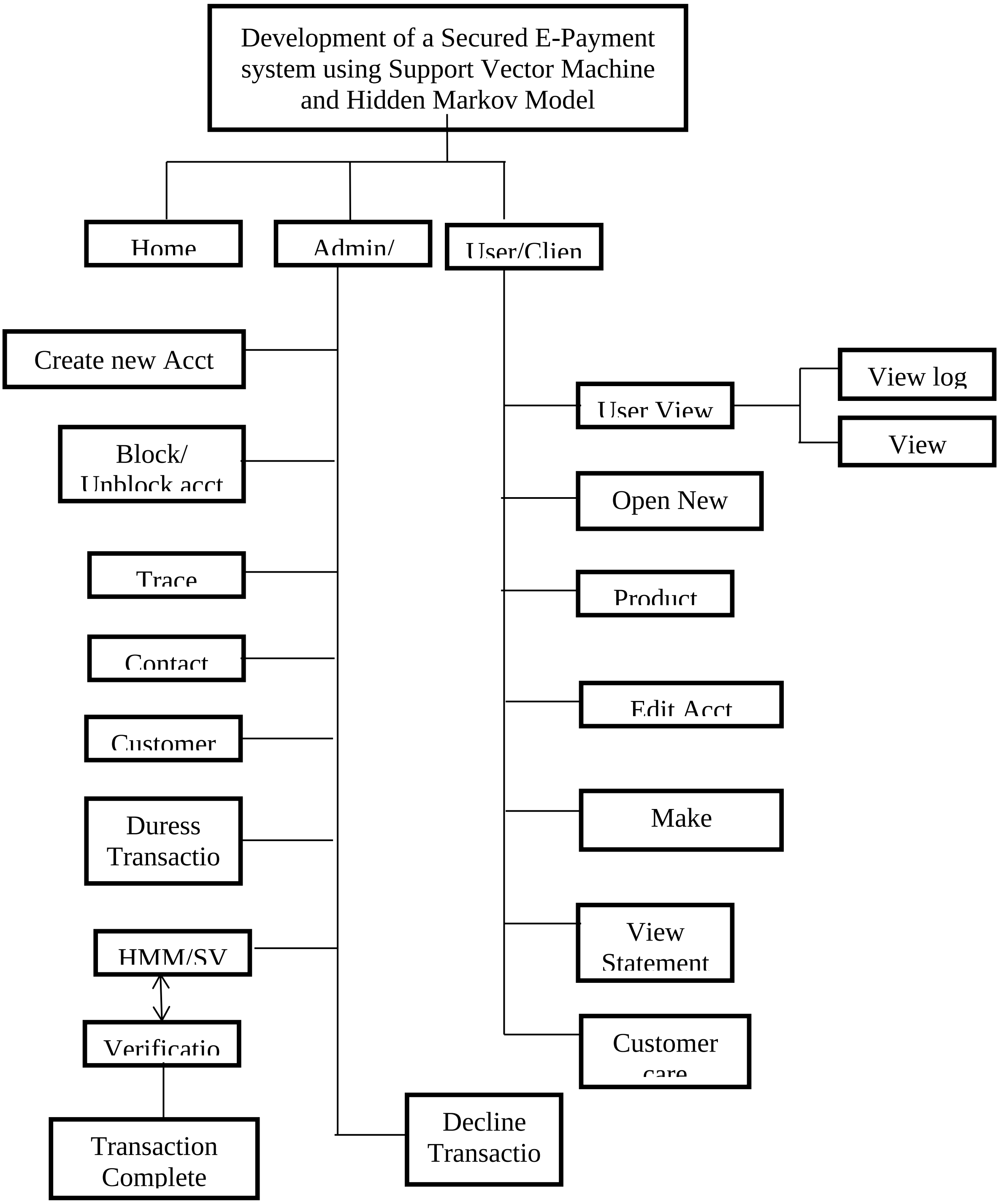

Diagram B: High Level Model of the Proposed System

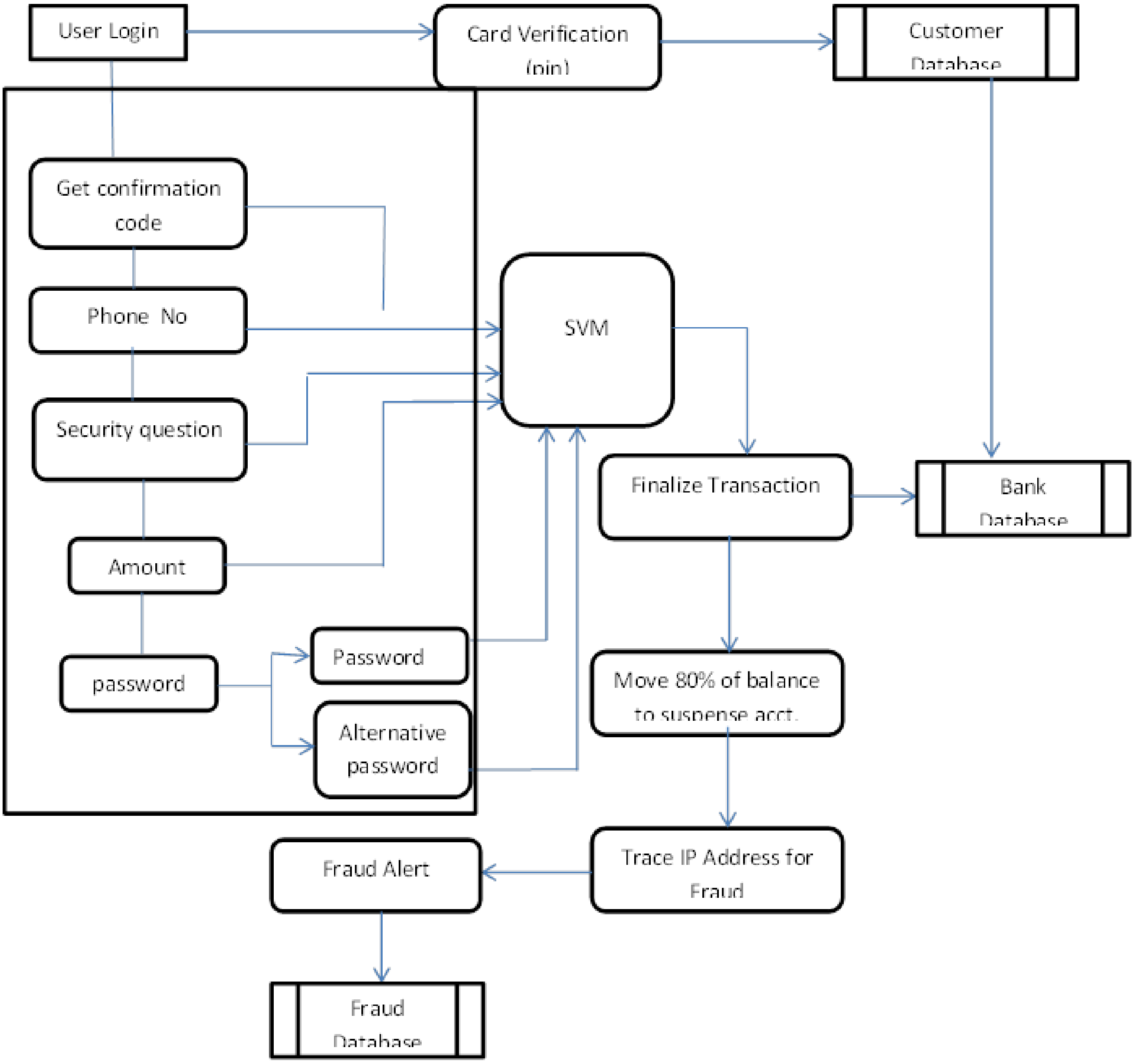

Diagram C: Data Flow diagram of the e-payment fraud detection system using HMM and SVM

## VI. CONCLUSION

Ecommerce businesses rely on electronic transactions to charge customers for products and services. The increased volume of electronic transactions has also resulted in an increase in fraudulent activities. As fraudsters grow in perpetrating evils, reliable and secured ways of protecting online transactions should be developed in order to have sustainable and dependable financial institutions in Nigeria. As Nigeria is going cashless in its financial transactions as recently spelt out by the Central Bank of Nigeria, card-holders should be way of unprotected and vulnerable online platforms for their transactions.

## VII. RECOMMENDATIONS

Having studied this model, we believe that it is a reliable and secured way of protecting card-holders money, especially those under force or duress. Users should understand that their own education and interaction with their financial institutions contribute greatly to the mitigation of fraud. We however recommend the following for users, financial institutions, and governments. Users should regularly monitor accounts as card fraud is frequently detected by cardholders and more frequent monitoring leads to earlier detection of potential fraud.

- User should know that a genuine financial institution or firm can never ask for your PIN, full password or to move money to another account, never be tricked into giving a fraudster access to your personal or financial details.
- Do not automatically click on a link in an unexpected email or text, do not keep written PIN numbers with the credit card and also report lost or stolen cards.
- Financial institutions should as a matter of urgency adopt strong and reliable authentication systems for their online transactions.
- Banks should always educate their staff as well as their customers on the need to secure their personal identification numbers for effective and reliable transactions.
- Finally, all stakeholders especially the government should review and adopt this model for efficient and secured e-payment system in Nigeria.

## REFERENCES

[1]. Ayoub, M., Khalid, J., “Credit Card Fraud Detection by Improved SVDD” Proceedings of the World Congress on Engineering, London, U.K., 2022.

*[2].* Biago, B., and Massimo C., "The Oversight of the Payment Systems: A Framework for the Development and Governance of Payment Systems in Emerging Economies" The World Bank, pp.7, 2001.

*[3]. Ben-Hur, A., Horn, D., Siegelmann, H., Vapnik, V. N., ""Support vector clustering" , Journal of Machine Learning Research. Vol.2, pp. 125–137, 2001*

[4]. Cortes, C., Vapnik, V., "Support-vector networks" (PDF). Machine Learning. Vol. 20, pp. 273–297, 1995.

[5]. John, O., Adebayo, O., and Samuel, A, “Credit Card Fraud Detection using Machine Learning Techniques: A comparative analysis” International Conference on Computing Networking and Informatics (ICCNI), 2017.

[6]. Jindal, K., Dalal, S., Sharma, K. K., "Analyzing Spoofing Attacks in Wireless Networks". 2014 Fourth International Conference on Advanced Computing Communication, 2014.

[7]. Lowry, P., Benjamin, E., (2006). "Online payment gateways used to facilitate e-commerce transactions and improve risk management" Communications of the Association for Information Systems.

[8] Ramzan, Z., (2010) "Phishing attacks and countermeasures". In Stamp, Mark; Stavroulakis, Peter (Eds.). Handbook of Information and Communication Security. Springer. ISBN 978-3-642-04117-4.

[9]. Satish, L., Gururaj, B.,. "Use of hidden Markov models for partial discharge pattern classification". IEEE Transactions on Dielectrics and Electrical Insulation, April 2003.

[10]. Schueffel, P., “The Concise Fintech Compendium. School of Management Fribourg, Switzerland, 2017.

[11]. Subramani, M., Walden, E., "The Impact of E-Commerce Announcements on the Market Value of Firms". Information Systems Research. Vol. 12 (2): pp. 135–154. doi:10.1287/isre.12.2.135.9698. ISSN 1047-7047

[12]. Turban, E.,. ”Electronic Commerce 2008: A Managerial Perspective”. London: Pearson Education Ltd. p.554, 2008.

[13]. Woolston, S. E., ” California State University, Long Beach ProQuest Dissertations Publishing, 2017. 10602012