Volume 9, Issue 7, July – 2024 International Journal of Innovative Science and Research Technology
ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUL959

Using Machine Learning Models to Detect the Increasing Threats of Financial Fraud in the Cyberspace

Atta Yaw Agyeman[1]; Samuel Gbli Tetteh[2]
D Jarvis College of Computing and Digital Media, DePaul University, Chicago, USA

Abstract:- In the dynamic landscape of the financial sector, the escalating menace of financial fraud presents pervasive implications for businesses and consumers alike. Particularly, detecting credit card fraud in real-time transactions has become a pivotal concern within the financial industry. This abstract delves into the critical role of data mining in addressing the complexities of credit card fraud detection, shedding light on the multifaceted challenges that confront this domain. The realm of financial business is increasingly besieged by the spectre of financial fraud, necessitating robust measures to combat its detrimental effects. As the sophistication and prevalence of fraudulent activities continue to evolve, the imperative of deploying effective strategies for fraud detection becomes more pronounced. Applying data mining techniques in this context is paramount in identifying and mitigating credit card fraud. Leveraging advanced data mining methodologies is essential for scrutinising live transactions and discerning anomalous patterns indicative of fraudulent behaviour. Credit card fraud detection poses formidable challenges, primarily attributable to two compelling factors. Firstly, the inherent dynamism of normal and fraudulent behavioural profiles engenders a perpetual need for adaptive and responsive detection mechanisms. Secondly, the highly imbalanced nature of credit card fraud data sets further complicates accurately identifying fraudulent activities, necessitating nuanced approaches to discern anomalies amidst voluminous transactional data effectively. In light of the foregoing, this abstract underscore the criticality of data mining in addressing the intricate landscape of credit card fraud detection, emphasising the need for agile and sophisticated methodologies to navigate the evolving nature of fraudulent behaviours and the skewed distribution of fraud-related data sets. By comprehensively elucidating these challenges, this abstract provides a foundational understanding of the nuanced complexities inherent in combatting financial fraud through the lens of data mining.

Keywords:- *Fraud Detection; Support Vector Machine Classifier; Naïve Bayes Classifier; Random Forest; Majority Voting.*

I. INTRODUCTION

The proliferation of credit cards and electronic payments worldwide has surged in recent decades, offering consumers convenience and accessibility across various platforms such as ATMs, POS terminals, the Internet, and telephony networks [1]. However, this rapid adoption has also ushered in a commensurate rise in financial fraud, posing significant global challenges to banking institutions, corporations, and governments. Fraud, characterised by illicit deception aimed at monetary gain, has become increasingly prevalent, particularly in credit card transactions, where the reliance on Internet technologies has created fertile ground for fraudulent activities.

Despite security guidelines issued by regulatory bodies like the European Banking Authority (EBA) to mitigate online payment risks, fraud continues to evade conventional deterrents [1]. In 2015, global losses attributed to fraudulent transactions on general-purpose payment cards amounted to $21.84 billion, underscoring the urgency for more effective preventive measures.

II. RELATED WORKS

In contemporary society, data proliferation from diverse sources, including human activities and digital devices, continues to expand exponentially, fueling the need for automated systems capable of processing and interpreting this wealth of information [2]. Machine learning, a cornerstone of modern data analytics, has emerged as a powerful tool for discerning patterns and trends within vast datasets.

The fraud detection domain, particularly in credit card transactions, represents a pivotal application of machine learning algorithms, often framed as a classification challenge in data mining [2]. Notably, the advent of credit cards as a ubiquitous form of cashless payment has spurred legitimate and fraudulent transactions. The confluence of advanced technologies and evolving fraud tactics necessitates innovative approaches to detection and prevention.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUL959

A. Credit Card

The evolution of credit cards as the preferred cashless payment mode underscores their ubiquitous presence in contemporary commerce [3]. From 2008 to 2013, non-cash payments surged to 61% in Singapore and 45% in the United States, reflecting a global shift towards electronic transactions [3]. Despite their convenience, credit card transactions are marred by significant fraud losses, with global fraud reaching $21.84 billion in 2015 [4].

Efforts to combat fraud have spurred the exploration of various detection models, including expert systems, machine learning, and deep learning [5][6]. However, the effectiveness of traditional techniques remains suboptimal, necessitating novel approaches to enhance fraud detection capabilities.

B. Credit Card Fraud

The pervasive nature of credit card fraud poses formidable challenges to consumers and financial institutions alike, with billions of dollars lost annually due to fraudulent activities [7]. While machine learning algorithms offer promise in identifying fraudulent transactions, the complexity and sophistication of modern fraud schemes demand adaptive and robust detection mechanisms [8].

Despite advancements in fraud detection methodologies, challenges persist in accurately identifying fraudulent transactions amidst vast datasets characterised by imbalanced distributions and privacy concerns [9]. The emergence of sophisticated fraud tactics underscores the imperative for continuous innovation in detection strategies.

C. Credit Card Fraud Detection

Classification algorithms serve as foundational tools in credit card fraud detection, facilitating categorising transactions into legitimate or fraudulent categories [10]. Techniques such as Naïve Bayes, Support Vector Machines, Random Forests, and Majority Voting offer diverse approaches to identifying fraudulent activities, each with its unique advantages and limitations [11].

Addressing the challenges of unbalanced datasets and data scarcity, researchers confront the inherent complexities of fraud detection, navigating the delicate balance between accuracy and scalability [12]. As fraud detection evolves, novel methodologies and interdisciplinary collaborations are essential to confront emerging threats effectively.

D. Challenges in Credit Card Fraud Detection

The landscape of credit card fraud detection is fraught with challenges, including imbalanced datasets, data scarcity, and computational constraints [13]. Imbalanced data distributions, where fraudulent transactions represent a minority subset, pose significant hurdles to accurate detection [14]. Moreover, the reluctance of financial institutions to disclose transaction data hampers research efforts, limiting access to real-world datasets [15].

E. Experimental Setup

This section delineates the experimental framework for evaluating credit card fraud detection algorithms. The dataset comprises simulated mobile-based payment transactions sourced from Kaggle, encompassing 284,807 transactions over two days in September 2013, with 492 instances of fraudulent activity [16].

Preprocessing techniques, including Principal Component Analysis (PCA), transform and format the dataset for model training and evaluation [16]. Classification algorithms such as Naïve Bayes, Support Vector Machines, and Random Forests are evaluated for their efficacy in distinguishing between legitimate and fraudulent transactions, with performance metrics such as accuracy, precision, and recall used to assess model effectiveness [17][18]. Through rigorous experimentation and analysis, researchers seek to elucidate the strengths and limitations of various fraud detection methodologies, paving the way for enhanced security measures in financial transactions.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUL959

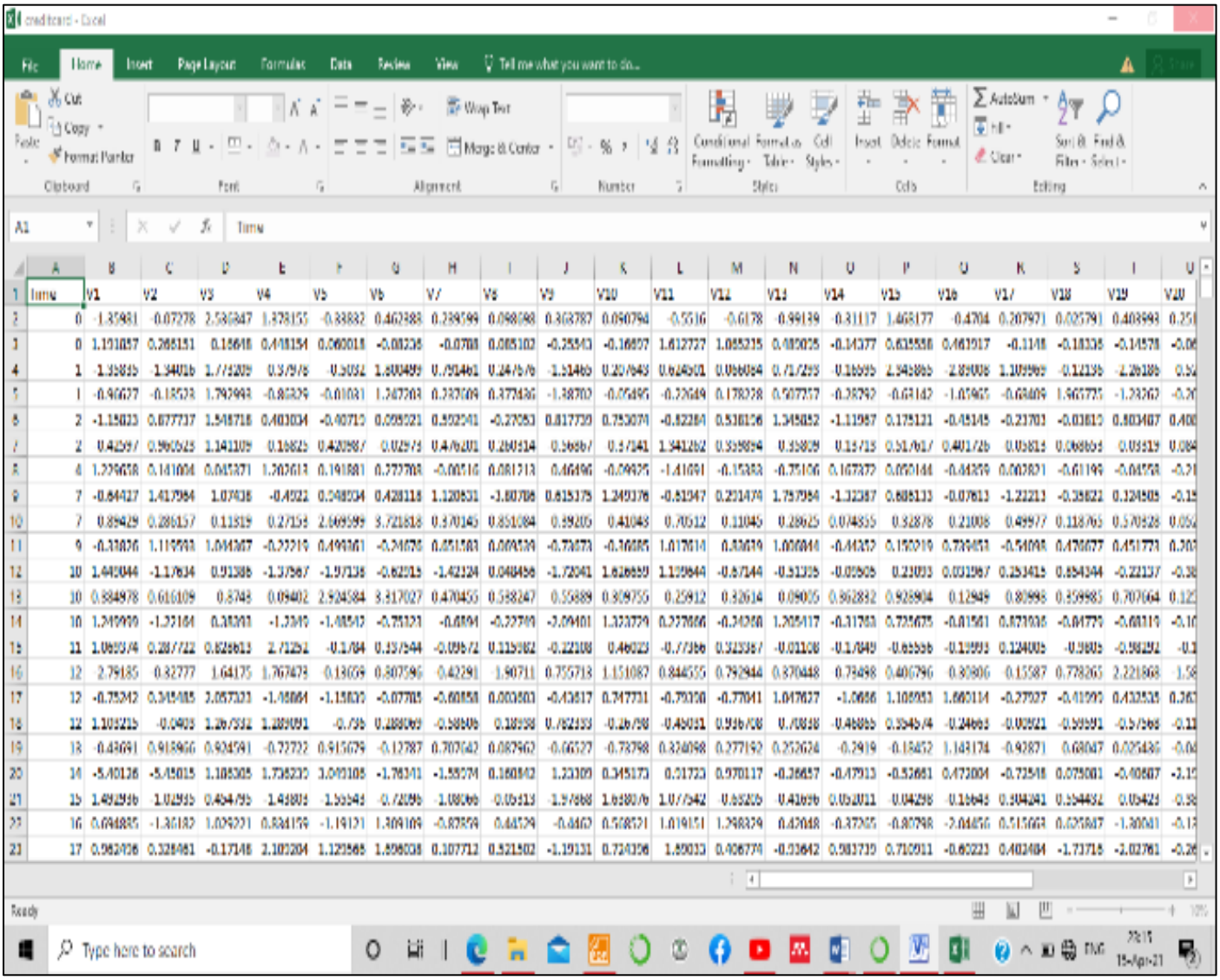

Fig 1: Screenshot of the Dataset

F. Data Cleaning

Following dataset analysis, the imperative next step involves data cleaning to ensure the integrity and reliability of the information. This crucial phase entails eliminating duplicate and null values within the dataset, thus laying the foundation for robust analysis and model development.

III. NAÏVE BAYES CLASSIFIER

In the seminal work by [2], the Naïve Bayes classifier emerges as a pivotal mathematical tool rooted in Bayesian theory. Leveraging Bayesian probability, this algorithm excels in decision-making by selecting the outcome with the highest likelihood, rendering it both efficient and scalable. Notably, Naïve Bayes operates on conditional independence among data features, enabling the integration of prior knowledge and logical reasoning into classification tasks.

$$P(c_i|f_k) = \frac{P(f_k|c_i) * P(c_i)}{P(f_k)} \qquad (1)$$

$$P(f_k|c_i) = \prod_{i=1}^{n} P(f_k|c_i) \;\; k = 1, \dots, n; i = 1,2 \qquad (2)$$

Central to its operation are conditional probability equations (1) and (2), which underpin the classification process by computing the likelihood of a given feature belonging to a specific class. By comparing these probabilities, the Naïve Bayes classifier delineates between binary classes, facilitating the identification of fraudulent and non-fraudulent transactions with remarkable accuracy.

If $P(c_1|f_k) > P(c_2|f_k)$ *then the classifier is* C_1
If $P(c_1|f_k) < P(c_2|f_k)$ *then the classifier is* C_2
c_i is the target class for the classification;

Where C_1, the negative is is class (genuine case) and C_2 is the positive class (fraud case)

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUL959

IV. SUPPORT VECTOR MACHINES (SVM)

In the groundbreaking study by [19], Support Vector Machines (SVM) emerge as a formidable pattern recognition and classification tool. This sophisticated classifier excels in discerning trends and patterns within datasets, particularly in fraudulent transaction detection. SVM's versatility lies in its ability to categorise data into two distinct groups, leveraging a linear classifier to delineate fraudulent and non-fraudulent transactions.

At the heart of SVM lies the optimisation problem (5), wherein the algorithm seeks to minimise classification errors while maximising the margin of separation between data points. Through the judicious selection of hyperplanes, SVM constructs a decision boundary that maximises the margin between fraudulent and non-fraudulent transactions, thereby enhancing classification accuracy.

$$f(x) = sgn(x.w) + b \quad (3)$$

Where x is the input vector which contains weight and b is a constant. Eqn (3) is used to find the decision boundary between two classes. The parameter values of w and b have to be learned by the SVM on the training phase and b are derived by maximizing the margin of separation between the two classes. The criterion used between by SVM is based on the margin maximization between the two classics

The margin is the distance between the two hyper planes. To find the hyper plane $H: y = w.x + b = 0$ and two hyper planes $H1: y = w.x + b = +1\ and\ H2: y = w.x + b = -1$

The threshold separating the two classes is H and the two margin boundaries are H1 and H2. Then the margin is $\frac{2}{||w||}$, where $||w||$the norm of the vector w is. In non-perfectly separable case, the margin is soft. That there is a chance of misclassification error. The misclassification errors should be minimized. It is minimized by introducing the slack variable ε_i. If $\varepsilon_i = 0$ then the classes are correctly classified. Let ε_i is non-negative slack variable for misclassifications.

y is the indicator of the class, where in the case of fraud detection $y = 1$ for the positive and $y = -1$ is the class for the negative class.

SVM requires that either

$w.x + b \geq 1 - \varepsilon_i\ or$

$x.w + b \geq -1 + \varepsilon_i$ which is simplified in eqn 4

$$y_i(x.w + b) \geq 1 - \varepsilon_i \quad (4)$$

Where i=1,2

The optimization problem for the calculation of w and b is given below in eqn 5

$$min\frac{1}{2}||w||^2 + C\sum_{i=1}^{n}\varepsilon_i \quad (5)$$

Subject to;

$$y_i(x.w + b) \geq 1 - \varepsilon_i \qquad \varepsilon_i \geq 0$$

By minimizing the $\frac{1}{2}||w||^2$ the complexity of SVM is reduced and by minimizing the slack variable the misclassification errors are reduced. C is a regularization parameter which weighs the classification errors. And it is the tradeoff between the two classes. The constrained optimization problem is solved by using the Lagrange function in eqn (5)

$$L(w,b,\varepsilon,\alpha,\beta) = \frac{1}{2}\left|\left|w\right|\right|^2 + C\sum_{i=1}^{n}\varepsilon_i - \sum_{i=1}^{n}\alpha_i - \{y[wx + b] - 1 + \varepsilon_i\} - \sum_{i=1}^{n}\beta_i\varepsilon_i \quad (6)$$

The solution of this optimization problem is obtained by minimizing $w, b\ and\ \varepsilon$ and maximizing $\alpha\ and\ \beta$. It is better to solve the problem by introducing the dual formulation in 7

$$\max_{\alpha\beta} w(\alpha,\beta) = \max_{\alpha\beta}\left\{\min_{\alpha,b,\varepsilon}(w,b,\varepsilon,\beta)\right\} \quad (7)$$

By substituting this, the problem is transformed into its dual formulation, as given by

$$max\left\{\sum_{i=1}^{n} a - \sum_{i=1}^{n}\sum_{j=1}^{n} a_i a_j y_i y_j \langle x_i y_j\rangle\right\} \quad (8)$$

And is maximized under the constraints,

$$\sum_{i=0}^{n} a_i y_i = 0\ and\ 0 \leq a_i \leq C\ for\ i = 1,2\ldots.,n.$$

The Kuhn-Tucker condition in eqn (9) is applied to eqn (8)

$$a_i\{y_i[w.x_i + b] - 1 + \varepsilon\} = 0 \quad (9)$$

$$where\ i = 1,2\ldots\ldots,n$$

The Lagrange vectors are the vectors needed to describe the hyper plane. In linearly separable data, all support vectors lay on the margin. The decision boundary is determined by the equation (10).

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUL959

$$f(x) = \sum_{i=0}^{Ns} a_i y_i \langle x, x_i \rangle + b \quad (10)$$

Where x is the input vector, (x, x_i) is the inner product, Ns is the number of support vectors, and b is the bias term.

V. MAJORITY VOTING

A pioneering approach to data classification, Majority Voting, as elucidated by Randhawa et al. (2018), harnesses the collective intelligence of multiple classifiers to render predictions. By aggregating individual predictions from diverse algorithms, Majority Voting synthesises a combined output, thus enhancing the robustness and reliability of classification outcomes.

Formally defined in equation (11), Majority Voting capitalises on the collective wisdom of classifiers to discern the most probable class for a given input. Majority Voting furnishes a final prediction by summating votes across multiple classifiers, affording enhanced accuracy and resilience against classification errors.

Consider K target classes (labels) with $C_i, \forall_i \in \Lambda = \{1, 2, \dots \dots, K\}$ represent the $i - th$ target class predicted by a classifier.

Given an input, x each classifier provides a prediction concerning the target class, yielding a total of K predictions, i.e. $P_1, \dots ., P_K$

Majority voting aims to produce a combined prediction for input $x, P_{(x)} = j, j \in \Lambda$ from all the K predictions, ie $P_k(x) = j_k, k = 1, \dots, K$

A binary function is employed to represent the votes, i.e.

$$V_k(x \in C_i) = \begin{cases} 1, if\ P_k(x) = i, i \in \Lambda \\ 0, otherwise \end{cases} \quad (11)$$

Then, sum the votes from all K classifiers for each C_i and the label that receives the highest votes is the final (combined) predicted class.

VI. PERFORMANCE EVALUATION AND RESULTS

In evaluating classifier performance, a suite of metrics, including True Positive Rate (TPR), True Negative Rate (TNR), False Positive Rate (FPR), and False Negative Rate (FNR), emerge as indispensable tools. These metrics, delineated in equations (12) to (15), provide nuanced insights into classifier accuracy, precision, and sensitivity across diverse classification scenarios.

Furthermore, performance metrics such as Accuracy, Precision, F1 Score, and Balanced Accuracy serve as yardsticks for assessing classifier efficacy in imbalanced binary classification problems. Through a comprehensive evaluation of Naïve Bayes, Support Vector Machines, and Hybrid classifiers, researchers glean valuable insights into classifier performance, culminating in identifying optimal models for fraudulent transaction detection.

In the empirical analysis, the proposed Hybrid classifier demonstrates significant improvements in True Positive Rate, True Negative Rate, and False Negative Rate values, underscoring its efficacy in discerning fraudulent activities with unprecedented accuracy and precision.

Four basic metrics are used in evaluating the experiments, namely True Positive Rate (TPR), True Negative Rate (TNR), False Positive Rate (FPR) and False Negative Rate (FNR) metric respectively.

$$\text{TPR} = \frac{\text{TP}}{\text{P}} \quad (12)$$

$$\text{TNR} = \frac{\text{TN}}{\text{N}} \quad (13)$$

$$\text{FPR} = \frac{\text{FP}}{\text{N}} \quad (14)$$

$$\text{FNR} = \frac{\text{FN}}{\text{P}} \quad (15)$$

The performance of Naïve bayes, Support Vector Machines and the proposed Hybrid classifiers are evaluated based on Accuracy, Precision, F1 Score, Sensitivity, Specificity, Balanced Accuracy, Prevalence, False Alarm Rate and Balanced classification Rate. These evaluation metrics are implored based on their relevance in evaluating imbalanced binary classification problem.

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{FP} + \text{TN} + \text{FN}} \quad (16)$$

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}} \quad (17)$$

$$\text{Sensitivity} = \frac{\text{TP}}{\text{TP} + \text{FN}} \quad (18)$$

$$\text{F1 Score} = 2 * \frac{\text{Precision} * \text{recall}}{\text{Precision} + \text{recall}} \quad (19)$$

$$\text{Specificity} = \frac{\text{TN}}{\text{TN} + \text{FP}} \quad (20)$$

$$\text{Balanced Accuracy} = \frac{\text{sensitivity} + \text{specificity}}{2} \quad (21)$$

$$\text{Prevalence} = \frac{\text{FP} + \text{FN}}{\text{TP} + \text{FP} + \text{FN} + \text{TN}} \quad (22)$$

$$\text{False Alarm Rate} = \frac{\text{FP}}{\text{FP} + \text{TN}} \quad (23)$$

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUL959

VII. RESULTS

This study developed and evaluated three distinct classifier models: Naive Bayes, Support Vector Machines (SVM), and Random Forest. The dataset was partitioned, with 70% allocated for training and 30% reserved for validation and testing purposes. The evaluation metrics employed to assess the performance of these classifiers encompassed a comprehensive array, including accuracy, sensitivity, specificity, precision, prevalence, F1-Score, and balanced classification rate.

Upon meticulous analysis of the metric tables, noteworthy improvements in key performance indicators were discerned, particularly within the proposed model. Specifically, significant enhancements were observed in the True Positive Rate, True Negative Rate, and False Negative Rate values, indicative of the model's heightened efficacy in accurately identifying fraudulent transactions while minimising false negatives.

The utilisation of diverse evaluation metrics facilitated a nuanced understanding of each classifier's strengths and weaknesses, enabling informed decision-making regarding their applicability in real-world scenarios. Moreover, the meticulous partitioning of the dataset for training, validation, and testing purposes ensured the robustness and reliability of the findings, underscoring the study's methodological rigour and validity.

In essence, the results of this study underscore the pivotal role of classifier selection and performance evaluation in the domain of fraudulent transaction detection. Through a judicious combination of algorithmic approaches and comprehensive evaluation frameworks, researchers can harness the full potential of machine learning techniques to mitigate financial risks and safeguard against fraudulent activities in contemporary financial ecosystems.

Table 1: Performance Results for the Three Classifiers

Metrics	Classifiers			
	SVM	NB	RF	Majority Voting
Accuracy	0.998	0.980	0.760	0.999
Sensitivity / Recall	0.670	0.890	0.725	0.950
Precision	0.890	0.530	0.855	0.985
F1-Score	0.730	0.550	0.780	0.905
False Alarm Alert	0.002	0.020	0.240	0.001

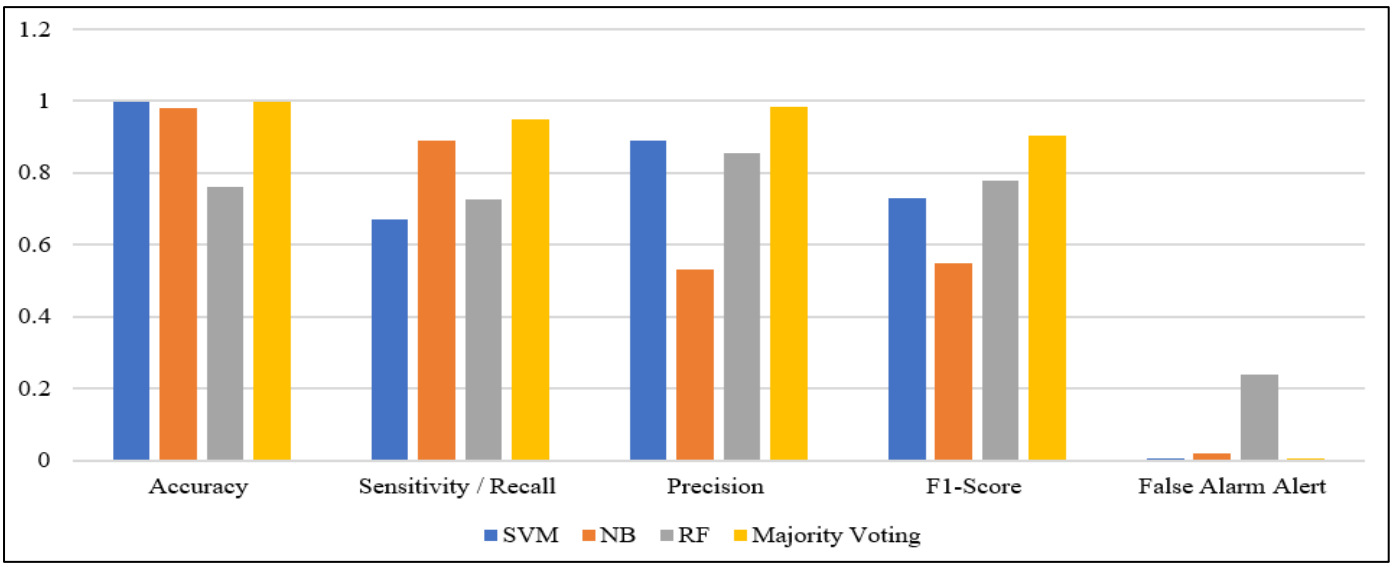

Fig 2: Performance Results for the Three Classifiers

VIII. COMPARATIVE ANALYSIS OF MACHINE LEARNING MODELS

In this study, we conducted a rigorous comparative analysis of four distinct machine learning models: Support Vector Machine (SVM), Naïve Bayes (NB), Random Forest, and Majority Voting. The objective was to evaluate their performance across key metrics and ascertain their efficacy in addressing the challenges of skewed datasets common in fraudulent transaction detection.

Among the individual models assessed, Support Vector Machines exhibited the highest level of accuracy, boasting an impressive rate of 99.8%. Following closely behind, Naïve Bayes demonstrated commendable performance with an accuracy of 98%, while Random Forest yielded a respectable accuracy of 76%. However, it is noteworthy that Random Forest's accuracy fell short compared to SVM and NB.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUL959

The utilisation of Majority Voting, a technique leveraging simple majority, yielded promising results, with accuracy rates ranging from 100% to 99% and an average accuracy of 99.9%. This underscores the potential of ensemble methods in enhancing predictive accuracy by amalgamating diverse models' outputs.

Interestingly, while Support Vector Machines showcased exceptional accuracy, its performance in terms of sensitivity, a critical measure particularly pertinent to skewed datasets, was relatively moderate. In contrast, the Majority Voting model exhibited notable improvements in sensitivity, outperforming individual models such as SVM and NB. Specifically, SVM achieved a sensitivity rate of 67%, whereas NB attained 89%. However, upon employing Majority Voting, the resultant model achieved a sensitivity rate of 88%, representing a substantial improvement over NB by approximately 21%.

These findings highlight the nuanced interplay between model selection, dataset characteristics, and performance metrics in the context of fraudulent transaction detection. Moreover, they underscore the significance of ensemble techniques like Majority Voting in mitigating the limitations inherent in individual models, thereby enhancing overall predictive capabilities.

Furthermore, the study underscores the potential for further advancements, particularly in enhancing SVM's performance through training on larger, more balanced datasets. By leveraging the strengths of diverse machine learning models and adopting sophisticated ensemble strategies, researchers can foster robust fraud detection frameworks capable of adapting to evolving threat landscapes and safeguarding financial ecosystems against illicit activities.

IX. CONCLUSION

The landscape of credit card fraud detection is evolving rapidly, driven by advancements in machine learning techniques. However, many existing methodologies excel primarily in post-fraud identification scenarios, presenting challenges in real-time detection and preemptive action against fraudulent activities. The crux of this challenge lies in the disproportionate distribution of fraudulent transactions, which typically account for a mere 1% of total transactions, rendering genuine fraud data scarce and inhibiting the development of robust detection frameworks.

The scarcity of authentic fraudulent data significantly impedes the exploration and implementation of effective fraud detection techniques. Consequently, the repertoire of methodologies employed in this domain remains relatively limited, hindering progress in the field. Innovative approaches are imperative to surmount these challenges and enhance the efficacy of fraud detection systems.

One promising avenue for addressing these drawbacks is the adoption of a Hybrid Approach, which involves amalgamating multiple detection techniques to harness their collective strengths and mitigate individual limitations. By integrating diverse methodologies, hybrid models have the potential to yield superior accuracy, reliability, and sustainability in fraud detection endeavours.

Integrating disparate techniques facilitates a comprehensive analysis of transactional data, enabling the identification of nuanced patterns indicative of fraudulent behaviour in real-time scenarios. Moreover, hybrid models offer a versatile framework adaptable to evolving fraud schemes, thereby enhancing the resilience of detection systems against emerging threats.

In conclusion, while challenges persist in credit card fraud detection, adopting hybrid approaches represents a promising strategy for overcoming existing limitations and advancing the efficacy of fraud detection mechanisms. By leveraging the synergies between diverse methodologies, hybrid models can revolutionise fraud detection practices, safeguard financial ecosystems, and preserve consumer trust in digital transactions. As research in this domain continues to evolve, the development and refinement of hybrid approaches are poised to play a pivotal role in enhancing the security and integrity of global financial systems.

REFERENCES

[1]. H. Harwani, J. Jain, C. Jadhav, and M. Hodavdekar, “Credit Card Fraud Detection Technique using Hybrid Approach: An Amalgamation of Self Organizing Maps and Neural Networks,” *Int. Res. J. Eng. Technol.*, no. July, pp. 5071–5075, 2020, [Online]. Available: www.irjet.net

[2]. J. O. Awoyemi and S. A. Oluwadare, “Credit card fraud detection using Machine Learning Techniques : A Comparative Analysis,” 2017.

[3]. S. Wang, G. Liu, Z. Li, S. Xuan, C. Yan, and C. Jiang, “Credit Card Fraud Detection Using Capsule Network,” *Proc. - 2018 IEEE Int. Conf. Syst. Man, Cybern. SMC 2018*, pp. 3679–3684, 2019, doi: 10.1109/SMC.2018.00622.

[4]. A. I. Kokkinaki, “On atypical database transactions: Identification of probable frauds using machine learning for user profiling,” *Proc. IEEE Knowl. Data Eng. Exch. Work. KDEX*, pp. 107–113, 1997, doi: 10.1109/kdex.1997.629848.

[5]. Y. Kültür and M. U. Çağlayan, “Hybrid approaches for detecting credit card fraud,” *Expert Syst.*, vol. 34, no. 2, pp. 1–13, 2017, doi: 10.1111/exsy.12191.

[6]. A. Dal Pozzolo, G. Boracchi, O. Caelen, C. Alippi, and G. Bontempi, “Credit card fraud detection: A realistic modeling and a novel learning strategy,” *IEEE Trans. Neural Networks Learn. Syst.*, vol. 29, no. 8, pp. 3784–3797, 2018, doi: 10.1109/TNNLS.2017.2736643.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUL959

[7]. E. Aleskerov, B. Freisleben, and B. Rao, "CARDWATCH: A neural network based database mining system for credit card fraud detection," *IEEE/IAFE Conf. Comput. Intell. Financ. Eng. Proc.*, pp. 220–226, 1997, doi: 10.1109/cifer.1997.618940.

[8]. K. Randhawa, C. K. Loo, M. Seera, C. P. Lim, and A. K. Nandi, "Credit Card Fraud Detection Using AdaBoost and Majority Voting," *IEEE Access*, vol. 6, pp. 14277–14284, 2018, doi: 10.1109/ACCESS.2018.2806420.

[9]. P. K. Chan, L. Ave, and N. York, "Distributed Data Mining in Credit Card Fraud Detection 1 Introduction," pp. 1–17, 1999.

[10]. A. O. Toluwase and S. A. Olumide, "A framework for detecting credit card f...sitive meta-learning ensemble approach.pdf." p. 15, 2020.

[11]. V. Dheepa and R. Dhanapal, "Hybrid Approach for Improvis...on Collective Animal Behaviour and SVM.pdf." p. 10, 2013.

[12]. N. Shirodkar, R. Sakhalkar, P. Mandrekar, K. M. C. Kumar, R. S. Mandrekar, and S. Aswale, "Credit Card Fraud Detection Techniques – A Survey," pp. 1–7, 2020, doi: 10.1109/ic-ETITE47903.2020.112.

[13]. H. Jiawei, Micheline Kamber, and P. Jian, *Data Mining Concepts and Techniques*, Third Edit. 225Wyman Street, Waltham: Morgan Kaufmann Publishers, 2012.

[14]. D. M. B, B. Janani, S. Gayathri, and N. Indira, "CREDIT CARD FRAUD DETECTION USING RANDOM FOREST," pp. 6662–6666, 2019.

[15]. I. Kaur and M. Kalra, "Ensemble Classification Method for Credit Card Fraud Detection," no. 3, pp. 423–427, 2019, doi: 10.35940/ijrte.C4213.098319.

[16]. M. Zareapoor and P. Shamsolmoali, "Application of Credit Card Fraud Detection_ Based on Bagging Ensemble Classifier.pdf." International Conference On Intelligent Computing Communication & Convergence, p. 8, 2015.

[17]. F. N. Ogwueleka, "DATA MINING APPLICATION IN CREDIT CARD FRAUD DETECTION SYSTEM," vol. 6, no. 3, pp. 311–322, 2011.

[18]. S. K.R. and M. Zareapoor, "FraudMiner: A Novel Credit Card Fraud Detection Model Based On Frequent Itemset Mining." Hindawi Publishing Corporation, p. 11, 2014.

[19]. V. Dheepa and R. Dhanapal, "BEHAVIOR BASED CREDIT CARD FRAUD DETECTION USING SUPPORT VECTOR MACHINES," vol. 6956, no. July, pp. 391–397, 2012, doi: 10.21917/ijsc.2012.0061.