MJoSHT
Malaysian Journal of Science, Health & Technology
[mjosht.usim.edu.my]

USIM

*Article*

# The Planning Process of the Online Transaction Fraud Detection Using Backlogging on an E-Commerce Website

Atiqah Solehah Mat Taupit and Nurdiana Azizan

*Faculty of Science and Technology, Universiti Sains Islam Malaysia, 71800 Nilai, Negeri Sembilan, Malaysia*

*Correspondence should be addressed to:*

*Nurdiana Azizan; nurdiana@usim.edu.my*

*Article Info*
*Article history:*
*Received:7 September 2022*
*Accepted:24 November 2022*
*Published:6 April 2023*

*Academic Editor:*
*Hanis Yahya*

*Malaysian Journal of Science, Health & Technology*

*MJoSHT2023, Volume 9, Issue No. 1*
*eISSN: 2601-0003*

*https://doi.org/10.33102/mjosht.v9i1.331*

***Abstract*— E-commerce is defined as the selling and purchasing of products, as well as the transmission of data or payments, through an electronic network. E-commerce is driven by the internet, where customers can browse through an online store and place orders for items or services using their own devices. Online transactions are used by e-commerce businesses to charge customers for goods and services. The rising number of online transactions has increased the number of payment frauds. Payment fraud refers to any type of fraudulent or illegal transaction carried out by a cybercriminal. The criminal utilizes the internet to deprive the victim of money, personal property, or sensitive information. The objective of this research is to investigate the gaps in the existing online transaction fraud detection on e-commerce websites, to propose and develop an online transaction fraud detection using backlogging on e-commerce websites that is safe against fraud and enables simple and efficient transactions and implement security measures to prevent a breach of the proposed system. The method for this research is using the Waterfall methodology as a Software Development Life Cycle.**

***Keywords*—** E-Commerce, Online Transaction, Payment Fraud, Backlogging, Software Development Life Cycle

## I. INTRODUCTION

This paper presents a review analysis under the requirements stage of the research. Online transaction fraud detection on an e-commerce website is a procedure that enables effective implementation of online transactions without fraud activities during e-commerce operations by utilizing a crucial application blockage known as backlogging. It is also regarded as a type of electronic commerce detector, allowing customers to directly purchase products or services from the vendor through the internet using a web browser without any possible fraud activity.

Transaction fraud poses a significant risk to online buying. As online transactions become more popular, the sorts of online transaction fraud linked with them are also on the rise and can negatively impact the financial system [1]. This fraud detection system has the capability of restricting and impeding the attacker's transaction using a real user's credit card information. To legitimize internet commerce and internet shopping, online transaction fraud detection employing backlogging on an e-commerce website allows a consumer to submit online orders for things or services from a store that serves online customers while ensuring that no fraud occurs.

To address these issues, this system has been designed to handle transactions that exceed the customer's existing transaction limit. During registration, the necessary information will be collected to allow the system to detect any fraudulent user behavior. The details of all individual transaction purchases are generally unknown to any Fraud Detection System (FDS) functioning at the bank that issues credit cards to cardholders. To overcome this issue, Behaviour and Location Analysis (BLA) is used.

FDS operates at a credit card issuing bank. Each impending transaction is sent to the FDS for verification. FDS obtains the card information and transaction value to determine whether the transaction is real or not. The FDS does not know the items acquired in that transaction. If FDS confirms that the transaction is fraudulent, the bank denies the transaction. The user's buying habits, and geographical location is utilized to validate their identification. In the case that an unexpected pattern is found, the system must be re-verified. The technology identifies unusual patterns in the payment method based on that user's past information. If any unusual patterns are detected, the system will block the transaction and a warning will be given to the user.

## II. BACKGROUND OF THE PROBLEMS

Nowadays, people all around the world are opting to purchase online any items they desire. By 2022, internet sales would account for 21% of all consumer purchases globally [2] because so many people make purchases online, which makes online payment fraud keeps increasing day by day. Reference [3] indicates that the role of digital transformation has increased in recent years. While this process has higher advantages and a favorable effect on a nation's growth, it also has certain risks for a large portion of the population. Online payment credentials are a common target for scammers since they do not even need the actual card, the scammers only need the card data that may be kept digitally. For consumers, having their credit card information stolen may be both annoying and frightening. Victims of online payment fraud spend two working days on average canceling their cards and dealing with the consequence.

Payment fraud happens when someone takes another person's credit card information and uses it to make illegitimate transactions or purchases. The actual cardholder or owner of the payment information then sees that their account is being used for transactions or purchases that they did not authorize and files a complaint. This is when the problem starts for company owners, as they will have to settle the disagreement, pay multiple penalties such as chargeback costs and investigation fees, and face an overall loss of time and resources. Due to the threat of fraud, merchant account providers such as banks may terminate a business's merchant account if they find it increasingly insecure to be involved in its transactions. It is simple to understand how payment fraud can be a major hassle for business owners.

Fraudsters are targeting organizations with inadequate fraud protection systems as customers seek to get online and retailers seek to accept more online transactions. Such fraudulent activity will most likely result in financial losses, as well as a negative impact on reputation, brand image, and client relationships. Furthermore, even when the fraudster's behavior is detected, prosecuting them might be challenging. It also requires a great amount of effort to collect evidence and establish criminal intent. Because the criteria for fraudulent activity change, it is no longer practical to rely on manual intervention and rule-based technology to detect fraudulent transactions.

Current fraud detection approaches, on the other hand, are far from accurate, resulting in huge financial losses, hassle, and consumer frustration [4]. In response to computation in the e-commerce business, e-commerce merchants deployed various technologies, systems, and procedures, as well as engaged knowledgeable specialists to maintain their market presence. Even if they manage their firm by combining technology and specialists, they cannot prevent fraudulent conduct from occurring.

The research questions for the research are (1) What are the gaps in the existing online transaction fraud detection on e-commerce websites? (2) What is the requirement to develop online transaction fraud detection using backlogging on e-commerce websites? And (3) How should the security measures for the proposed system be implemented to prevent a security breach?

The research objectives of the research are (1) to investigate the gaps in the existing online transaction fraud detection on e-commerce websites, (2) to propose and develop an online transaction fraud detection using backlogging on e-commerce websites that is safe against fraud and enables simple and efficient transactions, and (3) to implement security measures to prevent a breach of the proposed system.

The research is to develop an e-commerce site as a web-based system that can assist in detecting transaction frauds using backlogging on an e-commerce website when a customer purchases products from the seller through the internet using a web browser. The system is anticipated to be able to receive, store, and process data related to the customer who registers and uses the system. Furthermore, the system is expected to provide a better interactive feature in an e-commerce website and be able to detect any fraudulent transactions and can restrict and prohibit transactions carried out by an attacker. The system is expected to be secured with the implementation of authentication, a bcrypt hashing algorithm, and One Time Password (OTP). This research also comprises a literature study that provides background information on e-commerce, as well as the selection of an appropriate life cycle model and the development of a website prototype. The system will be designed with MySQL as the back end and the Visual Basic application package as the front end.

Cybercriminals or attacks are considered unauthorized activities to get access to a business system's important information. It employs various methods to carry out cyberattacks to harm business operations [5]. The most serious issue in the e-commerce sector is fraud. Reference [6] explains that computer intrusion is a type of behavior that results in fraud and intrusion assaults on e-commerce online platforms. Reference [6] indicates that fraud occurrences are often discovered using massive data sets such as recorded data and user behavior. Data acquired through logs and user behavior may be extremely useful for fraud detection to learn from recent assaults.

The issue is that the legal and competitive complexities of e-commerce make it exceedingly difficult for researchers to collect accurate data from organizations. Real e-commerce data is extremely difficult to obtain since it contains personal information that, if publicly revealed, would raise legal concerns under data protection rules. Furthermore, actual data may show possible weaknesses in an e-commerce site, causing a loss of confidence in the service being provided while opening the way to additional threats. Furthermore, researchers have concluded that automated fraud detection in the field of e-commerce is still a major challenge.

In today's world, credit cards are commonly utilized as an essential mode of payment. People used credit cards for a variety of reasons, including obtaining credit, obtaining a loan, making quick payments, and using a charge card. Some contentious issues have been addressed, not just in terms of the amount of credit flooding the country's economy, but also in terms of the number of transactions that result in payment default and the number of credit card fraud cases that have been recorded, both of which have put the economy in jeopardy. However, as technology has advanced and consumer behavior has changed, credit cards have become more prominent and useful in continuing to do operations [1].

The credit card industry is evolving. Numerous issues arose from the card issuer's perspective. The internet, as well as the ambiguity associated with the card, not present (CNP) transactions, pose new fraud control issues. Authentication of the cardholder is a need for monitoring fraud on the internet. There are no commonly used configurations. As a result, credit card fraud on the internet is far more prevalent than in the actual world. There are many types of online transaction fraud detection techniques. Table I discussed the comparison of previous research on fraud detection in e-commerce systems.

Reference [10] informs that, with the growth of cutting-edge technology and global connectivity, fraud has risen dramatically, and fraud can be detected using either preventative measures or detection techniques. A backlog is several things that have not yet been done but need to be done. With Behaviour and Location Analysis (BLA), the user's buying habits, and geographical location are utilised to validate their identification. The technology identifies unusual patterns in the payment method based on that user's information. If any unusual patterns are detected, the system will block the transaction and a warning will be given to the user. The difficulty of identifying fraudulent transactions arises after they have concentrated on fraud protection measures and associated procedures. There is a vast literature on a wide range of security solutions to protect transactions from unauthorized use or exposure of their private data and hence precious resources [1]. In each instance, fraudsters uncover a way to overcome a variety of preventative tactics. On the other hand, many transaction mediums, such as bank cards, or debit cards, need the use of pins, and passwords, and, in some circumstances, biometrics are used to verify the real owner.

Credit cards provide significant difficulties since they normally do not require a pin to be used, instead, only the cardholder's name, expiration date, and a record number are required. The most common method of illegally executing credit cards is to steal someone's identity and, in certain situations, create a new fraudulent identity. As a result, the key problem is fraudulent electronic credit card transactions. Reference [1] indicates that credit cards do not have to be available to execute over the internet, they may be used to fraudulently execute the web better and bigger losses for banks and their consumers when obtained by criminals.

The core principle in fraud detection is that fraud may be identified by observing significant deviations from a customer's normal behavior. That is the reason the behavior of a record might therefore be utilized to secure that account. Currently, banks have realized that detecting fraud requires a combined, global technique, including the frequent exchange of data concerning attacks. Credit card fraudsters do the crime in a variety of ways. As technology evolves, so does the technology of criminals, and hence the method by which fraudsters approach accomplishing fraudulent acts.

# I. METHODOLOGY

An appropriate method is required to develop a system. The developer may then fulfill the requirements and produce a high-quality solution in time. Thus, this section describes the process involved in developing the system, as well as the rationale for selecting that. The chosen methodology must also go through several phases and this section explains each phase. The Waterfall technique was selected as the Software Development Life Cycle (SDLC) for developing the system. The Waterfall process incorporates the steps of requirement, design, implementation, testing, and maintenance.

According to [11], the Waterfall approach is used when the requirements of an issue are generally clearly stated and well understood. As a result, the Waterfall technique is chosen since the requirements are well known. In terms of scope, budget, and schedule, a Waterfall methodology can produce a more predictable result. The development of the system can proceed to the next stage only when the present stage has been finished. Fig. 1 shows the flow of the Waterfall model.

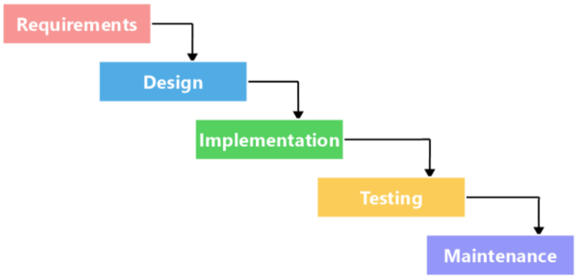


Fig. 1: Waterfall SDLC Model [12]

TABLE I. COMPARISON TABLE OF PREVIOUS WORK

| No | System | Platform | Functionalities and Specialities | Limitation |
|---|---|---|---|---|
| 1. | A Fraud Detection System Based on Anomaly Intrusion Detection Systems for E-Commerce Applications [6] | Application-based | -Employs several anomaly detection techniques to detect computer intrusion threats in e-commerce sites.<br>-While information is retrieved from queries generated when accessing server-side code on an e-commerce site, the system analyses these queries and creates models for various attributes. | -There may still be different vulnerabilities inside an e-commerce web application that allow intrusions by unauthorized users. |
| 2. | Fraud Detection for E-commerce Transactions by Employing a Prudential Multiple Consensus Model [7] | Application-based | -Maximize the model's effectiveness in detecting fraudulent transactions despite any data imbalance. | -Unbalanced distribution of the training data characterizing the past transactions which generate 40 different problems of over-fitting and lead to low performances of the adopted classifiers. |
| 3. | eFraudCom: An E-commerce Fraud Detection System via Competitive Graph Neural Networks [8] | Application-based | -Enables to detect of fraud behaviors in presence of the new fraud patterns.<br>-A case study using e-commerce system datasets demonstrates that Competitive Graph Neural Networks remain strong even after the fraud patterns have been improved. | -Merchants who have previously utilized a third-party fraud service platform to fulfill fraud transactions are likely to do that again.<br>- It is difficult to adapt to the continual evolution of fraud patterns since they rely heavily on the "fraudster seeds" predefined by domain specialists. |
| 4. | Fraud Detection in E-Commerce Using Machine Learning [9] | Application-based | -Machine learning techniques such as Sentiment Analysis, Support Vector Machine (SVM), Decision Tree algorithm, and N-gram model are used to detect fraudulent, incorrect, and spam reviews for fraud detection. | -It was discovered that while work on spam terms had been done using various methodologies, the detection was still lacking in several ways, which involved other elements such as IP addresses, MAC addresses, and Email accounts. Additionally, Machine Learning techniques were lacking, and very little work had been completed. |

The waterfall method aims to examine requirements from the beginning and did not allow the operation to start until the requirements were fully documented, understood, and significantly fixed. Requirement analysis involves understanding what to design, as well as its function and purpose, the input and output specifications, as well as the final product specifications are examined during this phase.

System design aids in the specification of hardware and system requirements, as well as the general architecture of the system. The process of selecting the database conceptual schema, logical diagram design, and software architecture design will take place during this phase. This phase produces a detail of how the system should be designed and implemented. Before moving on to the next step, the designs will be prototypes.

The source code is written by the requirements, and the physical design specifications are converted into workable code during the implementation phase. The programming language chosen is determined by the requirements for developing a web-based system. Thus, the programming languages that will be used during the implementation phase are JS, CSS, HTML, and Python. Table II will provide further information on these languages.

The system testing phase needed the actual testing and assessment of the proposed system developed to meet the original requirements. Bugs and device vulnerabilities are identified, fixed, and enhanced during this phase. To get the best possible results from the system, functional testing, which is a sort of black box testing will be employed in the online transaction fraud detection system. The testing phase is essential for producing a high-quality final product. Fig. 2 illustrates the technique of Black Box testing.

Black box testing is important in software testing since it aids in the overall system functioning validation [13]. Black Box Testing is a type of software testing in which the functioning of software applications is tested without understanding the underlying code structure, implementation details, or internal paths.

TABLE II. LANGUAGE AND TOOL USE IN SYSTEM IMPLEMENTATION

| Language/Tool | Description |
|---|---|
| **JavaScript** | JavaScript can be used to generate interactive and dynamic web content. It can modify and update both HTML and CSS. |
| **CSS** | Used to style the web content. |
| **HTML** | Used to manage the information and structure of a web page. |
| **Python** | It can be used to construct a wide range of applications. |
| **MySQL** | The system database. |
| **Apache** | Sends the requested files, images, and other data to the user. It is used to transfer the content of the web |
| **Visual Studio Code** | A tool for code implementation. |

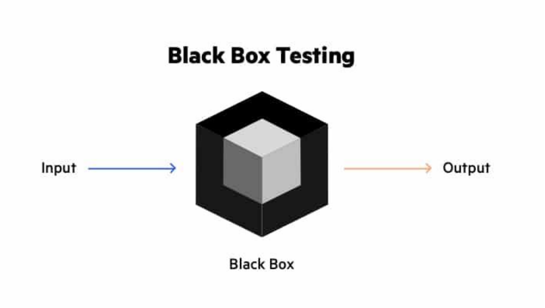


Fig. 2: Black Box Testing

Black Box testing is entirely dependent on software requirements, and it focuses on the input and output of software applications. This sort of testing is performed by the system's developer, and test cases are created to compare predicted and actual outcomes. If the two results do not match, the mistakes will be corrected by the developer.

Functional testing demonstrates that the evaluated features are present as described in the project requirements and documentation. Table III shows the main focuses of functional testing.

TABLE III. MAIN FOCUS OF FUNCTIONAL TESTING

| | |
|---|---|
| Valid Input | All correct input must be accepted. |
| Invalid Input | All incorrect input must be discarded. |
| Functions | The functions must be executed when they have been recognized. |
| Outputs | The application outputs that have been identified must be executed. |
| System | Interfacing systems and processes must be performed. |

According to [14], the final phase, which is system maintenance, is the process of adjusting or modifying a software system after it has been delivered to refine output, fix errors, and increase performance and quality. Software maintenance is conducted when users experience technical challenges. This phase allows users to express their satisfaction or dissatisfaction with the system. If the users request a modification, the developer must deal with the issue.

## II. EXPECTED RESULTS

This section presents the expected system design. The research purpose is to create a system that can effectively identify online credit card fraud. When a user's spending exceeds the predetermined transaction limit or the user's location deviates from the norm, the system detects an unusual trend and either requests re-verification or notifies the user and the associated bank. So based on the previous data of that user, the system recognizes unusual patterns in the payment procedure.

The use case diagram aids in identifying the interaction between the system and the actors. Use a case diagram to highlight the system’s functionality and scope. Fig. 3 illustrates the use case diagram. Their actors are divided into two which are users and administrators. Each actor has a role to interact with the system. They can view products, buy the product, pay through an online transaction, and view their transaction. They are also required to log out after using the system. User needs to register their account before they can log in to the system by using the correct credentials. After that, they can buy their desired product and proceed to the payment. After the transaction is validated, the payment is complete. The administrator also needs to register before they can access the system with the correct login information. The administrator can add a new product and view the transaction.

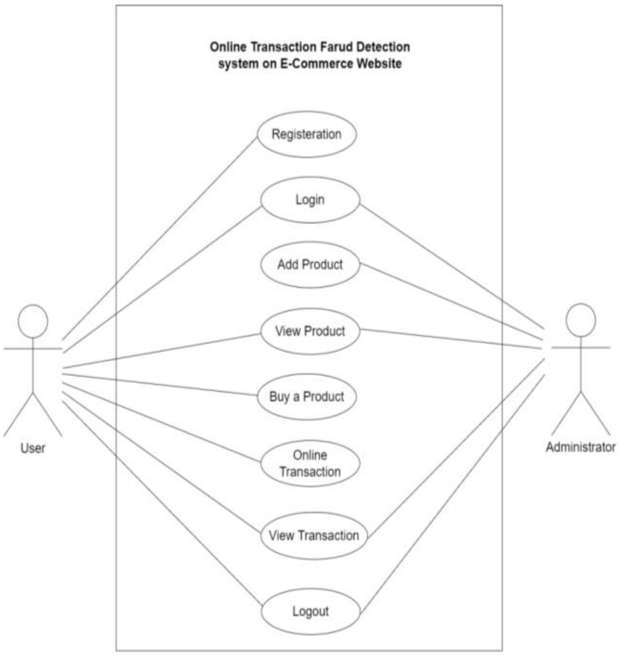


Fig. 3: Use Case Diagram

Features for the administration page include login and adding or viewing products. Fig. 4 presents the login page for the administrator. The administrator needs to log in using valid login credentials to access the system. Also, the administrator can add a new product with its details into the system.

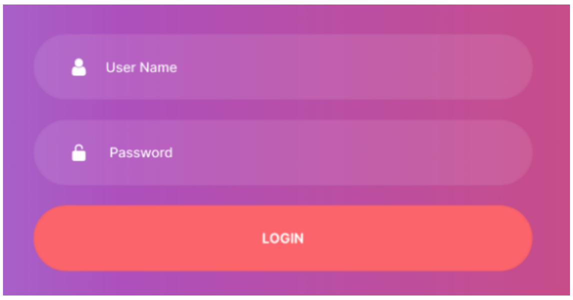


Fig. 4: Login Page for Administrator

Features for the user page include registration, login, viewing the product, and buying the product. Fig. 5 displays the user registration page. Here, users first need to register themself with details to access the system.

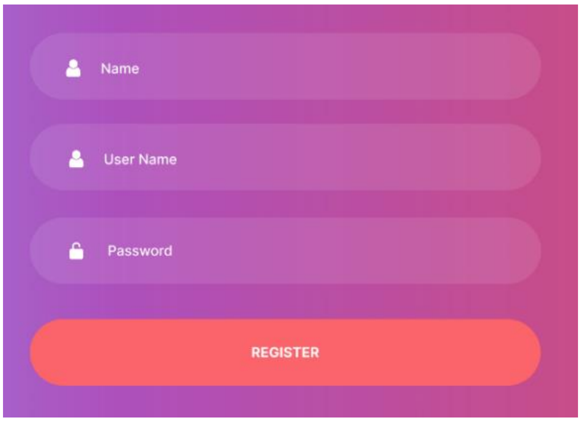


Fig. 5: User Registration Page

After successful registration, users then need to login into the system by inserting their credentials into the system (Fig. 6). Users can view multiple products with their details on the product page (Fig. 7). Interested users can purchase a product online transaction. User is required to fill in their card information which is their card number, CCV number, and expiry date to perform payment on the user payment process page (Fig. 8).

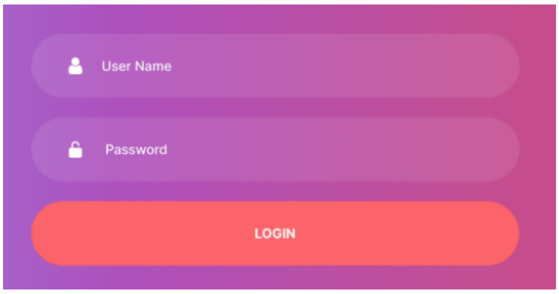


Fig. 6: User Login Page

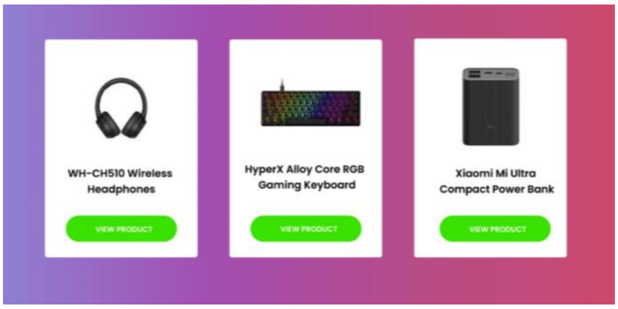

WH-CH510 Wireless Headphones
VIEW PRODUCT
HyperX Alloy Core RGB Gaming Keyboard
VIEW PRODUCT
Xiaomi Mi Ultra Compact Power Bank
VIEW PRODUCT

Fig. 7: Product Page

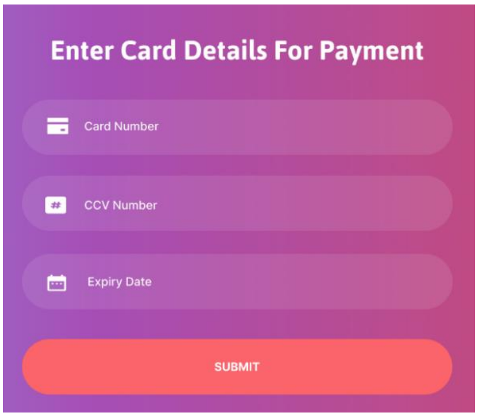
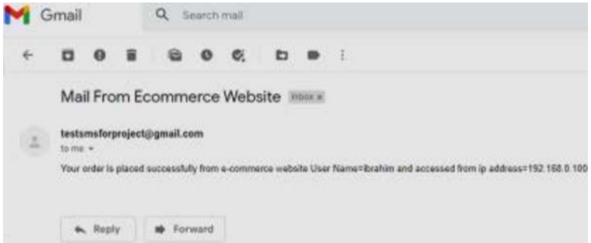


Fig. 8: User Payment Process

With the rise of e-commerce enterprises that offer services to worldwide clients, fraudsters have begun to target organizations from all over the world while remaining hidden in the background. In most situations, company owners find out about a scam after it has already occurred. It is now too late to respond before client complaints begin to arrive. In these circumstances, the business vendors must repay the card user, resulting in a significant loss in income. To counteract this problem, new fraud detection techniques (FDS) such as IP geolocation have been developed to aid in the identification of all types of illegal transactions as they occur. For example, geodata may be used to check all the specifics of a transaction performed from a certain country, and if any suspicious behavior is detected, it immediately examines the situation and confirms whether the individual making the transaction is genuine or a fraudster (Fig. 9). Fig. 10 presents the flowchart of the system.



Mail From Ecommerce Website

testsmsforproject@gmail.com
to me

Your order is placed successfully from e-commerce website User Name=Ibrahim and accessed from ip address=192.168.0.100

Fig. 9: Ordering with Geo Location Facility Confirmation

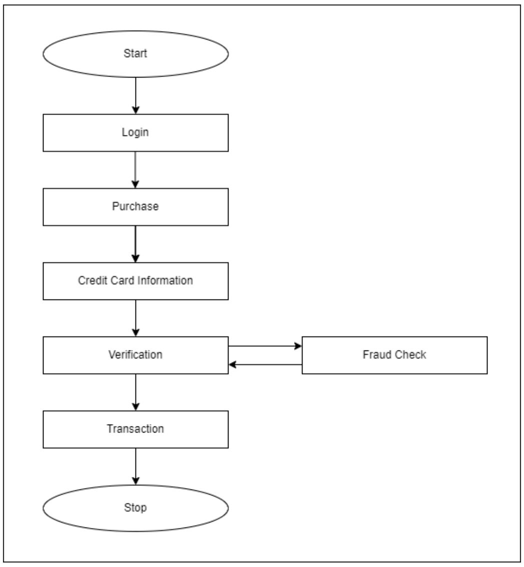


Fig. 10: Flowchart of the System

The following is the algorithm of the system.

Step 1: START
Step 2: Program initialization
Step 3: User login
Step 4: Product Purchasing
Step 5: Verification of card transaction limit
Step 6: If card limit > user limit
Step 7: Security questions / Alert
Step 8: If fraud is detected, then send the location IP, OTP and
username to cardholders
Step 8.1: FDS blocks transaction
Step 8.2: STOP

## III. CONCLUSION

This research uses behavior analysis to identify fraudulent online credit card transactions in real time. The algorithm also uses a multi-layered security-based strategy for the transaction restrictions established by the relevant user. The customer's spending limit is used to classify transactions, which aids in determining if the current transaction is legitimate or fraudulent. Finding out the user's location is vital in detecting credit card fraud. The system is useful in a small-scale website for detecting fraud, and with additional improvements, it might be employed in a large-scale e-commerce website where thousands of transactions can occur simultaneously.

## CONFLICT OF INTEREST

The authors declare that there is no conflict of interest regarding the publication of this paper.

## ACKNOWLEDGEMENT

We thank everyone who provided insight and expertise that greatly assisted the research, although they may not agree with all the interpretations and conclusions of this paper.

## REFERENCES

[1] T. S. Chandu, and M. Sreedevi, “Online transaction fraud detection using backlogging on an e-commerce website,” Journal of Xi'an University of Architecture & Technology, vol. 6(8), pp. 36-45, 2020 ISSN number: 1006-7930.

[2] M. Keenan. (2022) Global e-commerce explained: Stats and trends to watch in 2022. [Online]. Available: https://www.shopify.my/enterprise/global-ecommerce-statistics

[3] Ponce, Edwin Kcomt, Katherine Escobedo Sanchez, and Laberiano Andrade-Arenas. "Implementation of a web system: Prevent fraud cases in electronic transactions." International Journal of Advanced Computer Science and Applications West Yorkshire 13, no. 6 (2022): 865-876. https://dx.doi.org/10.14569/IJACSA.2022.01306102

[4] Padmalatha, N. A. "E-Commerce Frauds and the role of fraud Detection Tools in managing the risks associated with the frauds." International journal of advanced science and Technology 29, no. 4 (2020): 38-46.

[5] J. Joy. The implication of the cyber threats and its issues in the business process organization: A case study of Tesco. *Department of Computing and Informatics Bournemouth University*, 2022.

[6] Massa, Daniel, and Raul Valverde. "A fraud detection system based on anomaly intrusion detection systems for e-commerce applications." Computer and Information Science 7, no. 2 (2014): 117-140.

[7] R. Saia., S. Carta., D. R. Recupero., and G. Fenu, “Fraud detection for e-commerce transactions by employing a prudential multiple consensus model,” *Journal of Information Security and Applications*, vol. 46, pp. 13-22, 2019. https://doi.org/10.5539/cis.v7n2p117

[8] Zhang, Ge, Zhao Li, Jiaming Huang, Jia Wu, Chuan Zhou, Jian Yang, and Jianliang Gao. "efraudcom: An e-commerce fraud detection system via competitive graph neural networks." ACM Transactions on Information Systems (TOIS) 40, no. 3 (2022): 1-29. https://doi.org/10.1145/3474379

[9] Saeed, Muhammad Ahsan, Farrukh Yousaf, Osama Bin Khalid, Mushhad Gilani, Qamar Nawaz, and Isma Hamid. "Fraud Detection in E-Commerce Using Machine Learning." International Journal 10, no. 3 (2021). https://doi.org/10.30534/ijatcse/2021/1011032021

[10] S. Wangde, R. Kheratkar, Z. Waghu, and P. S. Lawand. Online transaction fraud detection system using machine learning & e-commerce. *International Research Journal of Engineering and Technology*, 9(4), 2022.

[11] S. M. Salve., S. N. Samreen., and N. K. Valmik, “A comparative study on software development life cycle models”, *International Research Journal of Engineering and Technology*, vol. 5(02), pp. 5, 2018.

[12] E. Finlay. (2021) 5 waterfall project management phases you should know about. [Online]. Available: https://blog.mindmanager.com/waterfall-project-management-phases/

[13] Nidhra, Srinivas, and Jagruthi Dondeti. "Black box and white box testing techniques-a literature review." International Journal of Embedded Systems and Applications (IJESA) 2, no. 2 (2012): 29-50. http://dx.doi.org/10.5121/ijesa.2012.2204

[14] Bassil, Youssef. "A simulation model for the waterfall software development life cycle." arXiv preprint arXiv:1205.6904 (2012). https://doi.org/10.48550/arXiv.1205.6904