PLATFORM D (THEORETICAL AND APPLIED COMPUTERS)

ONLINE TRANSACTION FRAUD DETECTION USING BACKLOGGING ON E-COMMERCE WEBSITE: A REVIEW

Atiqah, S.M.T. and Nurdiana, A.*

Faculty of Science and Technology, Universiti Sains Islam Malaysia (USIM), 71800 Nilai, Negeri Sembilan, Malaysia.

**Corresponding author: nurdiana@usim.edu.my*

***Keywords**: E-Commerce, online transaction, payment fraud, backlogging, software development life cycle.*

ABSTRACT

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 system can 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, bcrypt hashing algorithm, and One Time Password (OTP). 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. 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.

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 behaviour. 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.

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 favourable 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.

METHODOLOGY

The methodology for this research is a waterfall model that includes five phases namely requirements, design, implementation, verification, and maintenance. The requirements phase is to identify the user needs, the design phase is to develop the system, the implementation phase is to execute the system, the verification phase is to test the system, and the maintenance phase is to detect and fix the problems.

RESULTS AND DISCUSSION

Features for the user page include registration, login, view product, and buy the product. Figure 1 displays the user registration page. Here, users first need to register themself with details to access the system.

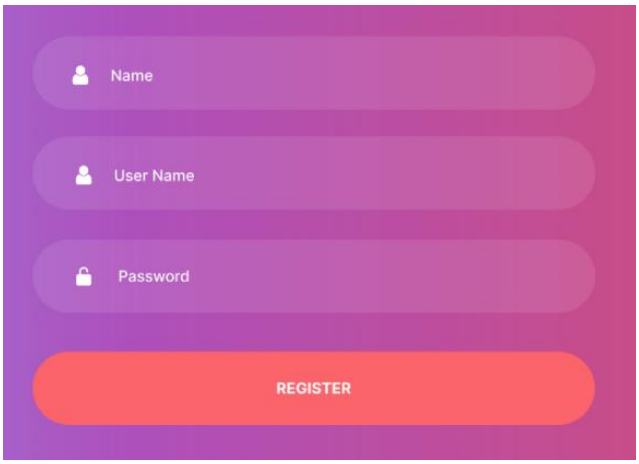

Figure 1. User Registration Page

After successful registration, users then need to login into the system by inserting their credentials into the system. Users can view multiple products with their details on the product page. 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.

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.

[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] E. K. Ponce, K. E. Sanchez, and L. Andrade-Arenas. Implementation of a web system: Prevent fraud cases in electronic transactions. *International Journal of Advanced Computer Science and Applications*, 13(6), 2022.