Credit Card Fraud Detection System Using Bayesian Network

Nwanyanwu, M.
Department of Computer Science
Port Harcourt Polytechnic
Rumuola, Port Harcourt, Nigeria
E-mail: mercynthia201@gmail.com
Phone: +234-8063852487

Anireh, V.I.E
Department of Computer Science,
Rivers State University
Nkpolu – Oroworukwo, Port Harcourt, Nigeria
E-mail: anireh.ike@ust.edu.ng
Phone: +234 -8033229172

ABSTRACT

This study presents an application of Bayesian network to detect fraud in credit card. Rule-based filter was used to classify an incoming transaction as Genuine/fraudulent by address match/mismatch, and compute an overall belief value for each transaction. Bayesian network measures evidences and arrive at optimal decisions using Bayesian learner algorithm to output genuine transaction and fraudulent transactions. The credit card fraud detection system was implemented in Bayes server. Result showed that the system yield log likelihood, conflict, and evidence that measures genuine and fraudulent transactions, thus, the system produces more genuine transactions than fraudulent transaction.

Keywords: Bayes Server, Bayesian Network, Rule base Filter, Credit Card. Fraud Detection System, Dempster-Shaffer Adder.

CISDI Journal Reference Format
Nwanyanwu, M. & Anireh, V.I.E. (2019): Credit Card Fraud Detection System Using Bayesian Network. Computing, Information Systems, Development Informatics & Allied Research Journal. Vol 10 No 1.Pp 47-60 Available online at www.cisdijournal.org
DOI Affix - https://doi.org/ 10.22624/AIMS/CISDI/V10N2P4

INTRODUCTION

An e-commerce payment system aids the recognition of online payment for online transactions. Its payment systems have become progressively more popular due to the well-known use of the internet-based shopping and banking. In traditional systems the fraud is detected only when the billing for credit card is done. A rapid growth in the number of credit card transactions has led to a substantial rise in fraudulent activities. Occurrence of credit card fraud is increasing dramatically due to the exposure of security weaknesses in traditional credit card processing systems resulting in loss of money every year. Credit card fraud can be defined as the illegal use of any system or, criminal activity through the use of physical card or card information without the knowledge of the cardholder. There are factors that can lead to credit card fraud for example Skimming and Phishing, information sharing and lost or stolen card.

Patidar, R. & Sharma, L. (2011) defined skimming as the "process where the real data on a card's magnetic stripe is electronically copied onto another". Fraudsters use special-purpose devices also known as skimmers to capture the information of credit cards that are encapsulated inside their magnetic stripes. They can use the stolen card information to create counterfeit physical cards in order to use them at actual shops or simply supply the card information at online shops. Skimming can be committed by an unfaithful employee, who may swipe customer's card using the skimmer device, while the customer is at the point of sale. The proposed system will use Rule-based Filter, Dempster Shaffer theory and Bayesian network model to detect credit card fraud. Bayesian networks (BNs) are probabilistic models that merge probability theory and graph theory (Pearl, 1988). They are used to represent causal and probabilistic relations among random variables that are controlled by probability theory. Inferences that have probability and decisions that are optimal can be made directly from Bayesian networks.

The present day techniques are not efficient enough to track the sequence of credit card transactions and detect fraudulent transactions, as they were based on the old methods of banking. This led to using the combination of Rule-based Filter, Bayesian Network (BN) and Dempster Shaffer theory to detect credit card fraud. Many organizations and individuals request payment using credit card, this has increased credit card fraud. Therefore there is the need to ensure that transactions are secured for credit-card owners when using their credit cards to make electronic payments for goods and services provided on the internet.

2. RELATED WORKS

Over the years several methods have been used by researchers to detect credit card fraud. This work presents the review of literature on several techniques deployed in credit card fraud detection and the limitations of several techniques used in fraud detection in relation to the method proposed by the researcher. Bayesian network was first introduced by Cooper and Herskovits (1992) where Bayesian method was used to construct probabilistic network for database. Bayesian was applied in area of computer-assisted hypothesis testing, and automated expert system. Bayesian belief networks are statistical techniques in data mining. Bayesian networks are very effective for modeling situations where some information is already known and incoming data is unsure or partially unavailable (Philip & Sherly 2012). The aim of using Bayes rules is to correctly predict the value of a designated discrete class of variable given a vector of predictors or attributes (Joseph, 2011).

Bayesian Network (BN) represents a set of random variables and their conditional independencies using a directed acyclic graph (DAG). Nodes in Bayesian represents random variables or parameters while edges (lines) links nodes to each other showing their relationship (Ben-Gal, 2007) In particular, the joint probability density function of the random variables in a BN can be written as a product of the individual density functions, conditional on their parent variables (Russell *et al,* 2003). A Bayesian network is made up of two parts: a directed acyclic graph and a set of conditional probabilities. The directed acyclic graph signifies qualitative dependencies among random variables and the conditional probabilities measures these dependencies. Bayesian networks are usable in fields where there is need for prediction and outcome is uncertain. Instead of just 'guessing', Bayesian networks help its users make intelligent, quantifiable and justifiable decisions (Lin *et al* 2013).

Bayesian networks have been used to model gene expression data (Chai *et al* 2014) and gene regulatory networks (Cho *et al* 2016, Xiao *et al,* 2016, and Wang. *et al* 2013) Different variations of the BN model have been used to analyze gene expression data (DeCampos *et al* 2009), including the naïve Bayes classifier (Osareh *et al* 2009), the Bayesian network augmented naïve Bayesian classifier (BAN) (Bosin *et'al…,* 2005), the k-dependence Bayesian classifier (KDB) (Armañanzas *et al,* 2008), and the general Bayesian network model (Hwang *et al* 2002). In this study, we used a general Bayesian network in which each node is an observed random variable that models the expression value of an Eigen gene.

The popularity and recognition gained by Bayesian Network (BN) in combating fraud is as a result of its application of Artificial Intelligence (AI) techniques and algorithms that can be implemented to detect or predict fraud through Knowledge Discovery from unusual patterns derived from gathered data. This is of great importance and has serious application in this design. Bayesian Networks are nowadays well established as a modeling tool for expert systems in domains with uncertainty (Zheng, 2016). Reason was because it is powerful tool, but conceptually transparent representation for probabilistic models in terms of a network. Their graphical representation, showing the conditional independencies between variables, is easy to understand for humans.

Sam *et al* (2002) used Bayesian network for credit card fraud detection. They constructed two hypotheses; firstly Bayesian network was used to model behaviour that assumed to be fraudulent and the second model a behaviour that is assumed to be genuine. The fraud network was set up using Expert system. The condition for detecting, predicting and reporting fraud has greatly increased as a result of Bayesian Network used to analyzed large datasets which might not be picked up by human analysts (Yue 2007). This recent revolution means that technologies such as voice recognition or image processing, which only a few years ago were performing at noticeably below-human levels can now outperform human at specific tasks (Markoff,2015).

Mukhanov (2008) used Bayesian Belief Network to detect fraud in credit card. In his work, he used the naive Bayesian classifier and Bayesian network where he applied the Rissanen's minimal description length principle which is based on quantitative characteristics. He developed a clustering algorithm to store all observed values needed. The result of his research shows that Bayesian network yielded a higher accuracy than the naive Bayesian classifier. Sam *et al* (2002) in their research work applied Bayesian and Artificial Neural Network (ANN) to detect fraud in credit card. They used the back propagation of error signal algorithm. In the ANN, they had three layers: the one that receives input, the one that is hidden and the one that connects the network to the outside world. The result of the work was high accuracy. The Bayesian network yielded a better result with reduced training period. Kadar *et al* (2018) constructed Bayesian Network using dataset of mobile payment which was created by PaySim simulator. They used variables like name of customers, initial balance of customers before and after transaction, the destination of transaction etc. the data was clean to remove inaccuracies, Greedy algorithm was used to speed up search. The result of the research gave 87% accuracy.

OngShu Yee et al (2018) proposed Bayesian Net Classifier, K2, along with other tools in their research work for fraud detection. They employed machine learning as data mining technique. They achieved 95% accuracy.
Several techniques have been applied in credit card fraud detection, but this study focused on using the Bayes server tool to implement the dataset derived.

3. METHODOLOGY

A. System Design

Agile software design methodology was applied in the study. Agile software design is a combination of iterative and incremental process models with focus on process adaptability and customer satisfaction by rapid delivery of working software product. Agile Methods break the product into small incremental builds. These builds are provided in iterations. Each iteration typically lasts from about one to three weeks, this will be used in Rule-based filter, Bayesian Network and Dempster-Shaffer model.

B. Data collection

Secondary data collection is adopted in the research due to unavailability of raw data from financial institutions. The credit card information for online shopping was gotten online from different domain and from users of credit cards.

4. ARCHITECTURE OF THE SYSTEM

The Fraud Detection System (FDS) consists of four components: Card Information, Rule-based filter (RBF), Dempster-Shafer adder (DSA), Bayesian Learner (BL). Rule-based filter consists of generic as well as customer-specific rules which classify an incoming transaction as fraudulent with a certain probability. This layer can have rules R1 “Address mismatch” and rule R2 “Outlier detection”. The role of the DSA is to combine evidences from the rules R1 and R2 and compute an overall belief value for each transaction. Bayesian learner is a tool to measure evidences supporting alternative hypotheses and arrive at optimal decisions. The proposed system architectural design is shown in figure1.

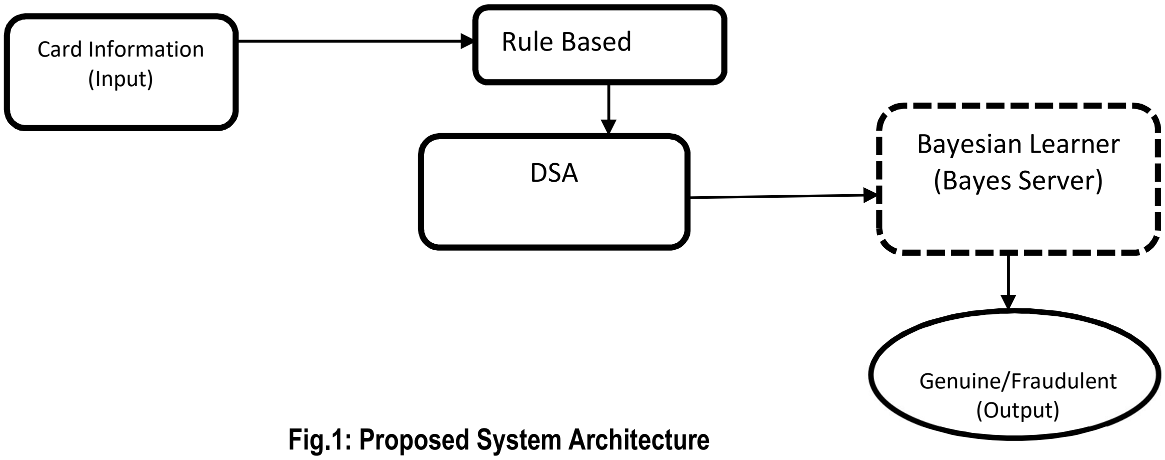


Fig.1: Proposed System Architecture

A. Card Information

The card information consists of all the information on the card. This information is used when carrying out any transactions with the card, which means, any incorrect information supplied by the user will make the transaction not to be successful. Such information like: name, card number and CVV are unique per user.

B. Rule Base Filter

The Rule Base Filter (RBF) is made up of generic as well as customer-specific rules which sort an incoming transaction as fraudulent with a certain probability. It quantifies the extent to which the transaction’s behavior moves away from the normal profile of the cardholder. This layer can have rules like average daily/monthly spending of a customer, delivery address being different from billing address. RBF uses Address Mismatch and Outlier Detection.

Address Mismatch

One of the basic rules that any purchase transaction, especially internet transaction, is subjected to, is to verify if the delivery address is the same as the billing address of the cardholder. Although we cannot declare a transaction to be fraudulent with certainty whenever this rule is violated, any transaction that satisfies this rule can be classified as genuine with a very high probability (except for the cases where the fraudster’s aim is only to attack the cardholder). The transactions that violate this check are labeled as suspect with weight W_a, which can be user-defined.

We can use the rule form of say:

R1 = Delivery address ≠ billing address - - - - - (1)

Outlier Detection

Since a customer is likely to follow a particular pattern or carry out similar kind of transactions, these can be visualized as part of a group or a cluster. Similarly, since the fraudster is likely to deviate from the customer's profile, his transactions can be detected as exceptions to the cluster, a process also known as outlier detection.

Density Based Spatial Clustering of Applications with Noise (DBSCAN) is a recently proposed density based clustering algorithm (Ester et al., 1996; Han and Kamber, 2001) in which for each point in a cluster, the neighborhood of a given radius has to contain at least a minimum number of points, that is, the density in the neighborhood has to exceed a certain threshold. And our rule 2 will have the form say:

R2 = Transaction amount > max specified limit - - - - (2)

For any credit card transaction, the possible attributes are transaction amount, billing address, shipping address and inter-transaction time gap. A transaction $T_{jp}^{Ck}$is detected as an outlier if it does not belong to any cluster in the set C

Such an observation gives evidence that the transaction could be fraudulent. We measure the extent of deviation of an incoming transaction by its degree of outlierness. If the average distance of the amount p of an outlier transaction $T_{jp}^{Ck}$from the set of existing clusters in C is v_{avg}, then its degree of outlierness $d_{outlier}$ is given by:

$$d_{outlier}= \begin{cases} 1 - \frac{\varepsilon}{v_{avg}} if\ |N_{\varepsilon}\ (p)| < MinPts \\ 0 \end{cases} \quad - \quad - \quad - \quad - \quad - \qquad (3)$$

Where MinPts is the minimum number of points required in the e-neighborhood of each point to form a cluster and Ɛ is the maximum radius of the neighborhood

$$N_{\varepsilon}\ (p) = \{q \in D | dist(pq) \leq \ \varepsilon\} \quad - \quad - \quad - \quad - \qquad (4)$$

Thus, the ''Address Mismatch" rule as R1 and the ''Outlier Detection" rule as R2 and the Rule-Based Components are the Customer-specific rules and Generic rules which are: "Delivery address ≠ billing address" and "Transaction amount > max specified limit".

C. Dempster-Shafer Adder (DSA)

DSA combines evidence from the rules R1 and R2 and compute an overall belief value for each transaction. It offers a rule for computing the confidence measures for genuine transaction and a transaction that is suspicious (unknown) based on data from new as well as old evidence. Dempster Shaffer Theory (DST) is a mathematical theory of evidence based on belief functions and credible reasoning. For every incoming transaction T_{jp}^{Ck} , the rules R1 and R2 give their independent observations about the behaviour of the transaction. It gives a numerical procedure for joining together observations from the rule-based filter to compute an overall belief for a transaction.

Two basic probability assignments m_1 (h) and m_2 (h) are combined into a third basic probability assignment m (h) as follows:

$$m(h) = m_1\,(h)\ \oplus m_2(h)\ = \frac{\sum_{x\cap y=h} m_1(y)}{1-\sum_{x\cap y=\emptyset} m_1(x) * m_2\,(y)} \qquad - \qquad - \qquad (5)$$

For any suspicious transaction T_{jp}^{Ck} given as
U = {fraud, ¬ fraud}
If Hypothesis h = {fraud}
It implies that transaction T_{jp}^{Ck} is fraudulent.

Hypothesis ĥ = {¬fraud} - - - - - - - (6)

It implies that transaction T_{jp}^{Ck} is not fraudulent.

Transaction Database History

Transaction database history keeps records of both fraudulent and genuine transactions. It keeps transactions history for individual customers from their past behavior. The information stored includes: card numbers, transaction amount and time since last purchase. The transaction amount information in the Transaction History Database is required for detecting outliers. To capture the frequency of card use, the time gap between successive transactions on the same card must be considered.

D. Bayesian Learner (Bayes Server)

Bayesian learning is used to measure evidences supporting alternative hypotheses and arrive at optimal decisions. This is used to update the suspicious score (which is the probability that the transaction is fraudulent) of a transaction in the light of the new evidence from the transaction of the database history. By using Bayes rule to determine whether fraud occurs, we output the hypotheses h: fraud and ĥ: ¬fraud. Figure 3 is the Bayesian Network for an online transaction

5. USE-CASE DIAGRAM OF THE PROPOSED SYSTEM

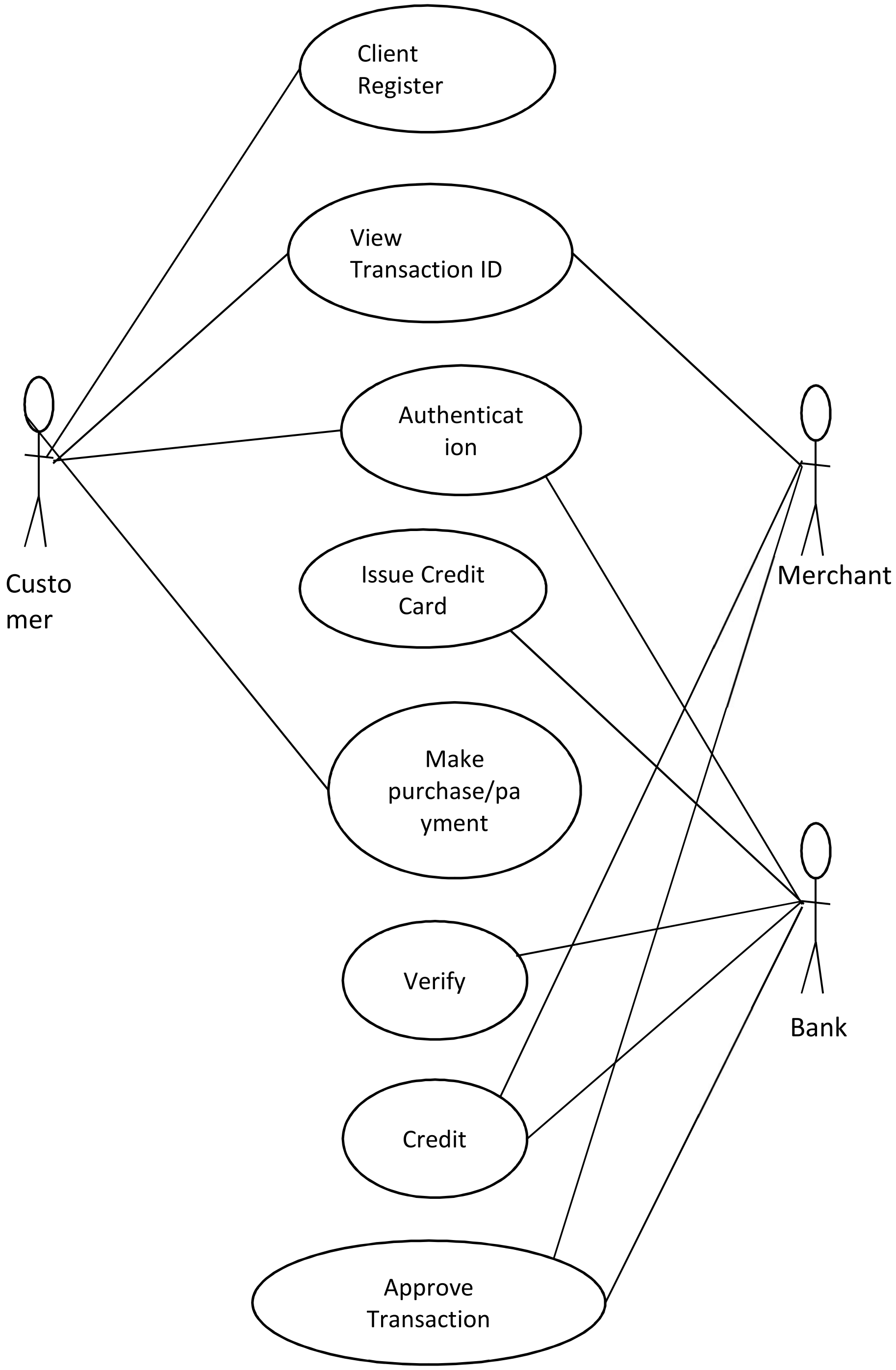


Fig.2: Use-Case Diagram of the proposed system

6. BAYESIAN GRAPH OF THE PROPOSED SYSTEM

The Bayesian Network has nine nodes indicating the link between each node. Computer Related Purchase can make Internet Purchase.

The figure 3 below shows the Bayesian Network for an online transaction using credit card for purchase.

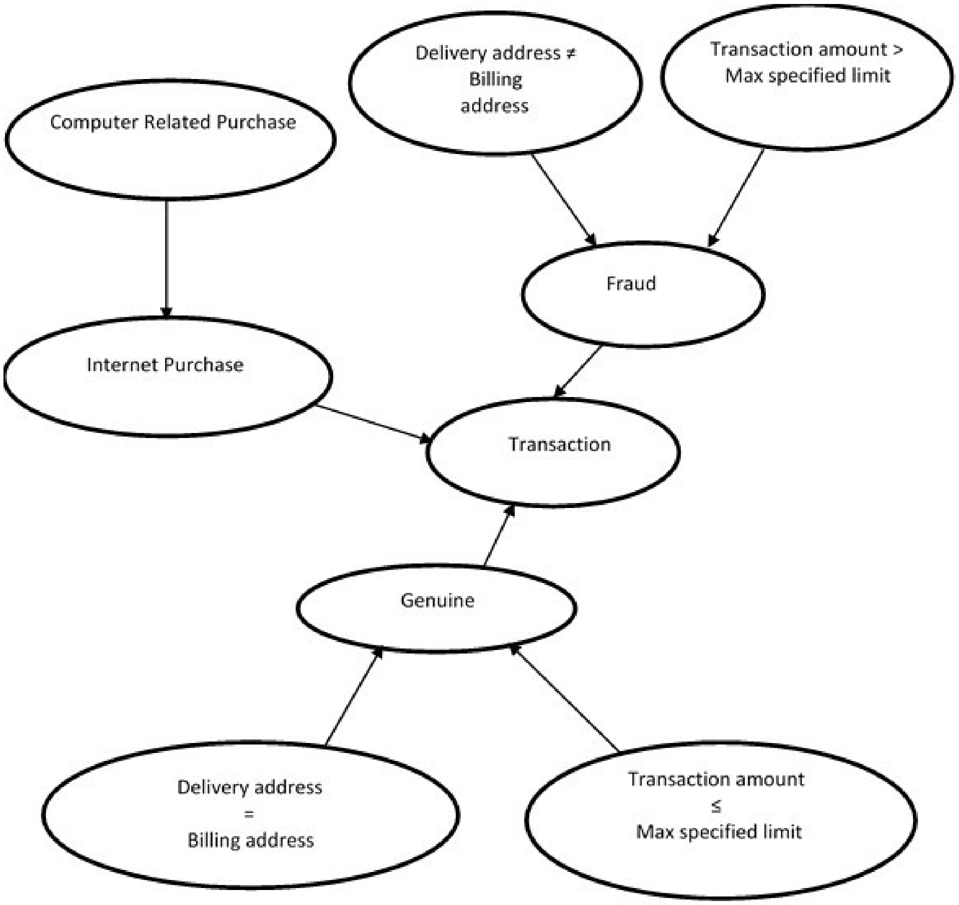


Figure 3: Bayesian Network for Online Transaction of the proposed system

Each Internet Purchase is a transaction that could be Genuine or Fraudulent.

Using the graph of expected causes, we can check for conditional independence of the following probabilities given;

P (Transaction) = [Internet Purchase, Genuine, Fraud]
P (Genuine) = [Delivery address = billing address, Transaction amount ≤ max specified limit]
P (Fraud) = [Delivery address ≠ billing address, Transaction amount > max specified limit]

7. RESULT AND DISCUSSIONS

A. Result Presentation

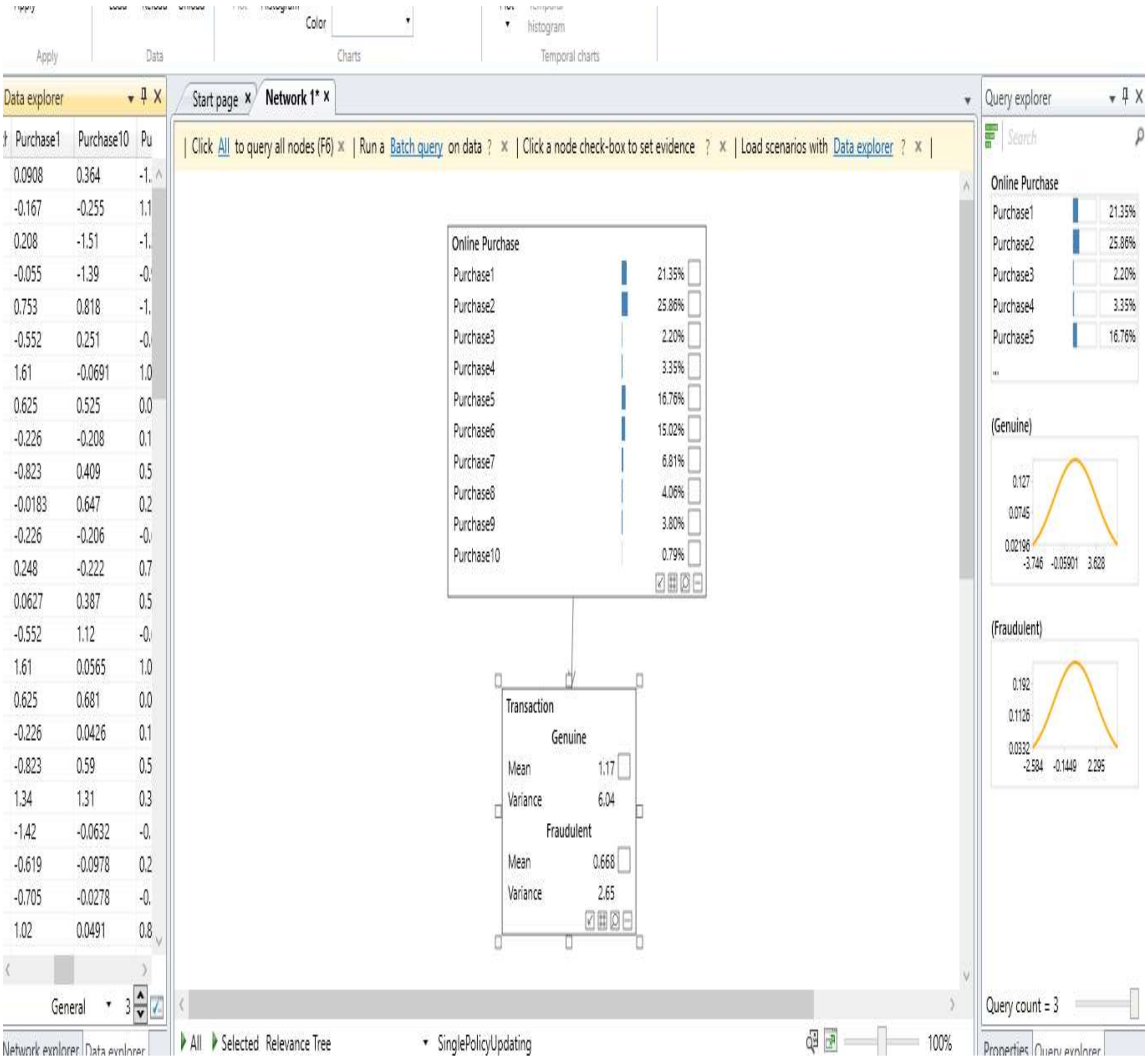
Data from the Kaggle datasets used in credit card fraud detection were gotten, analyzed and used for the implementation and experimentation of this system. In the data set we have the positive and negative values. Positive values are transactions values while negative values consist of sensitive information in the card such as customer's name, customer's location, time of transaction, card information; these customers' information in the data set was protected using Principal Component Analysis (PCA) dimensionality reduction (for example, name of individuals who made the transaction and their locations are not exposed).

Table 1 Credit Card Transaction Dataset

S|N	Purchase 1	Purchase 2	Purchase 3	Purchase 4	Purchase 5	Purchase 6	Purchase 7	Purchase 8	Purchase 9	Purchase 10
1	0.090794	-1.359807	-0.072781	2.536347	1.378155	-0.338321	0.462388	0.239599	0.098698	0.363787
2	-0.166974	1.191857	0.266151	0.16648	0.448154	0.060018	-0.082361	-0.078803	0.085102	-0.255425
3	0.207643	-1.358354	-1.340163	1.773209	0.37978	-0.503198	1.800499	0.791461	0.247676	-1.514654
4	-0.054952	-0.966272	-0.185226	1.792993	-0.863291	-0.010309	1.247203	0.237609	0.377436	-1.387024
5	0.753074	-1.158233	0.877737	1.548718	0.403034	-0.407193	0.095921	0.592941	-0.270533	0.817739
6	-0.5516	-0.617801	-0.99139	-0.311169	1.468177	-0.470401	0.207971	0.025791	0.403993	0.251412
7	1.612727	1.065235	0.489095	-0.143772	0.635558	0.463917	-0.114805	-0.183361	-0.145783	-0.069083
8	0.624501	0.066084	0.717293	-0.165946	2.345865	-2.890083	1.109969	-0.121359	-2.261857	0.52498
9	-0.226487	0.178228	0.507757	-0.287924	-0.631418	-1.059647	-0.684093	1.965775	-1.232622	-0.208038
10	-0.822843	0.538196	1.345852	-1.11967	0.175121	-0.451449	-0.237033	-0.038195	0.803487	0.408542
11	-0.018307	0.277838	-0.110474	0.066928	0.128539	-0.189115	0.133558	-0.1083	0.005274	0.647376
12	-0.225775	-0.638672	0.101288	-0.339846	0.16717	0.125895	-0.008983	-0.009431	0.798278	-0.20601
13	0.247998	0.771679	0.909412	-0.689281	-0.327642	-0.139097	-0.055353	-0.190321	-1.175575	-0.221929
14	0.062723	0.502292	0.219422	-0.137458	0.141267	-0.6970497	-0.7677331	-0.311277877	-0.49811397	0.386672552
15	-0.55159953	-0.61780086	-0.99138985	-0.311169354	1.468177	-0.4704005	0.20797124	0.02579058	-0.00260185	1.124304216
16	1.61272666	1.06523531	0.48909502	-0.143772296	0.6355581	0.46391704	-0.1148047	-0.18336127	-0.84619138	0.05653255
17	0.62450146	0.06608369	0.71729273	-0.165945923	2.3458649	-2.8900832	1.10996938	-0.121359313	-0.51253274	0.680906259
18	-0.22648726	0.17822823	0.50775687	-0.287923745	-0.6314181	-1.0596472	-0.6840928	1.965775003	-1.63111176	0.042559512

B. Classification of Transaction

There are two nodes in the network, Online Purchase node and Transaction node. Figure 4 shows the classification of transaction. Purchase 1 to Purchase 10 having distribution values in percentage. The higher the distribution value, the higher purchase made. Purchase10 has the lowest transaction with low distribution value.



Purchase1	Purchase10	Pu
0.0908	0.364	-1.
-0.167	-0.255	1.1
0.208	-1.51	-1.
-0.055	-1.39	-0.
0.753	0.818	-1.
-0.552	0.251	-0.
1.61	-0.0691	1.0
0.625	0.525	0.0
-0.226	-0.208	0.1
-0.823	0.409	0.5
-0.0183	0.647	0.2
-0.226	-0.206	-0.
0.248	-0.222	0.7
0.0627	0.387	0.5
-0.552	1.12	-0.
1.61	0.0565	1.0
0.625	0.681	0.0
-0.226	0.0426	0.1
-0.823	0.59	0.5
1.34	1.31	0.3
-1.42	-0.0632	-0.
-0.619	-0.0978	0.2
-0.705	-0.0278	-0.
1.02	0.0491	0.8

| Click All to query all nodes (F6) × | Run a Batch query on data ? × | Click a node check-box to set evidence ? × | Load scenarios with Data explorer ? × |

Online Purchase

Purchase1	21.35% □
Purchase2	25.86% □
Purchase3	2.20% □
Purchase4	3.35% □
Purchase5	16.76% □
Purchase6	15.02% □
Purchase7	6.81% □
Purchase8	4.06% □
Purchase9	3.80% □
Purchase10	0.79% □

Transaction

Genuine

Mean	1.17 □
Variance	6.04

Fraudulent

Mean	0.668 □
Variance	2.65

Query explorer

Online Purchase

Purchase1	21.35%
Purchase2	25.86%
Purchase3	2.20%
Purchase4	3.35%
Purchase5	16.76%
...	

(Genuine)

(Fraudulent)

Query count = 3

Figure 4: Classification of Transaction

C. Credit Card Transaction outcomes

Table 2 shows log likelihoods figures that is used for anomaly detection. This figures lies between [- infinity, 0], for networks that contains one or more continuous nodes (with or without discrete) the log likelihood lies in the range [-2, -19]. The table shows clearly the genuine transactions and fraudulent transactions and the conflicts.

Table 2: Credit Card Transaction Outcome

LogLikelihood	Conflict	Genuine	Fraudulent	EvidenceCount
-19.8	15.3	0.0908	1.19	3
-3.78	-0.425	0.208	1.07	3
-6.89	-0.34	0.753	1.38	3
-6.34	-0.352	0.625	1.35	3
-5.23	-0.0611	0.248	1.77	3
-5.34	-0.0394	0.0627	1.79	3
-5.83	-0.251	0.462	1.55	3
-6.69	-0.031	0.24	1.8	3
-6.19	-0.298	0.0987	1.47	3
-7.36	-0.417	0.364	1.11	3
-4.01	0.429	0.0661	1.97	2
-3.39	0.0338	0.178	1.61	2
-3.12	-0.114	0.538	1.34	2
-3.02	-0.112	0.278	1.35	2
-3.01	-0.174	0.772	1.12	2
-3.07	-0.123	0.502	1.31	2
-2.63	-0.192	0.266	1.02	2
-2.6	-0.194	0.166	1.01	2
-2.9	-0.157	0.448	1.2	2
-2.81	-0.156	0.06	1.21	2
-2.61	-0.191	0.0851	1.02	2

Conflict is a measure that detects evidence that is conflicting or rare. From table 2, it shows that the greater the conflict value above zero, the more likely the evidence is in conflict, or rare. Conflict = log ((P (e_1) P (e_2)...P (e_i)) / P (e)), where P (e_1), P (e_2) are the likelihoods of each variable considered in isolation, and P (e) is the likelihood of the all the evidence together. Evidence refers to information that is currently known about the genuine and fraudulent in a network, this is in the case of Dempster Shaffer; a set of possibilities under consideration, for instance numerical values of a variable (genuine or fraudulent) asking whether it is genuine or fraudulent. The genuine transaction appears as zero's (0) while fraudulent transactions are one's (1). From the table 2, since the number of zero is greater than one that means we have more of genuine (valid) transactions than fraudulent transaction.

D. Discussion of Results

The Kaggle dataset used for the experimentation of this system contains dataset of 281 online purchases as contained in table 1; this dataset was used to predict which transaction is genuine or fraudulent. In the data set we have the 10 parameters, time, and amount of the transaction. In the class of 1 and 0, 1 means a fraudulent transaction and 0 is genuine transaction. Purchase1 to Purchase10; this is a result of Principal Component Analysis (PCA) dimensionality reduction that was used to protect sensitive information in the data set (for example: we do not want to expose the name of individuals who made the transaction and their locations). The negative numbers in Purchase 1 to Purchase 10 contains information such as name of customer, location, card information, time of transaction.

A Bayesian Network of online transactions of credit card having two nodes (Online Purchase Node and Transaction Node). Online Purchase Node consist of discrete variables with 10 parameters (Purchase1, Purchase2, Purchase3, Purchase4, Purchase5, Purchase6, Purchase7, Purchase8, Purchase9, and Purchase10), each has a distribution value. Transaction Node consist of multiple variables (discrete and continuous) Genuine and Fraudulent are discrete while mean and variance are continuous variables.

The greater the conflict value above zero, the more likely the evidence is in conflict, or rare. Conflict = log ((P (e_1)P(e_2)...P(ei)) / P(e)), where P(e_1), P(e_2) are the likelihoods of each variable considered in isolation, and P(e) is the likelihood of the all the evidence together. Evidence refers to information that is currently known about the genuine and fraudulent in a network, this is in the case of Dempster Shaffer; a set of possibilities under consideration, for instance numerical values of a variable (genuine or fraudulent) asking whether it is genuine or fraudulent. The genuine transaction appears as zero's (0) while fraudulent transactions are one's (1). The number of zero is greater than one that means we have more of genuine (valid) transactions than fraudulent transaction.

8. CONCLUSION

In this paper, recent findings in the credit card field were reviewed and different types of fraudulent practices were identified such as: bank account fraud, counterfeit fraud, theft, application fraud and behavioural frauds. Bayesian Network method was used as one of the measures to detect these fraudulent practices. This paper analyzed the Bayesian Technique of the credit card fraud detection exploiting the use of Bayes Server Tool for the Network classification for genuine and fraudulent practices online and from kaggle dataset; the system produced more genuine transactions than fraudulent transactions.

REFERENCES

1. Armañanzas, R., Inza, I. & Larrañaga, P. (2008). Detecting reliable gene interactions by a hierarchy of bayesian network classifiers. *Computer methods and programs in biomedicine* 91, 110–121.
2. Ben Gal, I. (2007). *Bayesian Networks, in Encyclopaedia of Statistics in Quality and Reliability*. In F. Ruggeri, R. S. Kenett, & F. Faltin (Eds.), Bayesian Networks (pp. 179–185). UK: Wiley.
3. Bosin, A., Dess, N., Liberati, D. & Pes, B. (2005). Learning bayesian classifiers from gene-expression microarray data. In *International Workshop on Fuzzy Logic and Applications*, 297–304.
4. Chai, L.(2014). A review on the computational approaches for gene regulatory network construction. *Computers in biology and medicine* 48, 55–65.
5. Cho, H., Berger, B. & Peng, J. (2016). Reconstructing causal biological networks through active learning. *Plos One* 11, 65-76.
6. Cooper, G & Edward, H.(1992). Bayesian method for the induction of probabilistic networks from data. Machine Learning. Vol. 9, Issue 4, 309–347.
7. De Campos, L. M., Cano, A., Castellano, J. G., & Moral, S. (2011, November). Bayesian networks classifiers for gene-expression data. In *2011 11th International Conference on Intelligent Systems Design and Applications* (pp. 1200-1206). IEEE.
8. Ester, M., Kriegel, H. P., Sander, J., & Xu, X. (1996). A density-based algorithm for discovering clusters in large spatial databases with noise. In *Kdd* (Vol. 96, No. 34, pp. 226-231).
9. Han, J., & Kamber, M. (2001). Data mining concept and technology. *Publishing House of Mechanism Industry*, 70-72.
10. Hwang, K., Cho, D., Park, S., Kim, S. & Zhang, B. (2002). Applying machine learning techniques to analysis of gene expression data: cancer diagnosis. In *Methods of Microarray Data Analysis*, 167–182.
11. Joseph, K. (2011). Improving Credit Card Fraud Detection using a Meta-Learning Strategy", *Chemical Engineering and Applied Chemistry.* University of Toronto.
12. Kadar D., Qian, K., & Alate, N (2018). *Identifying Fraudulent Transactions in Mobile Payments.* Stanford University Stanford, CA.
13. Kasanen E., Lukka K., and Arto S. (1993).The Constructive Approach in Management Accounting Research. *Journal of Management Accounting Research* JMAR Volume 5.
14. Lin, L. & Zhu, J. (2013). Using simulated data to evaluate bayesian network approach for integrating diverse data. In *Gene Network Inference*, 119–130.
15. Markoff, J. (2015). A learning advance in artificial intelligence rivals human abilities. *The New York Times*, *10*.
16. Mukhanov, L. (2008, February). Using bayesian belief networks for credit card fraud detection. In *Proc. of the IASTED International conference on Artificial Intelligence and Applications, Insbruck, Austria* (pp. 221-225).
17. Osareh, A. & Shadgar, B. (2009).Classification and diagnostic prediction of cancers using gene microarray data analysis. *Journal of Applied Sciences* 9, 459–468.
18. Patidar, R. & Sharma, L. (2011). "Credit Card Fraud Detection Using Neural Network," *International Journal of Soft Computing and Engineering (IJSCE),* vol. 1, no. NCAI2011, pp. 2231-2307,
19. Pearl, Judea *(1998). Causality: Models, Reasoning, and Inference.* Cambridge University Press.
20. Pearl,J. (1998). Probabilistic reasoning in intelligent systems: Networks of plausible inference. Morgan Kauffman, San Mateo, CA.
21. Philip, N., & Sherly, K. K. (2012). Credit card fraud detection based on behavior mining. *TIST International Journal for Science, Technology & Research*, *1*, 7-12.
22. Russell, S., Norvig, P., Canny, J., Malik, J. & Edwards, D. (2006). *Artificial intelligence: a modern approach*. Malaysia; Pearson Education Limited.

23. Maes, S., Tuyls, K., Vanschoenwinkel, B., & Manderick, B. (2002, January). Credit card fraud detection using Bayesian and neural networks. In *Proceedings of the 1st international naiso congress on neuro fuzzy technologies* (pp. 261-270).
24. Wang, M.(2013). Legumegrn: A gene regulatory network prediction server for functional and comparative studies. *Plos One* 8, e67434
25. Xiao, F., Gao, L., Ye, Y., Hu, Y., & He, R. (2016). Inferring gene regulatory networks using conditional regulation pattern to guide candidate genes. *PloS one*, *11*(5),
26. Yee, O. S., Sagadevan, S., & Malim, N. H. A. H. (2018). Credit card fraud detection using machine learning as data mining technique. *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, *10*(1-4), 23-27.
27. Yue, Y., Finley, T., Radlinski, F., & Joachims, T. (2007, July). A support vector method for optimizing average precision. In *Proceedings of the 30th annual international ACM SIGIR conference on Research and development in information retrieval* (pp. 271-278). ACM.
28. Zheng, J., Ren, F., Tan, Y., & Chen, X. (2016). Optimizing Two-Sided Promotion for Transportation Network Companies: A Structural Model with Conditional Bayesian Learning. *Available at SSRN 2842440*.