Detecting Fraud in Transactions Using Diversity in Behavior

Y. Dasaratha Rami Reddy[1], T.Poovizhi[2]

1,UG Student, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, India
2,Assistant Professor, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai India.
3,Assistant Professor, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai India.

Email: dasarathreddy7723@gmail.com,poovizhit.sse@saveetha.com,ndeepa.sse@saveetha.com

Abstract: Transaction fraud is predominant nowadays as many people prefer shopping through online. This made the research on detecting fraud to become an important part of research at present times. Based on records of transaction of several users, B_p (Behavioral Profile) is extracted and then verification takes place in order to find the frauds occurring. Usage of Markov models does not give relevant results, thus making unsuitable to use in such scenarios. Attributes from several transaction records are classified in the proposed system to represent a graph like structure. The probability of path from one attribute to another is calculated along with computation of diversity of several different users behaviors in transaction. For every user a B_p is constructed and is verified whether the transaction is allowed incoming or not to detect the fraud. The experimental results show the efficacy of the system.

Keywords: Behavior Profile, Markov model, Online shopping, Transaction

1. Introduction

Online shopping increased the amount of electronic transaction in the industrial world nowadays. E-commerce market also keeps on increasing the net worth as it may reach heights by the year 2020. For shopping things online, credit cards are also been utilized also including the online transaction methods like Paypal. This also causes fraud in transaction thereby affecting the users always. Compared to frauds that occur offline, online frauds are more and also people suffer a lot. While doing shopping online, presence of a card is not necessary. A fraudster needs only the card related information in order to fake the user.

In case of misuse identification, signatures which are fraudulent are collected and stored as a database. Several methods like logistic regression as well as neural networks are also utilized to obtain the patterns. In case of detecting the anomaly, user profile pattern is extracted from their usage of transactions. B_p which is termed as behavior profile is a model that depicts different behavior of several users. Markov models are also used to depict the B_p based on the attributes involved in the transaction. The different behaviors of users is taken into account when a new model is designed and our model focuses on that. Attribute value classification is performed in the proposed system from which a graph is represented to indicate the various transaction records.

The paper is organized as follows: Section 2 deals with literature review, Section 3 presents the proposed system, Section 4 discusses the results obtained from the system and finally Section 5 concludes the paper.

2. Literature Review

The methods available in literature for detecting fraud can be classified as the ones detecting the misuse and the other ones detecting anomalies. Each transaction is identified by an authenticated signature from the user. If the signature is not valid, then the transaction is declared to be invalid. Several methods have been used to obtain the patterns in fraud such as neural networks or logistic regression and so on. As individual attention is missing here, this method was not used predominantly by many users.

In order to provide individual attention for each user the pattern of each user in terms of transaction is extracted and used to find behavior profile (B_p). With this profile, the acceptance ratio of each transaction is calculated. Thus the method can be used by several users due to its feasibility

Hongyu Wang etal. discussed about prominence of Master-card has extraordinarily sped up the exchanges among vendors and cardholders. Be that as it may, Master-card extortion has been inferred, which finishes in misfortunes of billions of euros for each annum.

As of late, AI and information preparing innovation are wide used in misrepresentation location and accomplished positive exhibitions. The vast majority of those examinations utilize the innovation of under-inspecting to shake the high awkwardness of Master-card data.

Ankit Mishra et al discussed about nowadays, as net speed has augmented and therefore the costs of mobile have attenuated a great deal in past few years. Conjointly the information costs too square measure a great deal cheap to most of the individuals. This has resulted into the digitisation of most of the institutes because it is simple and convenient for the individuals and conjointly for the authority to take care of the records. So, it resulted in most of the banks and alternative institutes receiving and transferring cash through credit cards.

3. Proposed System

Transaction records for several users need to be represented in a table format. Pre-processing starts from the original data itself where the items are classified and segmented as groups first. One of the main factor to be considered while classification is transaction time of records with respect to users available during the transaction. Each user may have variations in their time of transacting records. Also the location of transaction is also noted with the time of activity taking place, for example either in the morning or in the evening. The relation dependency of values of attributes need to be noted along with the transaction record of each user.

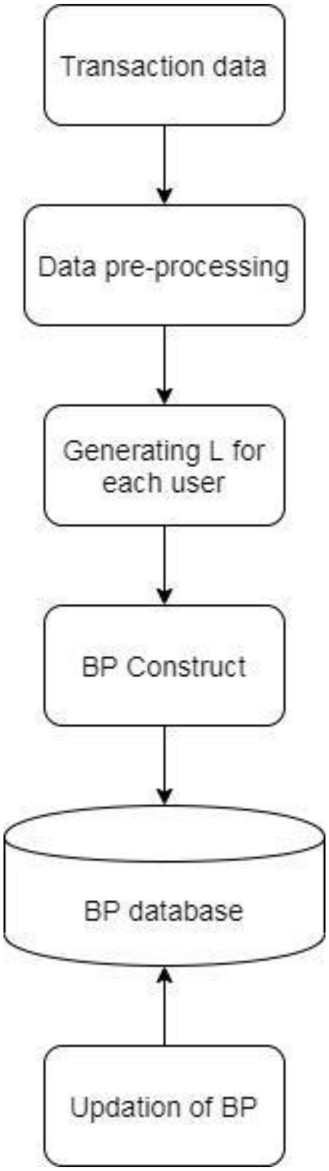

Fig.1. Updation of BP

4. Results and Discussion

The transaction attributes of several states has been represented in the following Table.1.

Table 1: Transaction Attributes

Fraud record	Fraud transaction attributes				
	Time	Location	Category	Money	Address
Record1	Fn	Chennai	DR	10000	CH
Record2	Fn	Delhi	OD	15000	DL
Record3	An	Banglore	SD	2000	BL
Record4	Fn	Manglore	OD	30000	ML
Record5	An	Chickmagulur	DR	15200	CML
Record6	Fn	Pune	SD	60000	PN
Record7	Fn	Mumbai	DR	12000	MBI
Record8	An	Satara	OD	18000	STR
Reord9	An	Sholapur	SD	25000	SLR
Record10	Fn	Amritsar	SD	52000	AMT

Where
DR= door delivery, OD= office delivery, SD= school delivery, in address CH=Chennai, DL=delhi, BL=banglore, ML=manglore, CML=chickmagulure, PN=pune, MBI=mumbai, STR=satara, SLR=sholapur, AMT=amritsar

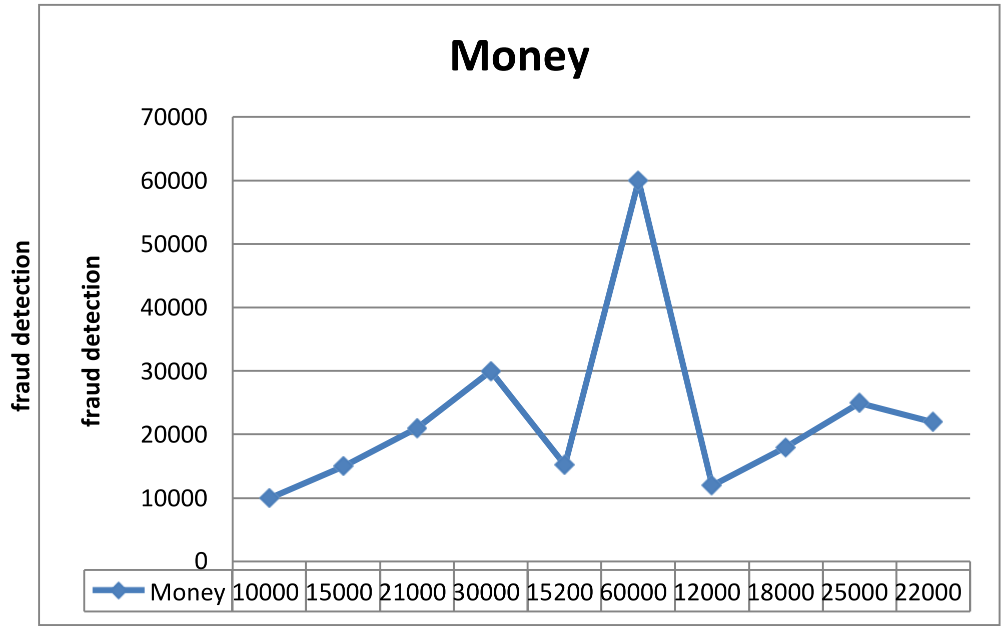

Fig.2. Behavioral Changes

This graph shows the data of money of fraud detection. Upto 60000 has recorded in the fraud transaction. At lowest 10000 has been record.

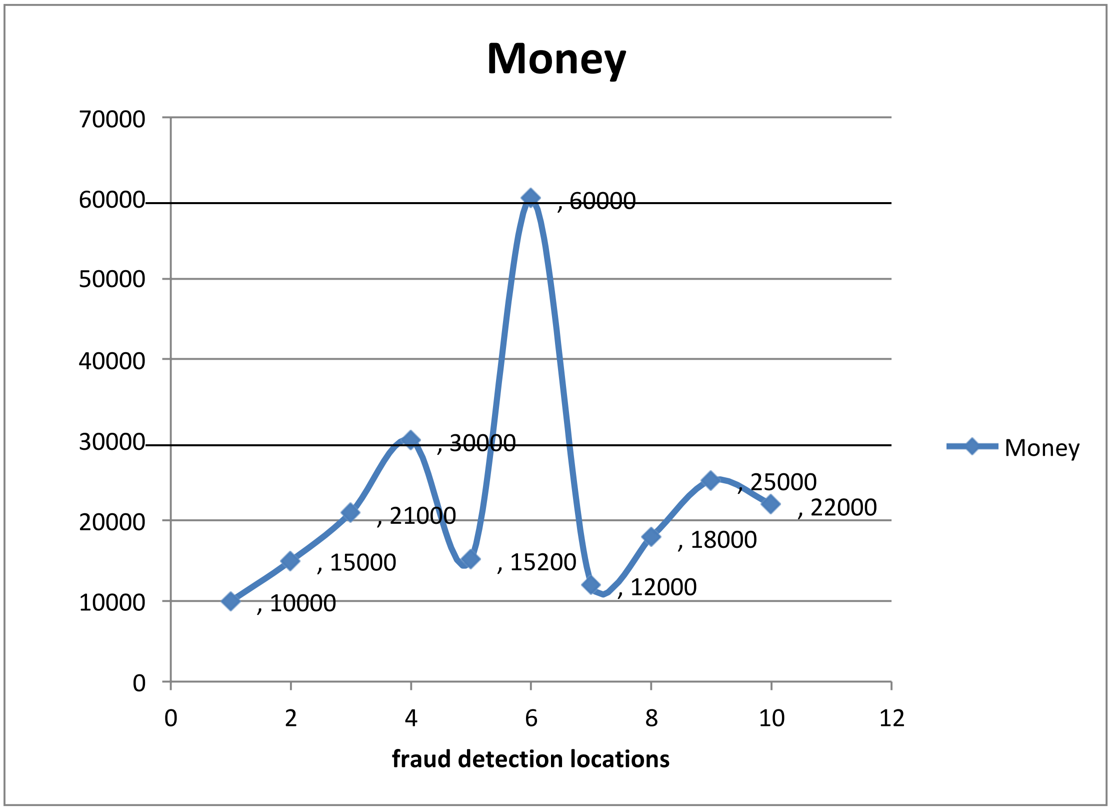

Fig. 3 Location changes during transaction of several users

This graph shows the data between fraud detection location and money. This graph shows the range of money has been faced by fraud. Pune is in the higher percentage in fraud transactions. It is mostly done in FN. As compare to other cities Pune is at higher and Manglore is at second place. Very less fraud transactions has been done in Chennai.

5. Conclusion

In this paper to detect transaction fraud in online shopping scenario we used a method to find BP of users basing on their transactional records. The diversity of user behaviors is characterized in Markov chain model is overcome by our model. By the experiments we can illustrate the advantages of our method. To characterize the personal behavior of users we use machine learning methods. It can classify the transaction attributes. Based on user comments we plan to extend BP considerations.

6. References

[1] W. van der Aalst, T. Weijters, and L. Maruster, “Workflow mining: Discovering process models from event logs,” IEEE Trans. Knowl. Data Eng., vol. 16, no. 9, pp. 1128–1142, Sep. 2004.

[2] A. Abdallah, M. A. Maarof, and A. Zainal, “Fraud detection system: A survey,” J. Netw. Comput. Appl., vol. 68, pp. 90–113, Jun. 2016.

[3] N. Abdelhamid, A. Ayesh, and F. Thabtah, “Phishing detection based associative classification data mining,” Expert Syst. Appl., vol. 41, no. 13, pp. 5948–5959, 2014.

[4] N. M. Adams, D. J. Hand, G. Montana, D. J. Weston, and C. W. Whitrow, “Fraud detection in consumer credit,” Autumn, vol. 9, no. 1, pp. 21–29, 2006.

[5] C. Arun, “Fraud: 2016 & its business impact,” Assoc. Certified Fraud Examiners, Austin, TX, USA, Tech. Rep., Nov. 2016.

[6] A. Azaria, A. Richardson, S. Kraus, and V. S. Subrahmanian, “Behavioral analysis of insider threat: A survey and bootstrapped prediction in imbalanced data,” IEEE Trans. Comput. Social Syst., vol. 1, no. 2, pp. 135–155, Jun. 2014.

[7] V. Bhusari and S. Patil, “Application of hidden Markov model in credit card fraud detection,” Int. J. Distrib. Parallel Syst., vol. 2, no. 6, pp. 203–210, 2011.

[8] R. Brause, T. Langsdorf, and M. Hepp, “Neural data mining for credit card fraud detection,” in Proc. IEEE Int. Conf. Tools Artif. Intell., 1999, pp. 103–106.

[9] T. Carter, An Introduction to Information Theory and Entropy, S. Fe, Eds. CiteSeer, 2007.

[10] R. C. Chen, S. T. Luo, X. Liang, and V. C. S. Lee, “Personalized approach based on SVM and ANN for detecting credit card fraud,” in Proc. Int. Conf. Neural Netw. Brain, Oct. 2005, pp. 810–815.

[11] C. Cortes and D. Pregibon, “Signature-based methods for data streams,” Data Mining Knowl. Discovery, vol. 5, no. 3, pp. 167–182, 2001.

[12] V. Dheepa and R. Dhanapal, “Behavior based credit card fraud detection using support vector machines,” ICTACT J. Soft Comput., vol. 4, no. 4, pp. 391–397, 2012.

[13] S. G. Fashoto, O. Owolabi, O. Adeleye, and J. Wandera, “Hybrid methods for credit card fraud detection using K-means clustering with hidden Markov model and multilayer perceptron algorithm,” Brit. J. Appl. Sci. Technol., vol. 13, no. 5, pp. 1–11, 2016.

[14] Global Online Payment Methods: Full Year 2016, GmbH & Co. KG, Berlin, Germany, Mar. 2016.

[15] S. Gordon and R. Ford, “On the definition and classification of cybercrime,” J. Comput. Virol., vol. 2, no. 1, pp. 13–20, 2006.

[16] S. Gupta and R. Johari, “A new framework for credit card transactions involving mutual authentication between cardholder and merchant,” in Proc. Int. Conf. Commun. Syst. Netw. Technol., Jun. 2011, pp. 22–26.

[17] P. Hoffman and B. Schneier, Attacks on Cryptographic Hashes in Internet Protocols, document RFC 4270, 2005.

[18] C. Jiang, J. Song, G. Liu, L. Zheng, and W. Luan, “Credit card fraud detection: A novel approach using aggregation strategy and feedback mechanism,” IEEE Internet Things J., to be published, doi: 10.1109/JIOT.2018.2816007.

[19] W.-H. Ju and Y. Vardi, “A hybrid high-order Markov chain model for computer intrusion detection,” J. Comput. Graph. Stat., vol. 10, no. 2, pp. 277–295, 2004.

[20] A. Kundu, S. Panigrahi, S. Sural, and A. K. Majumdar, “BLAST-SSAHA hybridization for credit card fraud detection,” IEEE Trans. Dependable Secure Comput., vol. 6, no. 4, pp. 309–315, Oct. 2009.

[21] C. X. Ling, J. Huang, and H. Zhang, “AUC: A statistically consistent and more discriminating measure than accuracy,” in Proc. Int. Joint Conf. Artif. Intell., vol. 3, 2003,

pp. 519–524.

[22] J. Lopes, O. Belo, and C. Vieira, “Applying user signatures on fraud detection in telecommunications networks,” in Proc. Ind. Conf. Data Mining, 2011, pp. 286–299