International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-6, March 2020

Location-Based Credit Card Fraud Detection with Two Way Authentication

K. Vineela, K. Mounisha, S.Prayla Shyry

Abstract: ***The quick expansion of internet transactions has provided rise to a considerable quantity. Nevertheless,the Internet world is opened, your shopping devices have pesky insects, and also crooks can make use of a negative methods such as for instance Trojan and also pseudo base station. This leads to major raising of credit card fraud functions. If a criminal steal or perhaps cheats the info on the credit card of a cardholder, the criminal can utilize the credit card to ingest. Based on the Nilson Report in October 2016, over thirty-one trillion dollars have been produced globally by internet transaction methods within 2015, boosting 7.3 % than 2014. Globally losses at credit card fraud rose to twenty-one billion dollars throughout 2015, and can perhaps attain thirty-one billion dollars by 2020. Our proposed system is capable to stay away from the fraud transactions using previous data achieving the anticipated security level.***

Keywords: Credit card; Application Access;Security;Crooks;

I. INTRODUCTION

Credit card fraud detection is a method to stop fraud functions, and is generally classified into two techniques: i) anomaly detection ii) classifier-based detection. Anomaly detection concentrates on calculating the distance among the information areas in the garden. By calculating the distance between the new transaction as well as the cardholder's profile, an anomaly detection technique can easily filtrate a new transaction that will be sporadic together with the cardholder's profile. The next method uses a lot of monitored mastering solutions to instruct a classifier based on the foundation of specified natural transactions as well as fraud transactions. The monitored mastering concentrates on removing fraud capabilities from fraud transactions. Nevertheless, each of them has limits.

Manuscript received on March 12, 2020.
Revised Manuscript received on March 25, 2020.
Manuscript published on March 30, 2020.
*correspondence author
Vineela K*, student, Computer Science and Engineering, Sathyabama Institute of Science and Technology, Chennai, Tamil Nadu, PIN-600119, , EMAIL- kolagani.vineela@gmail.com
Mounisha K, student, Computer Science and Engineering, Sathyabama Institute of Science and Technology, Chennai, Tamil Nadu, PIN-600119, EMAIL- kondurumounisha99@gmail.com
Dr S PraylaShyry, Professor, School of Computing, Sathyabama Institute of Science and Technology, Chennai, Tamil Nadu, EMAIL- praylashyry@gmail.com

For anomaly detection, it has absolutely no power to show fraud characteristics though it is able to show card-holders' transaction actions.In existing system, the transaction is going to take place if the person uses the right pin pass which is stored inspecific flash memory card.As there is an enhanced engineering method that can hack theend-user credit card information and operator pin quantity. Dealing with the above-mentioned difficulties, we extract the transaction actions of a cardholder utilizing each his/her historic transaction information and also the information of a few identical cardholders. In addition, we proposed a responsemechanism that may adjust towards the cardholder's transaction actions seasonally.

II. LITERATURE SURVEY

Sahayasakila et., al.(2019), proposed to detect creditcard fraud using machine learning algorithms. Two main concepts used are the whale optimization algorithm (WOA) and Smote(synthetic minority oversampling techniques) algorithms. In this, whale optimization mainly consists of three operators that stimulate prey search, prey encircling and bubble-net scratch around the humpback Whales behavior. This method is mainly used to improve the detecting speed of the fraud transaction but it lacks an accuracy rate of solution. Smote technique provides a solution to class imbalance issues. In this method, the transactions(data) are trained. It differentiates between fraud transactions from normal transactions that are done by card-holders. The experimental analysis showed that fraud detection using these machine learning algorithms is much more efficient than BP neural networks.

Ramyashree.K et., al. (2019),introduced a fraud detection method using a mining algorithm called “machine learning algorithm” which recognizes credit card fraud. It proposed to initially use this algorithm and then apply hybrid methods namely Adaboost and majority vote method. Random forest, logistic regression, support vector machine algorithms are analyzed for credit card extortion identification. Various creature replicas together blender form a hybrid replica. Hybrid replica comprises of multilayer perceptron neural system,support vector machine(SVM),logistic regression model(LOR) and harmony search (HS) headway is used for corporate duty avoidance. Harmony search helps in finding the best parameters for the course models.

The true world dataset is used for detection. In majority voting method casting a ballet is the dominant part for which most of the time is utilized for information grouping which includes joined models that involves more like two calculations. This method is used to upgrade execution using various kinds of calculations. The majority voting method and Adaboost method gives strong performance and robustness.

Apapanpumsirirat et.,al.(2019), proposed the detection of online transaction fraud using unsupervised learning algorithms.Thismethod mainly aims to detect fraud that a supervised algorithm cannot detect. It focuseson creating deep auto-encoder and restricted Boltzman machine that reconstructs normal transactions which find anomalies from the normal patterns. This unsupervised algorithm applies backpropagation by setting input equals to output. RBM comprises of two layers i) input layer(visible) ii) hidden layer. Using AE, the bank transfers the input which is the amount of time, money, date, location and the other information. The AE uses past behavior to be trained first and then uses the new transaction as a validation test for the transaction. RBM uses all the transactions from acquiring the bank as an input and then reconstructs the model by transferring the new input from the activation function back to the output.

Dr. S. Geetha et., al. (2018),describes the credit card fraud detection using Bayesian network. It uses ASP.NET to create web-based applications and SQL servers to store and retrieve data. Almost all the time the real card-holder doesn't know that someone else has seen or stolen his card details. The only way to overcome this problem is to analyze the security details given by registered users of this site. Every card-holder exhibit behavior pattern like typical purchase category, time since the last purchase, location, etc. any large deviation from such patterns indicates that fraud being committed or there is a threat to the system. Using this technique, we can get the most accurate detection.

C.Sudhaet., al. (2018), creditcard frauddetection using K-Nearest Neighbor algorithm. This method proves accuracy in minimizing false alerts. The key perception is to analyze the spending actions of the user. Address matching is done if the billing address and shipping address are found the same, then the transaction is presumed to be genuine or else it is considered as a fraudulent transaction. But the customer might order a product to the different address or maybe to his friend, this shows that customer's behavior changes constantly. Soin this paper, the main objective is to identify fraudster behavior and then detect new kinds of frauds. This is a debauched method along with high false alerts.

Dahee Choi et., al.(2018),describes "An artificial intelligence approach to financial fraud detection under IoT environment" refers to the unauthorized use of mobile transactions uses mobile platforms through credit card stealing to obtain money illegally. It suggests a new detecting method by using both supervised and unsupervised learning algorithms. It aims to discover hidden behaviors. This model consists of data preprocessing, sampling, feature selection, application of classification and clustering algorithm based on machine learning. This model was validated using a real financial transaction dataset occurring in Korea,2015.

II. RELATED WORK

Globalization has set up more and more arduous monetary in addition to political interdependencies and offers inhibited simple assumptions pertaining to sovereignty furthermore, the function of nation-state [1]. The newest authentication and essential comprehension designismaking use of smart flash remembering flash memory cards. To satisfy the OTP requirement for credit card-holders, the smart flash remembering flash memory card has become an important gadget [2]. Lately, the accessible version of Urban Audit statistics started to have the ability to assess the components finding out the complete functionality of smart urbanized facilities on credit card focus [3]. Much more helpful technique is merging two or perhaps element authenticator to relish benefits within safeguard as well as hassle-free of credit card. This will likely guard us for instance from biometric fabrication by changing the end-user specific credential, and that is as simple as turning the token which has the arbitrary info [4]. Receptors are usually directed over to monitor an assortment of issues, such as data attack, money,and pressure through computational electrical capacity in between automated machines and the person aided by the face recognition. Wise effort is a future-oriented work environment to deliver quick internet business transactions and handy for owners. For households as well asdifferent internationalnations, it is now prompting the launch of wise labor [5]. To be shielded dull as soon as the primary key component or perhaps password shared between two individuals is yanked as an outcome associated with a small cluster of values. The main goal of password-based authenticated essential exchange protocols is limiting the adversary for this particular circumstance simply [6]. To provide a clear option for this particular problem. Systematically have a look at the organic conflicts as well as inescapable tradeoffs among the crucial components [7]. Figuring out an essential way in addition to hinting exploration agendas relating to cities since they invest cash on new ways to become "smart."; Identify and also discuss troubles, accomplishment pieces, and even impacts of credit card [8]. Employing this particular suggested model, the authentication of Citizen is attained from the tactful electric signatures, and also that's the main crucial part of electric accreditation. The suggested software program technique key in a strong item-oriented point of view, and correct gain access to management mechanism, isthe demand on the hourbecause the information kept within the storage area has to be shielded properly [9]. A great deal of concentration continues to be obtained by the utilization of public significant encryption to provide secured local community interaction. Algorithmsand characterizations that might be used to ascertain method defense within the models, are supplied and also the storage space capability could extremely be enhanced with the usage of the credit card. Cloud computing is a supple, economical as well as confirmed shipping and delivery wedge for offering services with a credit card. [10]

III. PROPOSED APPROACH

We proposed a new method to identify the credit card fraud detection based on the location where the person utilizes the credit card. The credit card transaction of money is done by a person. Throughout the transaction, the server is going to save the info like location and amount out of the location where the transaction happens. In case a transaction happens from a new place, the server transmits the info to credit card consumer for the next fitness level authentication. When the next fitness level authentication is completed thetransaction happens therefore, we are able to stay away from credit card fraud.

Toidentify the fraud transaction, server have to record operator transaction information such as transaction prepared area, merchant title, and then the quantity of transaction that will process according to the server information.

A. Account Creation & Server Authentication

Original card user needs to build the own account of his and register the credit card detail of his within the server. As soon as the server purchase the end-user, server is going to provide pin quantity to the end-user to use the credit card and also stuff which info on repository server. The data source server is going to maintain the end-user individual information and also most of the transaction information which is approached by the person. In order to confirm the person is genuine card user, the server is going to send an OTP to Cardholder's e-mail id. Once the OTP has confirmed the cardholder's bank account development system will be finished.

B. Generating Transaction Data

Original card user has to offer a bit of transaction information after the server approves the transaction which info is going to be packed towards the repository server. The info which is packed within the data source server is the transaction info such as area, merchant, amount, just about all the information will be packed within the server according to the distinctive id on the flash memory card quantity. The prototype of the project of ours involves a movable program in which flash memory card user is able to choose the preferred spot and also choose their ideal groups. In line with the selected class listing of merchants will likely be shown with the assistance of Google API.

C. Identifying the Transaction

To determine the fraudulent transaction, server will cross confirm the transaction which has long been prepared through the person, server is going to verify all the previous transactions done by the card-holder. If the current transaction is done in the same place, no issue will be raised. When transaction is being done in some other different location other than those locations that are stored in the server, then multilevel authentication will be elevated. The server is going to verify all of the pastinformation to determine the end-user transaction. Throughout the transaction method as whenever a person taps the card of theirs for a fee, the Server of ours will begin filtration system using the prior transaction information with the present transaction information. In line with the variants in every single key element, multilevel authentication is going to be brought on.

D. Multilevel Authentication

For each transaction,server will cross confirm the standing end-usertransaction with the transaction pattern, any deviation from the pattern takes place in a different location, it subsequently raises serious concern to look into the transaction as next degree of authentication and sends OTP to the registered mobile number. By asking confirmation towards the end-user in case if the person verify the identity then the transaction will proceed or else server will blockthe transaction.

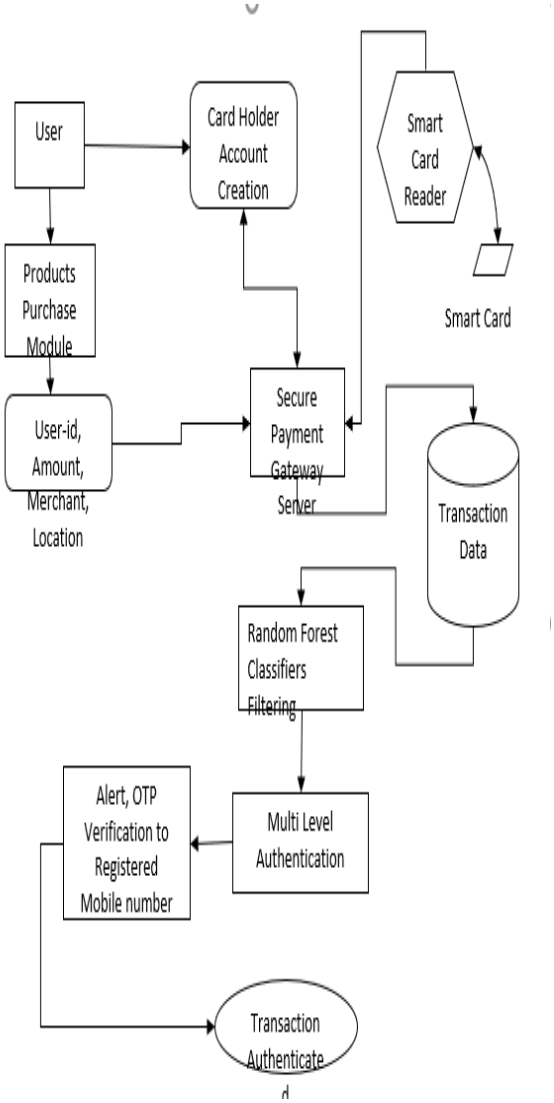


Fig. 1 Architecture Diagram

IV. EXPERIMENTAL RESULTS

The experiments are performed using the TOMCAT 7.0 and MYSQL 5.0 version. The computations are performed using Toolbox that is readily available in TOMCAT. In Fig. 2, user login screenshot, here user can give their register account name for getting entry into the transaction with OTP.

Parameters	Existing System	Proposed System
Utilization of Server	Low	High
Penetration of intruder	More chances	Less chance
Accuracy Rate	Less	More

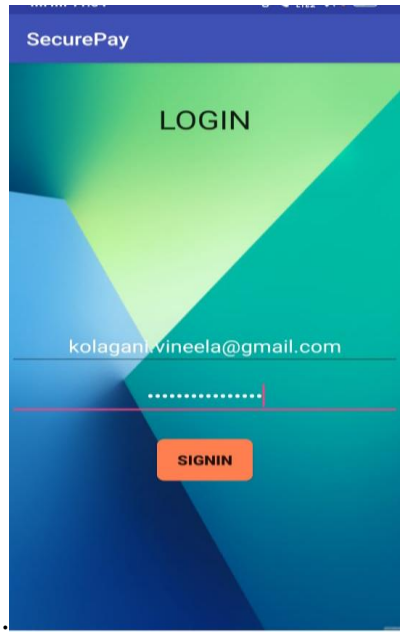


Fig. 2 Register with OTP

After getting registered with OTP, the customer will perform the transaction.

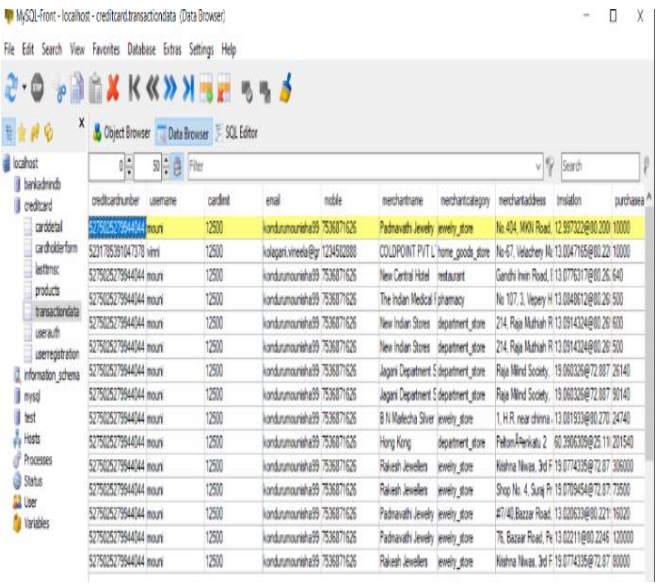


Fig. 3 Detection Process

Fig.3 shows the fraud detection system for securing the credit card details with previous data. Fig. 4 shows the second-level authentication. The data are then trained with a proposed scheme which is widely used for all techniques. Some databaseis kept for training and the rest are kept for testingthe proposed schemes. Hence the result satisfies the expected output, achieving the security level on comparing with the existing model.

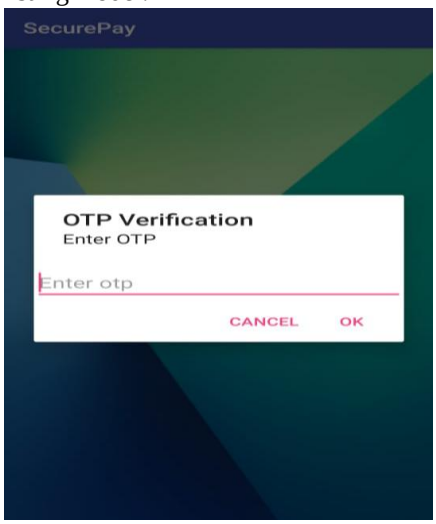


Fig. 4. Second-level Authentication

When theentire verification process is completed, a transaction completed message is shown as below.

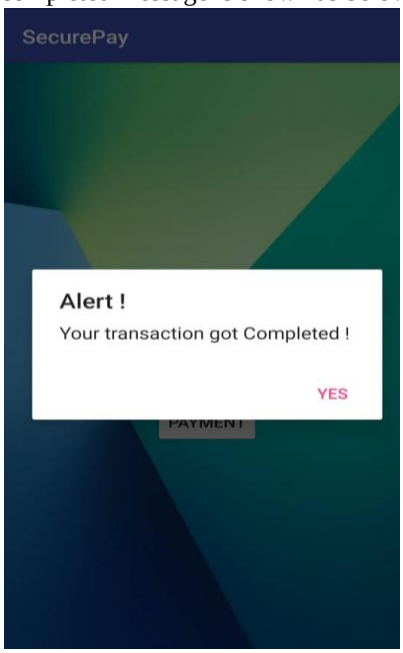


Fig. 5. Transaction success

V. CONCLUSION

Credit card data management offers to help small to moderate businesses and people to shift the conventional data of their dependent authentication systems to far more protected transactions. Protection and confidentiality difficulties of migrating the securityprogram on the credit card data are recognized sensibly. Attainable imperfections and the effects are talked about.

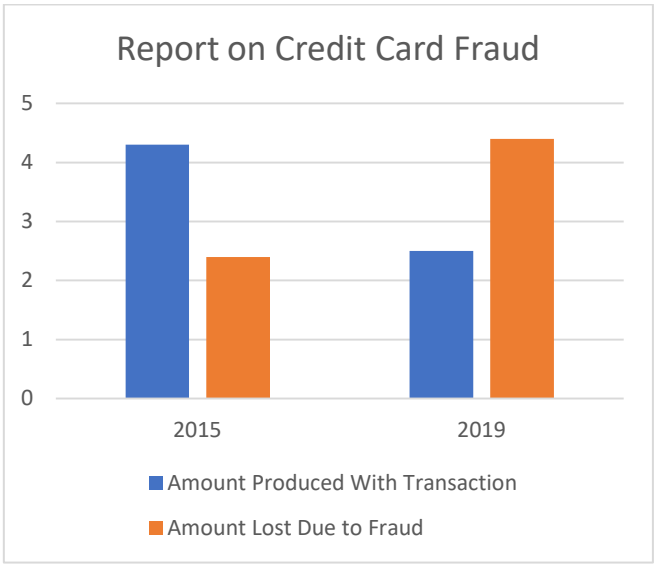
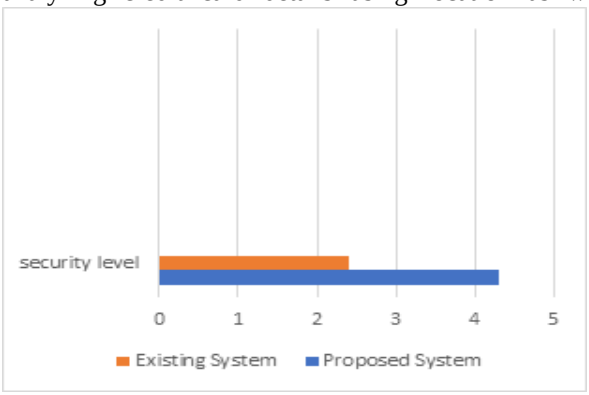


Fig.7. Nilson Report

Safety measures & sensible remedies have been claimed. It must be pointed out that the suggested structure doesn't try to resolve the weaknesses of traditional username/password use like learning vulnerability or problem against wondering strikes. Hence, we have proved the security level on analyzing credit card details using location as well as



amount of money. Our project has obtained 99% accuracy rate.

Fig.6. Security Level

REFERENCES

1. Fang, Y., Guo, Y., Huang, C., & Liu, L. (2019). Analyzing and Identifying Data Breaches in Underground Forums. IEEE Access, 7, 48770-48777.
2. Andringa, M., Glau, L., & Slaton, J. (2019). U.S. Patent No. 10,445,837. Washington, DC: U.S. Patent and Trademark Office.
3. [3]Mayhew, K., & Chen, W. (2019, May). Blockchain-Can It Solve the Security Issues and Fraud Expenses for Credit Card Commerce? In 2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing,(HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS) (pp. 37-41). IEEE.
4. Tomeo, M., Mutale, W., Scarpino, J., & Cottrell, L. (2019). A Comparative study analyzing computer programming college students'pre-knowledge and post-knowledge of software application security using OWASP. Issues in Information Systems, 20(2).
5. Kim, B., Johnson, K., & Park, S. Y. (2017). Lessons from the five data breaches: Analyzing framed crisis response strategies and crisis severity. Cogent Business & Management, 4(1), 1354525.
6. Graves, J. T., Acquisti, A., & Christin, N. (2018). Should Credit Card Issuers Reissue Cards in Response to a Data Breach? Uncertainty and Transparency in Metrics for Data Security Policymaking. ACM Transactions on Internet Technology (TOIT), 18(4), 1-19.
7. Cohen, M. C. (2018). Big data and service operations. Production and Operations Management, 27(9), 1709-1723.
8. Curtis, S. R., Carre, J. R., & Jones, D. N. (2018). Consumer security behaviors and trust following a data breach. Managerial Auditing Journal.
9. Choi, H. S., Lee, W. S., & Sohn, S. Y. (2017). Analyzing research trends in personal information privacy using topic modeling. Computers & Security, 67, 244-253.
10. Muttoo, S. K., Gupta, R., & Pal, S. K. (2016). Analysing Security Checkpoints for an Integrated Utility-Based Information System. In Emerging Research in Computing, Information, Communication and Applications (pp. 569-587). Springer, Singapore.

AUTHORS PROFILE

Vineela K, currently pursuing her B.E in the School of Computing from Sathyabama Institute of Science and Technology, Chennai, Tamil Nadu, India. Her research interests include areas of Machine Learning, Internet of Things, Cloud Computing.

Mounisha K, currently pursuing her B.E in Computer Science and Technology at Sathyabama Institute of Science and Technology, Chennai, Tamil Nadu, India. Her research areas include Machine Learning, Cyber Security.

Dr S. PraylaShyry, currently working as Professor in the department of Computer Science and Engineering at Sathyabama Institute of Science and Technology. She acquired her M.E from Annamalai University and Ph.D from Sathyabama University in the year 2014. She has also been a reviewer in reputed journals. She has also published more than 45 national, international journals and conferences. Her area of specialization includes Cyber Security, Network Security and Artificial Intelligence, Overlay Networks, Machine Learning. She has also published patents and many products.