Online Transaction Fraud Detection using Back Logging

Yahye Sh Hussein Ibrahim[#1], Dr. A. Sivakumar[*2]

[#]*Student, M.Sc Information Technology, Rathinam College of Arts and Science,
Coimbatore, Tamil Nadu, India -641021*
yahyeshhusseinibrahim.mit20@rathinam.in

[*]*Assistant Professor, Department of Computer Science,
Rathinam College of Arts and Science, Coimbatore, Tamil Nadu, India -641021*
sivakumar.cs@rathinam.in
ORCID iD: https://orcid.org/0000-0003-3517-816X

Abstract - **Due to a rapid advancement in the electronic commerce technology, the use of credit cards has dramatically increased. As credit card becomes the most popular mode of payment for both online as well as regular purchase, cases of fraud associated with it are also rising. In this paper, we model the sequence of operations in credit card transaction processing using a Back Logging (BL) and show how it can be used for the detection of frauds. An BL is initially trained with the normal behaviour of a cardholder. If an incoming credit card transaction is not accepted by the trained BL with sufficiently high probability, it is considered to be fraudulent. At the same time, we try to ensure that genuine transactions are not rejected. We present detailed experimental results to show the effectiveness of our approach and compare it with other techniques available in the literature. In this we converted the transaction on credit card in series and trained the card initially with the normal usage of the card holder. If the usage is unnatural the transaction automatically blocked. If it is authentic the transaction process occurs normally. Here we are introducing a project for the online transaction fraud detection using Back Logging. It is done on the basis of the spending profile of the card holder. The usual spending of the cardholder is being checked by the FDS (Fraud Detection system) in the bank. The system checks all the spending of the user. When it turns unusual the method blocks the transaction on the card. And it alerts the bank. It occurs automatically. It doesn't need any man power.**

Index Terms - **Fraud Detection system, Back Logging, Electronic Commerce.**

I. INTRODUCTION

The online fraud occurs with credit cards fraudulent are of two types, 1) Physical card and 2) Virtual card.

In physical card fraudulent occurs when the card getting transacted physically. It can be in two ways, when the card holder presents his/her card for purchase an attacker steal the card or the card holder loose his/her card and without being the awareness of the card is lost. In the second type of transaction the fraudster knows some important information about the card like card no, secure code and make use of it for a payment. On both the two types it leads to a large financial loss to the credit card company and to the card holder. To find out these types of credit card frauds only way is to analyzing the spending pattern figure it out the unnatural spending with compare to the usual spending. Card fraudulent detection on the basis of the spending profile is the most capable way to reduce the frauds.

II. SYSTEM STUDY

EXISTING SYSTEM:

All the existing method to detect the credit card was on the mode like the detection occurs only after the complaint of the card holder about fraud done. It is not a convenient way to avoid the loss happens to the card holder. After getting the complaint they detected the fraud on the basis of the IP address. For this they need the help of the Cybercrime to detect the fraud and make action on it. It takes so much man power.

Disadvantages of the Existing System:

1. The main disadvantage of the existing system is the detection occurs only after gets a written complaint.

2. In the existing system there is physical inconvenience exists.

3. The period occurs to detect the fraud will cause so many losses to the card holder.

4. There is no particular security system in the existing so a hacker can easily access others card. No accuracy in image.

5. The image can be compressed with loss of the clarity and loss of pixels.

THE PROPOSED SYSTEM:

Here we are introducing a project for the online transaction fraud detection using Back Logging. It is done on the basis of the spending profile of the card holder. The usual spending of the cardholder is being checked by the FDS (Fraud Detection system) in the bank. The system checks all the spending of the user. When it turns unusual the method blocks the transaction on the card. And it alerts the bank. It occurs automatically. It doesn't need any man power.

Advantages of the proposed system:

1. The main advantage is that the detection occurs much faster than any other method.

2. In all the existing systems the real card holder should checked for the Fraud detection. But in our method, there is no need of the physical inconveniences of the card holder. All the checking and the detection occur automatically.

3. This project needs no man power for the detection.

4. This project provides most accurate method in credit card fraud detection
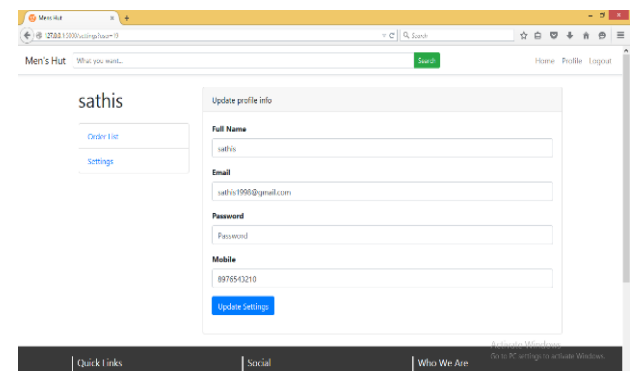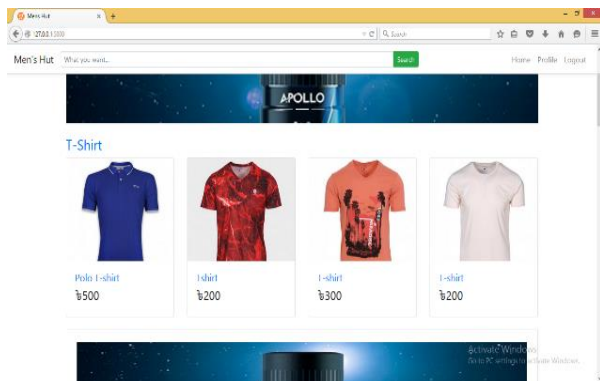
III. OUTPUT SCREENS
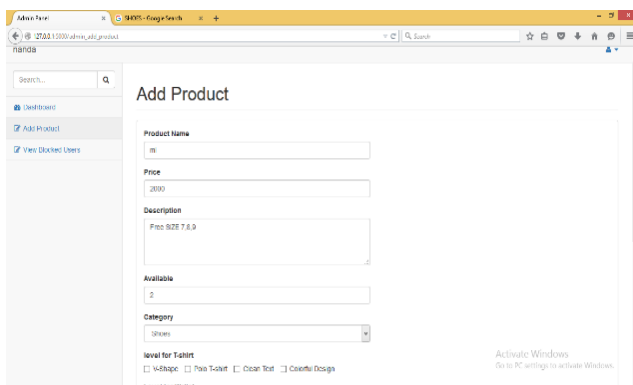### Login Form
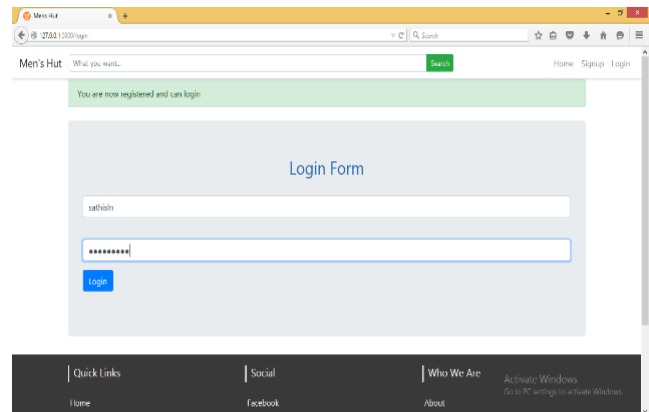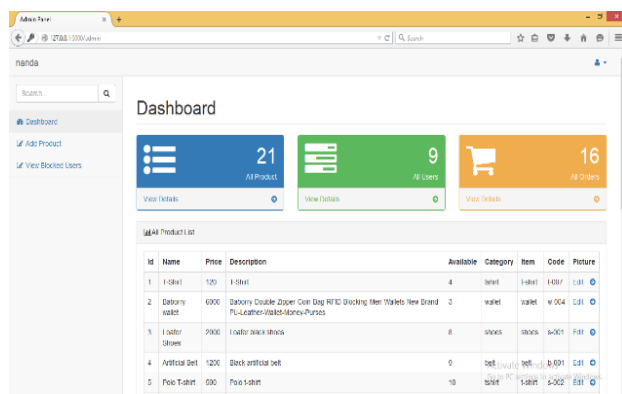

Registration Form
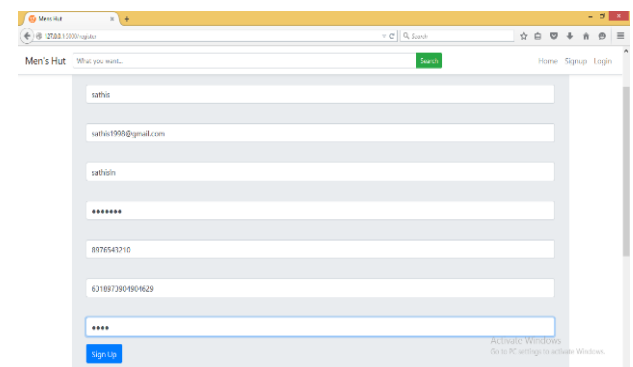
Update Profile

T-Shirt Details

Add Product

Dashboard

IV. CONCLUSION

In this project, we have proposed an application of BL in credit card fraud detection. The different steps in credit card transaction processing are represented as the underlying stochastic process of an BL. We have used the ranges of transaction amount as the observation symbols, whereas the types of items have been considered to be states of the BL. We 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 BL 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.

REFERENCES

[1] Iwasokun GB, Omomule TG, Akinyede RO. Encryption and tokenization-based system for credit card information security. Int J Cyber Sec Digital Forensics. 2018;7(3):283–93.

[2] Burkov A. The hundred-page machine learning book. 2019;1:3–5.

[3] Maniraj SP, Saini A, Ahmed S, Sarkar D. Credit card fraud detection using machine learning and data science. Int J Eng Res 2019; 8(09).

[4] Dornadula VN, Geetha S. Credit card fraud detection using machine learning algorithms. Proc Comput Sci. 2019;165:631–41.

[5] Thennakoon, Anuruddha, et al. Real-time credit card fraud detection using machine learning. In: 2019 9th international conference on cloud computing, data science & engineering (Confluence). IEEE; 2019.

[6] Robles-Velasco A, Cortés P, Muñuzuri J, Onieva L. Prediction of pipe failures in water supply networks using logistic regression and support vector classification. Reliab Eng Syst Saf. 2020;196:106754.

[7] Liang J, Qin Z, Xiao S, Ou L, Lin X. Efficient and secure decision tree classification for cloud-assisted

online diagnosis services. IEEE Trans Dependable Secure Comput. 2019;18(4):1632–44.

[8] Ghiasi MM, Zendehboudi S. Application of decision tree-based ensemble learning in the classification of breast cancer. Comput in Biology and Medicine. 2021;128:104089.

[9] Lingjun H, Levine RA, Fan J, Beemer J, Stronach J. Random forest as a predictive analytics alternative to regression in institutional research. Pract Assess Res Eval. 2020;23(1):1.

[10] Breiman L. Random forests. Mach Learn. 2001;45(1):5–32.