FRAUD DETECTION IN ONLINE PAYMENTS: A SYSTEMATIC LITERATURE REVIEW

Nishkal Gupta Myadam
mnishkalgupta@gmail.com

ABSTRACT

Ever since digitalization, online payments and transactions have become a common commodity among people as it reduces their work. The virtue of the occurrence of fraud in these online payments have become more and online security have always been an issue with emerging new technologies. Here the frauds will not only ruin the banks and payment company's reputation, but they will also have a fatal impact in their economic losses and the matter of public security, as people will have all their information embedded while processing an online transaction through the credit card or other means of transactions. The crime rate related to online frauds have been dramatically increased hence different techniques are used for detecting frauds. The main focus of this paper is to provide results of a systematic literature review on fraud detection in online payments with the help of primary study papers which were selected between the years 2014 to 2019 as we wanted to obtain the latest information in the field of research. Based on our analysis the reader can acquire knowledge about the existing techniques used to solve the problem. Moreover, as far as the author's knowledge there wasn't any systematic review based on this topic, which was one of the motivations behind choosing it.

BACKGROUND

With the rapid advancement in digitalization, technologies like online payment or e-payment are gaining a lot of popularity. People nowadays consider using online payment modes over offline or cash as it gives them a lot of conveniences and saves time. As a result, it leads to the usage of a large number of online payments, which in turn increases the vulnerability of fraud taking place. Fraudsters or people performing fraud take advantage of the transparency provided by online payment technology and in order to prevent them, we need to have fraud detection techniques. Fraudsters use different techniques to perform fraud such as hacking, phishing, spoofing, using spyware, theft of personal information, etc.

Fraud detection is done by analyzing the data during online payments or transactions. It uses various algorithms to detect if a transaction is fraud or not, they are generally classified as Machine Learning and Statistical techniques.

Machine Learning is the science of letting machines learn how to make decisions exactly like humans but without any instructions (Koza, Bennett, Andre, & Keane, 1996) (Bishop, 2006). They are classified into 3 types: Supervised, Unsupervised and Reinforcement Learning. The statistical technique, in general, is used to analyze the data using various parameters such as mean, median, mode, variance, etc. and draw summary from it.

Supervised Learning – It is the process of mapping input variables to the output variables after passing the input variables through the model where the mapping function is present. In simple terms, the input variables already have classes assigned to it and the role of the algorithm is to predict it accurately (Mohri, Rostamizadeh, & Talwalkar, 2012).

Unsupervised Learning – Unlike supervised learning, unsupervised learning doesn't have classes assigned to the input variables. The input variables after passing through the algorithm automatically cluster into classes based on feature extraction i.e. input variables which have similar features group them into the same class (Jordan & Bishop, 2004).

METHODOLOGY:

The methodology used in this systematic review consists of three main stages namely:
1.Planning
2.Conducting
3.Reporting/Documenting
The review for the above three stages is done by following the procedure given by "**Barbara Ann Kitchenham"** (Keele, 2007)**.** Below figure shows the steps involved in each stage.

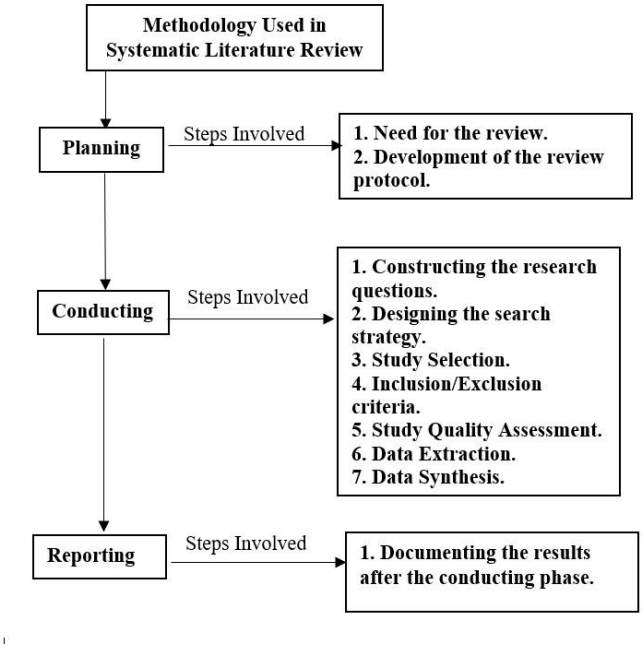

Figure-1

In the following subsections, we present a detailed understanding of the proposed protocol.

RESEARCH QUESTIONS

The main motive of this SLR is to analyze the different techniques used and implemented for detecting fraud in online payments or transactions. Below is the list of the research questions which was developed based on our motive.
RQ.1 What are the different techniques used for detecting fraud in online payments?
RQ.2 What are the different metrics used for evaluating the performance of the techniques considered for detecting the fraud?
RQ.3 What are the challenges faced for detecting the fraud in online payments? RQ.4
What type of data sets were used for detecting fraud?

DATA SOURCES AND SEARCH STRATEGY

This step helped us in picking the primary study papers which are related to our topic by using digital libraries. As this is a mini SLR we try limiting the search to only 2 databases so that we don't need to screen through too many titles and abstracts. Moreover, as there are a lot of papers related to this area we used a search strategy to select the desired and related papers. The following are the steps involved in our search mechanism:

1. Use of keywords and their synonyms for search, which is based on our research topic.
2. Inclusion of Boolean logic such as (AND, OR, Parenthesis, etc.) to search more relevantly. For example ("Fraud detection") AND ("Online Payments").

Digital Libraries

IEEE Xplore
Scopus

Table – 1

Keywords

Fraud Detection
Fraud Analysis
e-commerce transactions
Online Payments

Table - 2

STUDY SELECTION

The initial search was carried out with the help of 2 databases and the search strategy mentioned above. Once the search was done, we looked for the same papers that appeared in both the databases and selected only one out of them. The next step involved screening of the abstract to check whether the paper was related to our research or not. Later the papers were filtered by applying inclusion and exclusion criteria, the total number of papers selected after this step were 11 which are shown in Table-3. The last step was the Study Quality Assessment which was performed to make sure that we only selected papers which had a high quality, the quality was determined as high or low depending upon how many research questions the paper answered after reading the whole text, high if it answered 2 or more research questions and low if it answered below 2 questions, 2 papers were rejected after this step and we were left with a total of 9 study papers. The above process was performed by all the group members and in case of any conflicts, they were resolved by discussions and brainstorming sessions. Figure 3 shows the table used for assessing the quality of the papers. Refer to the appendix for the result of the assessment. We use binary method i.e. 1 if the research question is answered and 0 if it is not, this method was incorporated so that it would be easy for calculating the end results from the table.

S.No	Paper No	TITLE
1.	P1	Credit Card Fraud Detection using autoencoder based clustering
2.	P2	Combining Auto Encoders and One Class Support Vectors Machine for Fraudulant Credit Card Transactions Detection
3.	P3	Adaptive Type-2 Fuzzy Logic Based System for Fraud Detection in Financial Applications
4.	P4	Improved Fraud Detection in e-Commerce Transactions
5.	P5	Research on Bank Anti-fraud Model Based on K-means and Hidden Markov
6.	P6	A Survey on Credit Card Fraud Detection using Machine Learning
7.	P7	Intelligent Fradulent detection system based SVM and optimized by danger theory
8.	P8	Fraud Analysis and Prevention in e-Commerece Transactions
9.	P9	Usage signatures analysis an alternative method for preventing fraud in E-Commerce applications
10.	P10	Study of Hidden Markov Model in Credit Card Fraudulent Detection
11.	P11	Analysis on Credit Card Fraud Identification Techniques based on KNN and Outlier Detection

Table-3

S.No	Paper No	RQ.1	RQ.2	RQ.3	RQ.4

Table-4

INCLUSION & EXCLUSION CRITERIA

Inclusion criteria:

1. Papers/Articles focusing on fraud detection in online payments.
2. Papers/Articles must be written in English.
3. Papers/Articles published between the years 2014 and 2019.
4. Papers which had a high-quality assessment.

Exclusion criteria:

1. Papers which emphasized on fraud detection but not online payments.
2. Papers which emphasized on online payments but not fraud detection.
3. Papers which emphasized on offline payments.
4. Papers which were not published.
5. Papers which didn't have answers to our research questions.

DATA EXTRACTION

After selecting the final study papers, we created a data extraction form, the purpose of which is to fill the extracted data from the selected study papers. The form consists of different attributes which are shown below in the table-5. We used a coordinated approach between all the group members to avoid errors while filling the extracted data in the data form.

S.no	Paper No	Title	Author	Publisher	Published year	Techniques used	Metrics used	Challenges	Data set

Table-5

Refer to the appendix for the results filled inside the data extraction form.

DATA SYNTHESIS

After collecting the data from the primary papers and storing them into data extraction form, we perform data synthesis. The main objective of this section is to analyze accumulated data and resolve the research questions. We use a narrative synthesis method for Research questions RQ.1, RQ.2 & RQ.4 which accumulates the results in a table and graphically represents them whereas for RQ.3 we synthesize the data in a descriptive manner. Data synthesis is also performed to help us provide evidence for obtaining conclusive answers for our research questions by collecting or accumulating papers which have similar concepts or viewpoints.

Metrics	No. of papers	Paper no
Accuracy	1	P1,P9
False positive	2	P1,P5
F1 score/F measure	3	P1,P2,P7
Recall	3	P1,P3,P8
Precision	2	P1,P8
Geometric mean	1	P1
Root Mean Square Error	1	P4
Mean Square Error	1	P4
Mean Absolute Error	1	P4
True positive	1	P5
False negative	1	P5
true negative	1	P5
time complexity	1	P7

Table-6

Type of Algorithm	No. of Papers	Paper No
Supervised Learning	6	P3,P4,P5,P6,P7,P8
Unsupervised Learning	2	P1,P2
Statistical	1	P9

Table-7

		No. Of Papers	Paper No
Data Set	Synthetic	3	P4,P5,P7
	Real	5	P1,P2,P3,P8,P9

Table -8

From the above data synthesis, we observe the collection of different attributes from different selected study papers.

RESULTS AND PRINCIPAL FINDINGS

The main objective of this section is to provide the results for our Systematic Literature Review on "Fraud Detection in Online Payments" by answering and extending the discussions on the research questions proposed in this paper with the help of the data obtained from the primary papers selected. This section also gives us insight into the findings from our study papers.

RQ.1 What are the different techniques used for detecting fraud in online payments?

The above research question can be regarded as a fundamental question of this SLR as this helps in answering the technique used for detecting fraud in online payments. In this section, we mention the different techniques present in the selected primary studies so that the reader can have an insight into it.

From the primary papers, we have found that most of the techniques used for detecting the fraud were based on "Machine Learning" except for the technique used in paper P9 which is based on a statistical technique. Below is the graphical representation of the types of algorithms used by the papers.

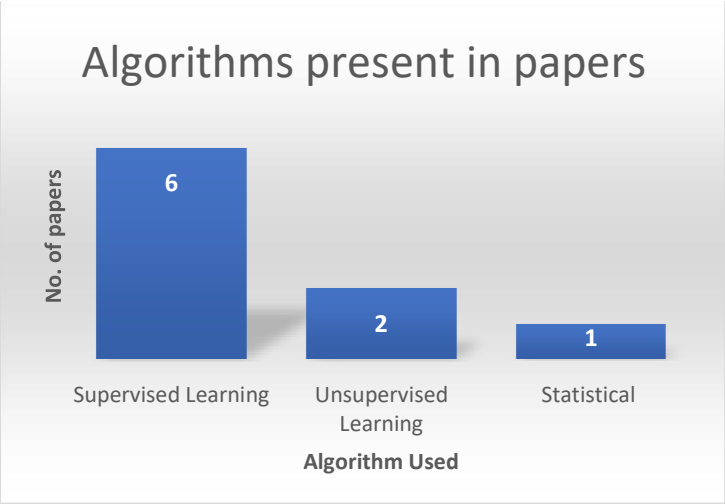

Figure-2

From the above graph, we can infer that the majority of the papers used supervised learning algorithms when compared to unsupervised learning and statistical algorithm.

From our findings, we can analyze that most of the data sets used in the primary papers have classes assigned to their input variables or attributes as 7 out of 9 papers rely on the supervised learning algorithm.

Type of Technique	No. Of Papers	Paper No	Algorithm used
Auto Encoders	2	P1,P2	Unsupervised
Support Vector Machine	3	P2,P6,P7	Supervised
Clustering	1	P1	Supervised
Fuzzy logic system	2	P3,P4	Supervised
K-Means	1	P5	Unsupervised
Hidden Markov Model	1	P5	Supervised
Artificial Immune system	1	P6,	Supervised
Bayesian belief network	2	P6,P8	Supervised
Logestic regression	2	P6,P8	supervised
Random forest	1	P8	Statistical
Decision tree	1	P6	Supervised
Danger theory	1	P7	Supervised

Table-9

The above table shows the different techniques and algorithms used in the selected primary papers. From the above table, we found that the Support Vector Machine, Auto Encoders, Fuzzy Logic System, Bayesian Belief Network and Logistic regression were the most commonly used techniques.

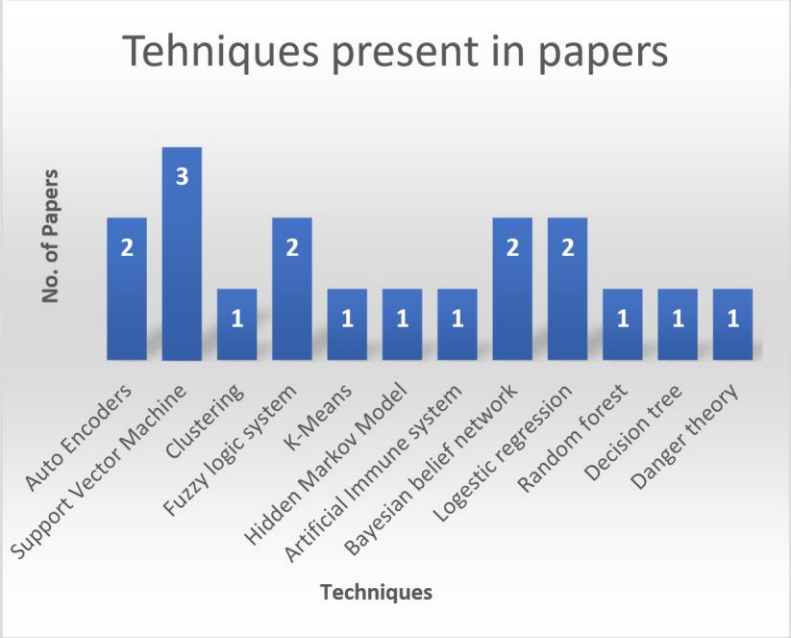

Figure-3

Let us now briefly discuss how the techniques mentioned above works.

- **Auto Encoders** – It is an unsupervised learning algorithm whose aim is to reduce the dimensionality of the given input features. For example, converting a multidimensional feature space into a single dimension. They are represented as a type of neural network (Zamini & Montazer, 2018) (Mohamad Jeragh, 2018).
- **Support Vector Machines** – It is a supervised learning algorithm which is basically used for classification and regression purposes i.e. it helps in determining which class the data point belongs to. Classification is done for discrete values for example 1 if fraud is detected and 0 if it is not, whereas regression is done for continuous values and also regression helps us in knowing the relationship between independent and dependent variables. SVM's can further be categorized based on a multi-class or single class. We use one class SVM in paper P2 where we are not aware of the different fraud transactions, but we are aware of good transactions hence any data which doesn't come under the good transaction class is considered as fraud. SVM creates hyper lines for differentiating different classes. Other primary papers which use SVM techniques are paper P6 & P7 (Mohamad Jeragh, 2018) (Isha Rajak, 2015) (Rimpal R. Popat, 2018).
- **Fuzzy Logic System** – Unlike standard logic system, fuzzy logic takes any real values for its variables between 1 and 0 i.e. it is a many-valued logic. In paper P4 and P5 we see the combination of neural networks and fuzzy logic to detect fraud in online payments (Saeed Khalil Saeed, 2018) (Jisha Shaji, 2017).
- **K means** - It is another unsupervised learning algorithm which clusters data points based on knearest neighbors. Initially, it identifies the centroid of a cluster and later uses a distance measure to detect the nearest data point to it. Paper P5 uses this method along with the hidden Markov model to detect fraud (Xiaoguo Wang, 2018).

- **Hidden Markov Model** – It consists of states variables and transition probabilities. They include 2 states: observed and unobserved whereas in Markov model there are no unobserved states. In HMM we see probabilities of a sequence of observations. It trains on historical data. Paper P5 gives us more insight into how this technique is used to detect fraud (Xiaoguo Wang, 2018).
- **Artificial Immune system –** This concept is built based on the human biological system. It creates cells which fight against the antigens or foreign bodies. They are divided into 2 types namely clonal selection and negative selection as referred in paper P6 (Rimpal R. Popat, 2018).
- **Bayesian Belief network –** This is a supervised learning algorithm solely based on the Bayes theorem. It is based on the conditional probability between outcome variables i.e. probability occurrence of A depends upon the condition of the probability of occurrence of B. Paper P6 & P8 explains how we can use this for detecting the fraud (Rimpal R. Popat, 2018) (Evandro Caldeira, 2014).
- **Logistic regression –** This technique is used for binary classification and comes under unsupervised learning. It explains the relationship between one dependent binary variable and other independent variables.
- **Decision Tree -** It uses the acyclic graph which consists of nodes and edges to make the decision regarding a particular event. They are further divided into classification tree and regression trees. Paper P6 gives us a good explanation about it (Rimpal R. Popat, 2018) (Evandro Caldeira, 2014).
- **Danger theory –** It is similar to how the immune system works and similar to an artificial immune system which was defined above. Paper P7 uses Danger Theory and SVM to detect frauds (Isha Rajak, 2015).
- **Signature Analysis –** It is a statistical technique which is based upon the data stream. A data stream source is a continuous flow of data which will establish a usage pattern in a specific branch by selecting a group features which will later calculate the summaries involved in the data set using statistical parameters (Gabriel Mota, 2014).

RQ.2 What are the different metrics used for evaluating the performance of the techniques considered for detecting the fraud?

The main purpose of this question is to provide us with the details of the different metrics used in the primary papers selected in this SLR.

Metric helps in evaluating the performance of the techniques used for detecting the fraud. During our investigation, we came across different metrics which we can see in table-6. In order to know about different metrics, we need to first know about the confusion matrix. Confusion matrix which is also known as error matrix is a 2x2 matrix which helps us in easily identifying confusion between true class and predicted class i.e. it helps us in identifying if one class is mislabeled as other. Below is the confusion matrix

	Predicted Class A	Predicted Class B
Actual Class A	True positive	False Negative
Actual Class B	False Positive	True Negative

Here let's consider class A as positive and class B as negative. To define what is positive and negative let's take an example, if our observation is detecting a fraud then fraud being present is positive and fraud being absent is negative.

True Positive: Our observation is positive, and our prediction is also positive

True Negative: Our observation is positive, but our prediction is negative

False Positive: Our observation is negative, but our prediction is positive
False Negative: Our observation is negative, and our prediction is also negative
From the above knowledge of the confusion matrix, we can derive different metrics used to measure the performance of our model.
Accuracy = (TP+TN)/(TP+TN+FP+FN).
Accuracy helps us in knowing how close our observation is to our prediction.
Recall = (TP)/(TP+FN)
Recall can be explained as the ratio of correctly identified positive samples by the total no of positive samples. Higher the value of recall, higher the prediction of a sample being classified into a correct class.

Precision = (TP)/(TP+FP)
Precision can be explained as the ratio of correctly identified positive samples by the total no of predicted positive samples. It helps us in knowing how close our observations are to each other.
F-measure/F1 Score = 2*recall*precision/recall + precision, it helps us in knowing the test accuracy with the help of both recall and precision.
Geometric mean = sqrt(a1*a2*……*an), here sqrt is the square root and a1,a2,…an are the sample outputs. Extremely large or small samples have no effect of the geometric mean.
Root mean square error = sqrt(sum(predicted value – observed values)/total no. of values)) It helps us in finding the difference between the predicted values and observed values.
Mean Square error is the same as the root mean square error except for the square root which is applied in the RMSE in order to have the same scales for both predicted and observed samples.
Time complexity helps us in determining the speed of execution of a model i.e. it tells us how fast or slow an algorithm takes to test a data set. (Mohamad Jeragh, 2018)

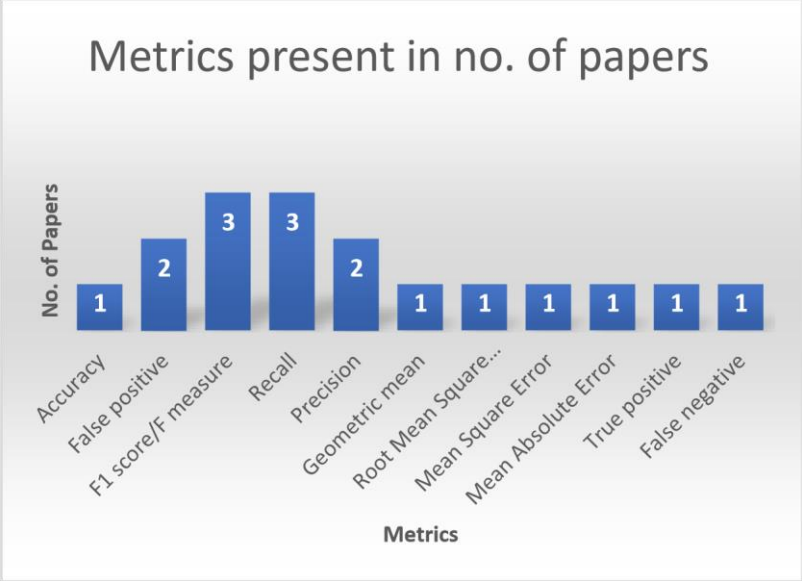

Figure-4

The above figure helps us give a graphical insight about the no. of papers using different metrics. We can observe from our findings that F-measure, Recall and False positive rate were more used than other metrics for evaluating the performance of the detection technique.

RQ.3 What are the challenges faced for detecting the fraud in online payments?
Detecting fraud is not so easy as it looks, it has a few challenges associated with it. This question helps us in determining what the challenges are faced in detecting fraud in online payments. Below are the points

that have been extracted from the primary papers selected, only 3 primary papers out of 9 have addressed this question.
As online payments are large in number, the data sets associated with them are also large and hence it is a challenge for developers to develop fast and efficient algorithms (Jisha Shaji, 2017).
It becomes challenging for the model to showcase good performance in case of imbalanced data sets or data sets having fewer data points (Xiaoguo Wang, 2018).
One of the major challenges for fraud detection in real-time is a limited time span for rejection or acceptance of payment (Jisha Shaji, 2017).
Another challenge is the availability of real data sets due to privacy issues, the true performance of a model can only be evaluated using real data sets (Xiaoguo Wang, 2018).
As Fraudsters indulge in using new approaches each and every time, they perform a fraud it becomes challenging for the system to adapt accordingly as the retraining cost is high (Jisha Shaji, 2017) (M. Zareapoor, 2015).
Challenging part in constructing the model for detecting the fraud is the selection of features, as different features have different calculations and response time (Rimpal R. Popat, 2018) (M. Zeager, 2017). Avoiding overfitting while using machine learning algorithms is one of the biggest challenges as it concentrates on tendencies particular to training dataset rather than test data set (Rimpal R. Popat, 2018). Future work can be made to overcome the above challenges so that detecting the fraud can be more efficient.

RQ.4 What type of data sets were used for detecting fraud?

The role of this question is to help us identify the different types of data sets used for detecting fraud in online payments. The input parameters for the technique used is obtained from the data set, hence it is important to know the nature of the data set. The data set used was mainly classified as 2 types: 1. Simulated or Synthetic

2. Real Data sets.

Further, the data sets were also divided into open-source and private. The information regarding the private data sets was not shared by the researchers and hence it is hard to verify the results performed on these data sets whereas the results can be easily verified using the open-source data sets. Below is the graph that represents the type of data set used by our primary studies in validating the techniques used.

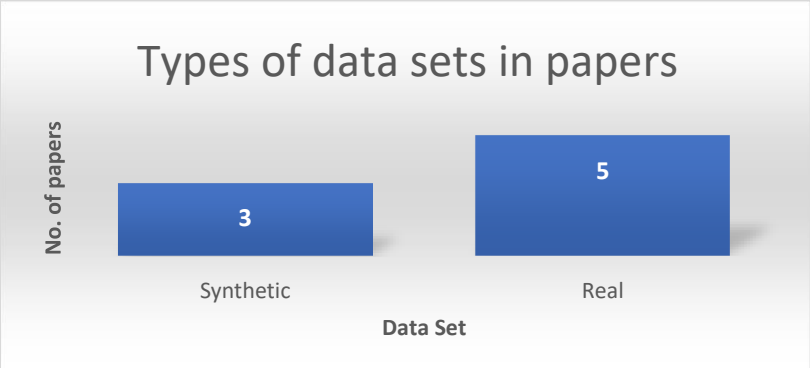

Figure-5

From the above graph, we can observe that most of the papers selected for the SLR used real data sets, from which we can infer that most of the techniques used were performed under real circumstances. The performance of a technique is accurately known using real data sets rather than the one simulated as the simulation is done according to our needs and it's not the same in case of real data sets. Below is the table which shows the names of different data sets used in the papers.

Paper No	TITLE	DATASET USED
P1	Credit Card Fraud Detection using autoencoder based clustering	Real(European bank)
P2	Combining Auto Encoders and One Class Support Vectors Machine for Fraudulant Credit Card Transactions Detection	Real(the Kaggle Credit Card dataset)
P3	Adaptive Type-2 Fuzzy Logic Based System for Fraud Detection in Financial Applications	Real(data provided by Alshamal Islamic Bank (SHIB) in Sudan)
P4	Improved Fraud Detection in e-Commerce Transactions	synthetic(German credit dataset) open source
P5	Research on Bank Anti-fraud Model Based on K-means and Hidden Markov	synthetic to check the feasability of data, real dataset for evaluation
P6	A Survey on Credit Card Fraud Detection using Machine Learning	None
P7	Intelligent Fradulent detection system based SVM and optimized by danger theory	synthetic(German credit dataset)open source
P8	Fraud Analysis and Prevention in e-Commerece Transactions	Real(Pag Seguro) Web service for online payments
P9	Usage signatures analysis an alternative method for preventing fraud in E-Commerce applications	Real(confidential) e-commerce

We can see that paper P6 didn't use any data set as it only addressed RQ.1 and RQ.3 i.e. techniques used and challenges faced. Other papers used data sets obtained from various sources such as Banks (paper P1 and P3), Web service for online payments by Pag Seguro (paper P8), e-commerce site (paper P9) and others used simulated open-source data sets (papers P4, P5, and P7).

CONCLUSIONS AND RECOMMENDATIONS

We performed an SLR to analyze different fraud detection techniques in the area of online payments. The above review gave a complete insight into the research questions mentioned in this paper. We were successful in finding, analyzing and discussing different techniques, metrics, challenges and data sets used for detecting fraud in online payments. From our analyses, we have found that the common detection techniques used for detecting fraud were Support Vector Machine, Auto Encoders, Fuzzy Logic System, Bayesian Belief Network and Logistic regression where most of the techniques were based on supervised learning. This SLR also lead to the conclusion that most of the techniques were evaluated on real datasets. Based on our findings we would like to recommend opportunities for future work in this area. More empirical experiments must be performed on adaptive systems for detecting fraud. More research work should be carried out using unsupervised learning algorithms so that fraud can be detected if the input data is not labeled.

REFERENCES

1. Bishop, C. M. (2006). Pattern Recognition and Machine Learning, Springer.
2. Evandro Caldeira, G. B. (2014). Fraud Analysis and Prevention in e-Commerece Transactions. *2014 9th Latin American Web Congress.* IEEE.
3. Gabriel Mota, J. F. (2014). Usage signatures analysis an alternative method for preventing fraud in ECommerce applications. *2015 International Conference on Computer, Communication and Control (IC4).* IEEE.
4. Isha Rajak, D. M. (2015). Intelligent Fradulent detection system based SVM and optimized by danger theory. *IEEE International Conference on Computer, Communication and Control (IC4-2015).* IEEE.
5. Jisha Shaji, D. P. (2017). Improved Fraud Detection in e-Commerce Transactions. *2017 2nd International Conference on Communication Systems, Computing and IT Applications (CSCITA).* IEEE.

6. Jordan, M. I., & Bishop, C. M. (2004). Neural Networks". In Allen B. Tucker (ed.). Computer Science Handbook, Second Edition (Section VII: Intelligent Systems).

7. Keele, S. a. (2007). Guidelines for performing systematic literature reviews in software engineering. *Technical report, Ver. 2.3 EBSE Technical Report. EBSE*.

8. Koza, J. R., Bennett, F. H., Andre, D., & Keane, M. A. (1996). Automated Design of Both the Topology and Sizing of Analog Electrical Circuits Using Genetic Programming. Artificial Intelligence in Design '96. 151-170.

9. M. Zareapoor, P. S. (2015). Application of Credit card Fraud Detection: Based on Bagging Ensemble Classifier. *Elsevier International Conference on Intelligent Computing, Communication & Convergence, 201*, 679-685.

10. M. Zeager, A. S. (2017). Adversarial Learing in Credit card Fraud Detection. 112-116.

11. Mohamad Jeragh, M. A. (2018). Combining Auto Encoders and One Class Support Vectors Machine for Fraudulant Credit Card Transactions Detection. *2018 9th International Symposium on Telecommunications (IST).* IEEE.

12. Mohri, M., Rostamizadeh, A., & Talwalkar, A. (2012). Foundations of Machine Learning.

13. Rimpal R. Popat, J. C. (2018). A Survey on Credit Card Fraud Detection using Machine Learning . *Proceedings of the 2nd International Conference on Trends in Electronics and Informatics (ICOEI 2018)* (pp. 1120-1125). IEEE.

14. Saeed Khalil Saeed, H. H. (2018). Adaptive Type-2 Fuzzy Logic Based System for Fraud Detection in Financial Applications. *2018 10th Computer Science and Electronic Engineering (CEEC).* IEEE.

15. Xiaoguo Wang, H. W. (2018). Research on Bank Anti-fraud Model Based on K-means and Hidden Markov. *2018 3rd IEEE International Conference on Image, Vision and Computing.* IEEE.

16. Zamini, M., & Montazer, G. (2018). Credit Card Fraud Detection using autoencoder based clustering. *International Symposium on Telecommunications* (pp. 486-490). IEEE.

APPENDIX

S.No	Paper No	RQ.1	RQ.2	RQ.3	RQ.4	SUM	Selected
1.	P1	1	1	0	1	3	yes
2.	P2	1	1	0	1	3	yes
3.	P3	1	1	1	1	4	yes
4.	P4	1	1	1	1	4	yes
5.	P5	1	1	1	1	4	yes
6.	P6	1	0	1	0	2	yes
7.	P7	1	1	0	1	3	yes
8.	P8	1	1	0	1	3	yes
9.	P9	1	1	0	1	3	yes
10.	P10	1	0	0	0	1	no
11.	P11	1	0	0	0	1	no

Table-A

Table A represents the quality assessment whereas '1' represents that the research paper that answered the research question and '0' represents that the question was not answered by the paper. As we observe the last two columns that the paper was only considered if it answered at least two of the research questions.

S.NO	Paper No	TITLE	AUTHOR	PUBLISHER	YEAR	TECHNIQUES USED
1	P1	Credit Card Fraud Detection using autoencoder based clustering	Zamini Mohamad, Montazer Gholamali	IEEE	2018	Unsupervised fraud detection using autoencoder based clustering(MACHINE LEARNING)
2	P2	Combining Auto Encoders and One Class Support Vectors Machine for Fraudulant Credit Card Transactions Detection	Mohamad Jeragh, Mouza Alsulaimi	IEEE	2018	Unsupervised learning model combining autoencoder and OCSVM for fraud detection.
3	P3	Adaptive Type-2 Fuzzy Logic Based System for Fraud Detection in Financial Applications	Saeed Khalil Saeed, Hani Hagras	IEEE	2018	Adaptive Type-2 Fuzzy logic based system for fraud detection.(supervised learning)
4	P4	Improved Fraud Detection in e-Commerce Transactions	Jisha Shaji,Dalohata Panchal	IEEE	2017	Adaptive Neuro-Fuzzy Inference System (Supervised learning)
5	P5	Research on Bank Anti-fraud Model Based on K-means and Hidden Markov	Xiaoguo Wang,Hao Wu,Zhichao Yi	IEEE	2018	K-Means and Hidden Markov Model (Statistical technique and ML) (Supervised Learning)
6	P6	A Survey on Credit Card Fraud Detection using Machine Learning	Rimpal R. Popat,Jayesh Chaudhary	IEEE	2018	Artificial Immune System, Bayesian belief network,logistic regression,neural network,support vector machine,decision tree,generic algorithm (Supervised Learning)
7	P7	Intelligent Fradulent detection system based SVM and optimized by danger theory	Isha Rajak,Dr.K.James Mathai	IEEE	2015	Supervised training algorithm for fraud detection with the fusion of danger theory and svm
8	P8	Fraud Analysis and Prevention in e-Commerce Transactions	Evandro Caldeira,Gabriel Brandao,Adriano C.M. Pereira	IEEE	2014	Bayesian n/w, Neural Network, Logistic Regression and Random Forest (Supervised Learning)
9	P9	Usage signatures analysis an alternative method for preventing fraud in E-Commerce applications	Gabriel Mota,Joana Fernandes	IEEE	2014	Signature analysis (Supervised Learning)

Table – B.1

The table B.1 represents the title, author, publication, year of publication and techniques used in the wiring of the systematic literature review using the primary papers.

METRICS USED	CHALLENGES	DATASET USED
Accuracy, False positive rate,F1 score, recall , Precision		Real(European bank)
Geometric mean(GMean) , F1 score		Real(the Kaggle Credit Card dataset)
Average recall		Real(data provided by Alshamal Islamic Bank (SHIB) in Sudan)
Root mean square error,Mean square error,Mean absolute error	Detecting fraud when transaction is processed as transaction time is less,to avoid rejecting the genuine customers	synthetic(German credit dataset) open source
true positive,false positive,true negative,false negative	less data values in data sets and selection of parameters for evaluating its performance	synthetic to check the feasability of data, real dataset for evaluation(confidential)
F measure , time complexity	Feature selection, overfitting, retraining the classifier due to its cost	synthetic(German credit dataset)open source
Precision,Recall		Real(Pag Seguro) Web service for online payments
Accuracy		Real(confidential) e-commerce

Table – B.2

The table B.2 represents the metrics, challenges, and data used in the wiring of the systematic literature review using the primary papers.