

A REVIEW: CREDIT CARD FRAUD DETECTION

Muskan Naik^{*1}, Abha Choubey^{*2}, Prageet Bajpai^{*3}

^{*1}M.Tech Scholar, Department Of Computer Science, Shri Shankaracharya
Technical Campus Bhilai C.G. India.

^{*2,3}Assistant Professor, Department Of Computer Science, Shri Shankaracharya
Technical Campus Bhilai C.G. India.

DOI : <https://www.doi.org/10.56726/IRJMETS45256>

ABSTRACT

The detection of cheaters can be tough because to their unexpected nature and the absence of identifiable samples, rendering them difficult to identify. Fraudulent individuals endeavor to enhance their own gains by using prior advancements in a manner that detrimentally affects others. The individuals in question did not achieve success in successfully completing many detour protection exams, leading to a significant financial deficit amounting to millions of dollars. One approach to monitor fraudulent transactions is the utilization of statistical mining methods, aimed at analyzing unexpected physical transactions and identifying them as instances of deceit. The objective of this study is to conduct a comparative analysis of various artificial intelligence (AI) methodologies, including OK-closest neighbor (KNN), abnormal timberland, and backing vector machines (SVM). Additionally, this research aims to develop a comprehensive comprehension of AI techniques such as auto encoders, convolutional neural networks (CNN), restricted Boltzmann machines (RBM), and deep belief networks. The topic of discussion is exchanges, specifically referring to the concept of decentralized business networks (DBN). This application will utilize datasets from the European Union (EU), Australia, and Germany. There exist three distinct assessment measures that might potentially be employed. Three often used evaluation metrics in machine learning are the Area Under the Receiver Operating Characteristic Curve (AUC), the Matthews Correlation Coefficient (MCC), and the Cost of Error. This study presents an examination of the diverse targeting strategies employed.

Keywords: Fraud Detection, Machine Learning, Review.

I. INTRODUCTION

With the advent of Visa cards and the proliferation of online payment systems, a multitude of fraudulent individuals have developed strategies to exploit unsuspecting individuals, therefore illicitly acquiring their credit card details for the purpose of making unauthorized transactions. The utilization of these approaches has experienced significant proliferation since the introduction of Visas and online payment systems. Consequently, a substantial volume of fraudulent transactions occurs on a daily basis. Financial institutions and online platforms exclusively focused on conducting business digitally endeavor to detect and prevent fraudulent financial activities, with the aim of decreasing the likelihood of their recurrence. The utilization of artificial intelligence (AI) and strategies using deep learning techniques is being employed with the aim of preemptively thwarting fraudulent activities prior to their validation. Artificial intelligence (AI), a subfield of artificial cognition, is perhaps one of the most prominent concerns of the current decade. A diverse range of organizations are increasingly dedicating resources to the use of artificial intelligence (AI) with the aim of enhancing their administrative functions. Artificial intelligence (AI) refers to the computational techniques employed to empower computers to execute tasks without relying on intricate coding, achieved by the integration of diverse computer calculations with real-life demonstrations. The inclusion of "training statistics" has the potential to confer a competitive advantage to the winning model. From a detached perspective, one may either develop expectancies or engage in behaviors without being influenced by the immediate experience recordings. Artificial intelligence methodologies, such as Fake Neural Organizations, may incorporate in-depth investigation models as a constituent element. Convolutional neural networks, Profound Conviction Organizations, Auto-encoders, Recurrent Neural Networks, and Confined Boltzmann Machines are instances of approaches that exhibit diverse characteristics from one another. A well designed neural network would possess the capability to identify at least one form of connection throughout the entirety of the dataset. One

form of fraudulent activity referred to as "Visa misrepresentation" involves the utilisation of stolen MasterCard information or telephone-based methods, resulting in financial losses for both cardholders and merchants who possess safeguards against such incidents. In 2016, the Single Euro Payments Area (SEPA) witnessed a total of 1.8 billion euros in MasterCard fraud, accounting for a mere 0.4% decrease over the preceding year. This figure was part of a larger sum of four trillion euros. [1] According to the study conducted by Nelson (year not provided), the global financial losses associated with MasterCard transactions amounted to \$21.84 billion in 2015. It was projected that this figure would rise to \$32 billion by the year 2020...

II. LITERATURE SURVEY

Gajendra Singh and colleagues (2012) et al. The establishment of an online business platform has facilitated the exchange of digital currencies, aiming to provide a convenient and efficient method for generating profits. However, it is important to acknowledge that this platform also has inherent risks, particularly the potential for abuse of power and extortion inside the organisational structure. One example of fraudulent activity is Visa misrepresentation, which can occur through several techniques such as card theft, hacking by online programmers to get access to sensitive card information, and the use of stolen cards. The study conducted by Tuyls and colleagues (2013) This paper aims to elucidate some issues that are inherently related with the Extortion Discovery. Commencing with the analysis, the datasets utilised in this programming context exhibit a significant degree of skewness, whereby a mere fraction of the total records have relevance. Consequently, the task of constructing precise models is rendered notably challenging. The presence of several conflicting facts and overlapping designs may potentially lead to challenges rather than notable outcomes. Primarily, the elements associated with academic dishonesty persistently undergo transformations, necessitating character models to adapt and effectively address these evolving dynamics. The subsequent analysis presents an audit of the most relevant investigations undertaken in the field of extortion detection, which have employed artificial intelligence (AI) and deep learning models.

Evandro Caldeira and colleagues (2014) There is a hypothesis suggesting a significant increase in the volume of electronic transactions in recent years, primarily due to the rise of digital businesses operating online, such as Amazon.com, eBay, and AliExpress.com. Furthermore, there has been a notable surge in the frequency of extortion cases, leading to substantial financial losses amounting to billions of dollars annually on a global scale. Therefore, it is imperative and comprehensive to develop and execute methods that may effectively address and mitigate identity theft and fraud, which serves as the driving force for our research. The objective of this study is to employ and evaluate computational perception methodologies, including data mining and artificial intelligence, in order to distinguish instances of deceit in digital transactions. Specifically, the focus is on credit card obligations conducted through online payment gateways. The solutions are implemented and examined utilising a genuine dataset obtained from the prominent digital installment administration platform in Brazil. This affords us the opportunity to go further into the methodologies. Based on our research, it is evident that the organisation engaged in a proficient execution of false identification, leading to the generation of revenues equivalent to around 43 percent of the economic dimension.

Suryanarayana et al. (2018) Due to the extensive proliferation of Visa cards, the occurrence of fraudulent activities is a substantial concern for enterprises involved in transactions using MasterCard. Obtaining accurate statistics on the extent of misrepresentation is challenging due to the reluctance of agencies and banks to disclose the true magnitude of the negative consequences resulting from counterfeit activities. Consequently, the lack of transparency around this issue hampers the availability of specific information pertaining to the impact of misrepresentation. Simultaneously, the availability of public data for classroom exercises is infrequent, resulting in several unanswered inquiries on the optimal methodology. One additional concern that arises in the assessment of credit card fraud damage is the limitation of evaluating solely the identified instances of fraudulent transactions, thereby precluding an informed estimation of unreported or undetected fraudulent transactions. Due to the dynamic and fast-changing nature of misrepresentation schemes, it is imperative to reevaluate the field of extortion with a proactive approach. In recent times, there has been a growing interest in the use of artificial intelligence (AI) in several domains such as image identification, natural language processing, and discourse analysis. Therefore, it is imperative to employ sophisticated fraud detection algorithms that incorporate methodologies derived from the domain of artificial intelligence in order to

mitigate these financial setbacks and aid experts in combating extortion. This article presents a strategic approach that relies entirely on an artificial intelligence (AI) methodology to effectively distinguish instances of visa fraud. The results suggest that employing strategic relapse-based tactics yields the highest level of accuracy, making it a viable approach for investigators involved in cases of extortion.

Adi Saputra and colleagues (2019) As previously indicated, the proliferation of internet users is contributing to a rise in the volume of commercial transactions carried out through online platforms. It is evident that there is a rising trend in the occurrence of extortion cases on internet platforms. The development of an AI-based countermeasure to mitigate extortion in the realm of internet commerce is a potential avenue to explore. The present work aims to analyse and deconstruct the process of rational artificial intelligence computation. The computational methods to be employed include the Decision Tree, the Naive Bayes, the Random Forest, and the Neural Network. An imbalance persists in the use of information. Individuals Intentionally Rendered as a Minority In order to get stability information, the implementation of the Over-trying Out Strategy (Destroyed) level will be pursued. The assessment results indicate that the neural network achieved the highest accuracy of 96% while utilising the disarray lattice approach. The random forest, Naive Bayes, and decision tree algorithms achieved accuracies of 95%, 95%, and 91% respectively. The Engineered Minority Over-examining Process (Destroyed) demonstrates the capacity to enhance the average F1-Score to 94.5 percent and the average G-Mean to 84.6 percent. The aforementioned increments arise as a direct consequence of the eradication of EMOAP's deleterious functionalities.

Elena-Adriana and colleagues (2019) et al. The user has suggested a potential solution or idea. The act of extortion poses an elevated level of risk for internet-based enterprises engaged in selling, promoting, and e-commerce within the context of contemporary online marketing operations. The misrepresentation of products through the use of 'snap' is widely recognised as a significant concern within the realm of internet commerce. Irrespective of the extent to which online sponsors actively strive to enhance methods for differentiating visitors, it is conceivable that they are nonetheless in search of optimal strategies to detect fraudulent clicks. Therefore, it is imperative for internet marketing companies to do a thorough evaluation of the misrepresenting area in order to establish credibility. The objective of this study is to assess the accuracy of a state-of-the-art artificial intelligence algorithm in order to understand the rapid occurrence of fraudulent activities in an online setting. During the duration of our inquiry, we examined the click-through behaviours seen within a dataset including over 200 million clicks across a four-day period. The main objective of this study was to examine the trajectory of a customer's snap inside their portfolio and banner IP, with a particular focus on users who generate a significant number of snaps but do not actively engage in providing packages. To do this, a test for Light GBM is employed, which belongs to a category of methods referred to as Gradient Boosting Decision Trees. This computation has resulted in achieving an accuracy rate of 98%. During the course of our inquiry, the writing review functioned as the principal means by which we substantiated our conclusions.

In a study conducted by S. P. Maniraj and colleagues in 2019, The ability to identify fraudulent MasterCard transactions is of paramount significance for organisations involved in MasterCard transactions. This measure guarantees that clients are not subjected to charges for things that they did not purchase. The field of information science facilitates the effective handling of such challenges, and its significance, when combined with artificial intelligence, is not expected to surpass its current level. This study aims to showcase the utilisation of artificial intelligence (AI) in tandem with credit card fraud identification to present an informative compilation of data. The issue of Visa misrepresentation location problem involves the provision of proof that beyond the scope of MasterCard transactions, by supplying factual information regarding instances that were identified as acts of extortion. Subsequently, this iteration is employed to ascertain the falsity of an alternate option. Currently, our primary goal is to effectively distinguish all instances of fraudulent transactions, while concurrently minimising the occurrence of incorrect extortion requests. The phenomena commonly referred to as charge card misrepresentation detection sometimes serves as a means of grouping. Throughout this period, our main emphasis has been on the analysis and organisation of data sets in order to facilitate the computation of distinct identification measures. Several computations may be cited as examples, such as the Neighbourhood

Anomaly Factor and the Seclusion Backwoods calculation. These calculations are specifically conducted on the PCA adjusted Visa Exchange data.

Branka Stojanovi'c and colleagues (2021) The phenomenon referred to as "monetary innovation," commonly referred to as "Fintech," is a response to the emergence of a new business sector in the global market. The utilisation of information technology (IT) for the purpose of automating financial operations is gaining significance due to the widespread adoption of online transactions. The implementation of financial technology (fintech) enables organisations to offer services to a global consumer base, operating continuously throughout the day and night. The accessibility of its services facilitates clients' ability to efficiently do transactions. In reality, the aforementioned advantages, such as those listed above, are factors that progressively stimulate client interest in the field of financial technology. However, the fact that Fintech transactions are created from records poses a significant difficulty in terms of assuring security. The presence of limitations in these systems renders them vulnerable to exploitation through fraudulent demonstrations, resulting in major detrimental consequences for both consumers and suppliers. Consequently, techniques derived from the discipline of artificial intelligence, specifically machine learning, are employed to get a comprehensive understanding of irregularities in financial technology (Fintech) applications. The researchers actively seek out indicators of potentially fraudulent behaviour inside economic data sets and construct predictive models to forecast the actions of prospective wrongdoers. Our contribution to this substantial task involves doing an examination of several tactics aimed at discovering anomalies that are relevant to this particular count. The experiments were sequentially done utilising a limited number of phone datasets sourced from both real-world and synthetic record sources. The observed results offer empirical evidence supporting the notion that machine learning approaches play a role in the detection of extortion, albeit with variable levels of effectiveness. As a result of this, we analyse the suitability of the particular tactics in relation to the rate of exploration. Moreover, it would be advantageous to construct the examination around certain facets of their presentation that were emphasised during their discourse. In the subsequent analysis, we will examine the potential effects of the highlighted consequences on the security of finch programmers within a short timeframe.

Larisa Găbudeanu and colleagues (2021) The current focus in the marketplace has been mostly on the accumulation and analysis of extensive amounts of data regarding transactions and client behaviour, as well as the improvement of algorithms used to detect fraudulent activities. Concurrently, the European Association has also adopted measures, such as the Second Payment Services Directive (PSD2), to exert regulatory pressure on stakeholders in order to detect and prevent fraudulent activities. However, it might be argued that the statute offers a comprehensive representation of the legal obligation at hand. However, the structures inside the market are becoming more extensive in terms of the data collected, particularly in efforts to generalize information for the purpose of generating more precise outcomes. This raises a concern that has not been extensively explored in scholarly literature or by policymakers. Specifically, it pertains to the security implications associated with the practise of creating profiles and collecting data for the purpose of identifying instances of fraud, as well as the accountability of individuals in identifying perpetrators in accordance with data protection laws. This article serves as a significant contribution to the field of research, as it encompasses two main components: (I) an examination of existing methods and approaches for detecting and addressing misrepresentation, considering their implications from a data protection standpoint, and (ii) an analysis of individuals' perspectives on privacy concerns when it comes to fraud detection in transactions, based on a survey conducted with 425 respondents. This article aims to bridge the gap between the implementation of data security regulations and the fulfilment of obligations related to fraud and identity theft under the law. It provides recommendations for achieving compliance with legal requirements while also addressing data protection concerns.

Najem, S.M. et al. (2021) The concept of conducting commercial transactions using digital platforms or online channels enables both companies and individuals to engage in buying and selling activities through the internet. In the contemporary era, characterised by the prevalence of the Internet and the rise of web-based commerce, a substantial amount of information is stored and transferred between various locations. The transmission of information might be vulnerable to exploitation by those engaging in fraudulent activities. There has been a significant increase in misrepresentation, resulting in the loss of a substantial amount of

money worldwide on a daily basis. There are several advanced methodologies for detecting fraud that are often recommended and applied in several industries. The primary problem of the Extortion vicinity pertains to the task of monitoring the activities of a substantial number of clients in order to identify any illicit behavior. Various strategies in information mining and artificial intelligence (AI) have been suggested and implemented in order to effectively mitigate these diverse types of attacks. In the past, several methodologies have been employed for the purpose of detecting fraud, such as Support Vector Machine (SVM), K-nearest Neighbor (KNN), neural networks (NN), Fuzzy Logic, Decision Trees, and others. These many methodologies have shown favorable results, but there is a need to enhance precision even more. This may be achieved by refining the existing methods or by implementing a hybrid learning approach to detect fraudulent activities. This paper presents an audit that aims to show the most recent studies on fraud detection in online commerce between the years 2018 and 2020. Additionally, it provides a comprehensive analysis of the findings obtained and identifies potential challenges for future research endeavors. This information might provide valuable insights into the optimal approaches for effectively presenting the most cost-effective and distinctive solutions for mitigating risks in online commercial transactions..

III. PROPOSED WORK

Machine learning: Machine Learning, sometimes known as ML, is an academic discipline that focuses on the investigation of computer algorithms capable of enhancing their performance via experience and the utilisation of data. In the present study, the researchers aim to investigate the effects of a particular intervention on a This phenomenon is seen as an instance of human-generated reasoning. AI computations, sometimes referred to as "information processing," include the construction of models using sample data to facilitate forecasts or decision-making processes without the need for explicit programming. This phenomenon is commonly referred to as the process of "constructing information." Artificial intelligence (AI) computations are employed in a diverse range of applications, including but not limited to medicine, email categorization, speech recognition, and computer vision. These applications rely on AI calculations due to the inherent challenges or infeasibility of utilizing conventional computations to do the required tasks. Artificial intelligence (AI) computations are utilised in these specific applications. Decision tree, random forests, neural network architecture for mobile devices, and naive. Bayesian networks are a category of artificial intelligence (AI) that are employed in facilitating the interaction between a system and its user. The present study aims to juxtapose the artificial intelligence computation with the procedure of identifying the most accurate findings.

Preprocessing Data: Preprocessing is used to extract, change, standardize, and scale new features that will be used in the AI calculation interaction. Preprocessing is the process through which raw data is converted into information of high quality. The preprocessing technique employed in this study involves the utilization of Principal Component Analysis (PCA), which is sometimes referred to as Guideline Segment Analysis. The main objectives of this technique are the extraction, transformation, standardization, and scaling of the data. Principal component analysis (PCA) is a commonly utilized technique for information compression. Moreover, this approach is commonly employed to mitigate the presence of highlights in data presented on a high-dimensional scale. Principal Component study (PCA) has the potential to simplify complex datasets by transforming them into more comprehensible measurements. This process can unveil latent components that were previously concealed, so enabling a more effective study of the underlying data generation process. Estimations utilizing Principal Component Analysis (PCA) include the inclusion of covariance frames in the computations. These frames serve the dual purpose of constraining and amplifying volatility..

Decision Tree: The use of this approach becomes advantageous in the analysis of extortion-related data, as it allows for the identification of hidden connections among many anticipated data elements and a certain target variable. When utilized as the final representation of various methodologies, decision tree integrates the analysis of deceptive data and its presentation, rendering it an ideal initial step in the process of information dissemination in all cases. A tree is a computational structure commonly employed in supervised learning, where a decision tree proves to be a valuable tool for organising computations. The dataset is partitioned into many subsets based on the decision tree, which is dependent on the decision criteria. The establishment of a correlation between information and yield credits functions as the governing principle for this decision framework.

- Root Hub: This addresses the whole population or test, and moreover, it is partitioned into at least two different parts. The process of parting is required in order to successfully divide a hub into at least two sub-hubs.
- Decision Hub — This refers to the process of breaking up a sub-hub into several smaller sub hubs.
- Leaf or Terminal Hub: Hubs whose functions are unknown are referred to as Leaf or Terminal hubs.
- The act of removing a sub-hub from consideration, also known as "pruning."
- Branch or Sub-Tree: The regions of a tree are referred to as either branches or sub-trees.
- Parent and Child Hub: A hub that is segmented off into smaller hubs for children and parents

Neural Organization: A neural organisation refers to a network or arrangement of neurons within an organism. From a contemporary perspective, a neural organisation might potentially refer to an artificial brain structure comprised of synthetic neurons or hubs. A neural organisation encompasses two distinct types: a natural brain structure composed of biological neurons, and an artificial neural organisation employed for problem-solving purposes in the realm of artificial intelligence. In this manner, a neuronal entity may be classified as either inherent or artificial. The loads serve as a means to show the interactions that are linked to the biological neuron. A positive weight signifies a correlation that promotes excitation, whereas negative qualities imply an inhibitory link. The weights of all the data sources are modified prior to their summation. The term "direct mix" is used to denote the specific action being discussed in this context. In summary, an actuation function is responsible for regulating the appropriate level of output. A commonly accepted range for yield is typically observed to fall within the interval of 0 to 1, however it may also encompass the interval of 1 to 1. The process of determining a numerical value or result through mathematical operations. The essential concept underlying the artificial intelligence technique known as neuronal Organisation is the use of a neuronal framework within the human body, whereby hubs are interconnected, as seen in Figure 1.

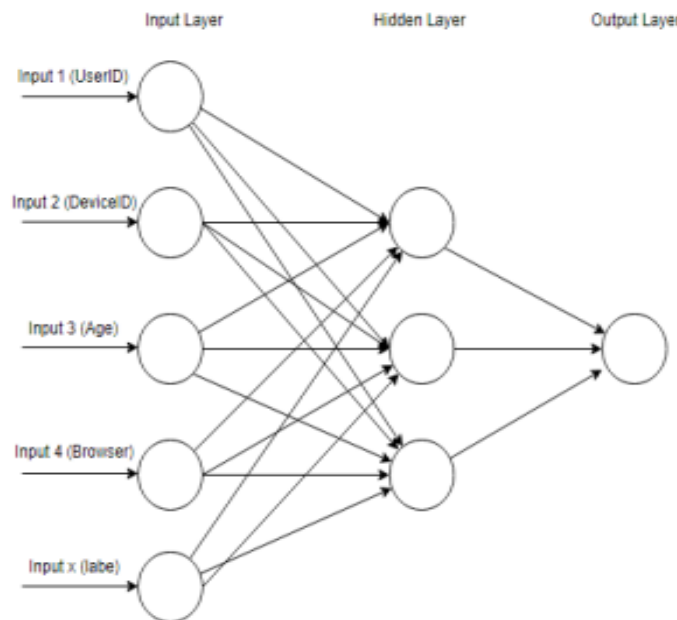


Figure 1: Architecture of Neural Network

IV. CONCLUSION

The Extortion Discovery examination has been in operation for over two decades and has employed various methodologies, including human inspection and client-side authentication, during its duration. Furthermore, artificial intelligence (AI) models have demonstrated significant achievements within this specific field. In recent times, there has been a notable increase in the use of deep learning models across many applications. This may be attributed to the improved computational capabilities and cost-effectiveness associated with these models. This research conducts a comprehensive examination of many artificial intelligence (AI) and deep learning models, assessing them based on several informative metrics in order to detect deceptive

advertisements. The objective of this study is to ascertain the most effective procedures for certain types of datasets, in order to provide suitable suggestions. This paper may potentially enhance people' and organisations' comprehension of the operational dynamics between various methodologies and datasets. Based on our study findings, it can be inferred that Support Vector Machines (SVMs), maybe in combination with Convolutional Neural Networks (CNNs) to enhance the credibility of the results, exhibit superior efficacy in detecting instances of data distortion within larger datasets. Support Vector Machines (SVM), Random Forests, and k-Nearest Neighbours (KNN) are three data collecting techniques that possess the capability to significantly enhance datasets with little records. Convolutional Neural Networks (CNN) exhibit superior performance when compared to alternative deep learning techniques, such as autoencoders, Restricted Boltzmann Machines (RBM), and Deep Belief Networks (DB). This study is subject to some limitations since it just examines the identification of deceptive material inside a simulated educational environment. Controlled learning techniques, such as Convolutional Neural Networks (CNN), K-Nearest Neighbours (KNN), and Arbitrary Timberland, have demonstrated favourable outcomes. However, their efficacy diminishes when applied in dynamic environments. This is in spite of the fact that these algorithms have the semblance of being agreeable. The techniques employed in acts of extortion have gained notoriety for their tendency to undergo evolutionary changes, rendering them difficult to obtain. Acquiring comprehensive sets of fresh information indexes, together with artificial intelligence (AI) models, is important in order to subsequently engage in retraining processes. Autoencoders are generally considered to be the optimal choice in the majority of situations. Taking these factors into account, the structure can be deemed satisfactory, provided that it is only intended for legitimate (i.e., non-deceptive) traffic. Given the aforementioned factors, it may be argued that the proposed framework is a logical and justifiable arrangement. A departure from the established trading protocol is commonly referred to as a fraudulent transaction. Previous studies have provided evidence that the utilisation of auto encoder training, despite its initial costliness, proves to be efficacious in the identification of pertinent indices. The utilisation of a substantial volume of labelled data is frequently observed in the retraining or construction of additional controlled models.

V. REFERENCES

- [1] Adi Saputra, Suharjito, "Fraud Detection using Machine Learning in e-Commerce", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 10, No. 9, 2019.
- [2] Branka Stojanovi'c , Josip Boži'c, Katharina Hofer-Schmitz, Kai Nahrgang, Andreas Weber, Atta Badii, Maheshkumar Sundaram, Elliot Jordan 3 and Joel Runevic, "Follow the Trail: Machine Learning for Fraud Detection in Fintech Applications", Sensors 2021, 21, 1594.
- [3] Elena-Adriana, Gabriela, "Light GBM Machine Learning Algorithm to Online Click Fraud Detection", IBIMA, 2019.
- [4] Evandro Caldeira, Gabriel Brandao, "Fraud Analysis and Prevention in e-Commerce Transactions", 2014 9th Latin American Web Congress, 978-1-4799-6953-1/14 \$31.00 © 2014 IEEE DOI 10.1109/LAWeb.2014.23.
- [5] Gajendra Singh, Ravindra Gupta, Ashish Rastogi, Mahiraj D. S. Chandel, A. Riyaz, "A Machine Learning Approach for Detection of Fraud based on SVM", International Journal of Scientific Engineering and Technology (ISSN : 2277-1581) www.ijset.com, Volume No.1, Issue No.3, pg : 194-198.
- [6] Larisa Găbudeanu, Iulia Brici, Codrut,a Mare, Ioan Cosmin Mihai and Mircea Constantin S, cheau, "Privacy Intrusiveness in Financial-Banking Fraud Detection", Risks 2021, 9, 104.
- [7] S P Maniraj, Aditya Saini, Swarna Deep Sarkar, "Credit Card Fraud Detection using Machine Learning and Data Science", International Journal of Engineering Research, Volume 8 Issue 09, September-2019.
- [8] S. Venkata Suryanarayana, G. N. Balaji , G. Venkateswara Rao, "Machine Learning Approaches for Credit Card Fraud Detection", International Journal of Engineering & Technology, 7 (2) (2018) 917-920.
- [9] Suha M. Najem, Suhad M. Kadeem, "A Survey On Fraud Detection Techniques in E-Commerce", Techknowledge Journal, Volume 1, Issue 1, 2021.
- [10] Tuyls, B. Vanschoenwinkel, B. Manderick. "Credit Card Fraud Detection Using Bayesian and Neural Networks", BioData Mining, 2013.