RESEARCH
www.commprac.com
ISSN 1462 2815

# IoT AND MACHINE LEARNING IN NONPROFIT MANAGEMENT TRANSFORMING SOCIAL AND ECONOMIC DEVELOPMENT PRACTICES

**P. Rajendran [1]*, Lavakush Singh [2], D. Barani [3] and Meera K. L [4]**

[1] Department of Management Studies, Chinmaya Vishva Vidyapeeth,
Deemed to be University, Ernakulam, Kerala, India.
*Corresponding Author Email: rajuprofessor.mba@gmail.com
[2] Department of Financial Management, Saibalaji International Institute of
Management Sciences, Pune, Maharashtra, India. Email: l.singh@sbiims.edu.in
[3] Department of Management Studies, Sharda University,
Uttar Pradesh, India. Email: d.barani@sharda.ac.in
[4] Centre of Management Studies, JAIN Deemed-to-be University,
Bengaluru, India. Email: meera_kl@cms.ac.in

**DOI: 10.5281/zenodo.11615948**

**Abstract**

This research intends to contribute to the exploration of the applicability of Internet of Things and Machine Learning in non-profit management. One of the problems that many non-profit organizations cannot avoid is connected with fraud and mismanagement of funds, which can impact the efficiency of the organization and decrease the trust of donors. This research will use IoT data from financial transactions and the way users interact with the educational platform. The results demonstrate the effectiveness of these algorithms in detecting fraudulent activities. Random Forest is able to achieve an accuracy of 95% and pinpoint transaction amount and user ID as significant features. GBM also shows strong performance in terms of R-squared and log-loss, with the R-squared being 0.87 and log-loss being 0.12. Finally, both SVM and KNN can reach a high accuracy of 94% and 92%, respectively, with precision, recall, and F1-score all being well-balanced. The research highlights the significant opportunities of IoT and ML application in the sphere of non-profit management, which allows for more efficient operation of businesses and preservation of their financial integrity. In the future, it is possible to develop and refine these algorithms and pay more attention to the identified challenges, such as privacy and other ethical concerns. As a result, more non-profits will have the ability to use breakthrough technologies that address the risks of fraud, distribution of funding, and opportunities for maintaining the integrity of their finance.

**Keywords:** Nonprofit Management, IoT, Machine Learning, Fraud Detection, Educational Platforms.

## 1. INTRODUCTION

Nonprofit organizations are the entities that provide the most drive to the social and economic development of countries and cover all the spheres of social activity of the world at the different levels. Nonprofit organizations function with the purposes of meeting the pressing needs of the society or some population that is defined as needy where both the functions of governments are defective and markets cannot solve these problems. These needs can be of different origin, be it health, educational, ecological problems or community needs. They play an important role in providing the economic and social development of the country as donors' and volunteers' money is used effectively for meeting social needs and advocating different issues [1]–[3].

At the same time, the contemporary nonprofit organization is the complex of factors that are maximally involved in their operation to obtain the most important results, having a number of challenges so that their operations can be ineffective and counterproductive. The most important problem of this kind of organization is their control and distribution of resources. Especially dangerous is the appearance of the

fraud types in these organizations, as important and worthy organizations they are completely dependent on the donations of people and grants of some organizations. Some types of fraud in the non-profit organization are common for businesses: this is the financial misreporting and embezzlement or laundering of the money. Several types of fraud are specific to non-profit organizations, as for example the misuse of funds or the excessive and unjustified compensation. There are many risks of development of fraud of these types: many problems are not or cannot be remembered to be fraud; a non-profit organization has no competencies in the sphere of financial and resource management [2]–[5].

Recently, the technologies of the Internet of Things and Machine Learning have been increasingly introduced and integrated in the managing of nonprofits in terms of detecting and preventing fraud. It is the growth of IoT devices that has increased as a result of the vast amount of data that they accumulate. These data are duly related to the processes within organizations and cover different aspects such as interaction with donors or financial transactions, to name a few examples. Inasmuch as guided by ML algorithms, these data aim to help nonprofit organizations, they allow detecting patterns which are explicitly or implicitly deemed to be risky and fraudulent and apply relevant measures to prevent them [6]–[8].

Since complex systems and the interaction of data with each other should be taken into account, along with the enormous volumes, to predict fraud, the relevant ML algorithms Random Forest, Gradient Boosting Machines, Support Vector Machines, and K-Nearest Neighbors are to be applied in order to assess and evaluate the data. The first kind of algorithms can help understand what are the most important features in the dataset and provide bad-rate estimate though out-of-bag error rates, while the last two algorithms can give information concerning accuracy of the individual metrics as well as precision, recall, and F1-score [9]–[11].

IoT and ML technologies in nonprofit management are not only limited to the detection of fraud, as they can be used to ensure more effective resource allocation and more efficient, effective, and impactful programs. By utilizing real-time data provided by IoT devices that track the implementation of a particular program, the nonprofit will be able to enhance its decision-making processes relative to the allocation of resources to it. The timely insight will also enable the program supervisors to determine whether the program is effective as implemented.

## 2. LITERATURE REVIEW

The integration of Internet of Things and Machine Learning technologies is increasingly used throughout all industries and promises significant improvements to management practices, nonprofits can benefit from this trend in truly revolutionary ways. The current assignments reviews the related literature and analyses the main conceptual points regarding how exactly the IoT devices and Machine Learning applications can help improve the processes of fraud detection and prevention and provides common machine learning algorithms used in this context [8], [12], [13].

Using IoT devices, the nonprofit organization can gain and utilize vast amounts of real-time data in various areas of their work, whether it is related to financial transactions, donor activism, or efficiency of program funding and implementation. All of the resulting data can be used in improving decision-making and solving various aspects of resource allocation, ensuring the implementation of statistical models, and

enhancing general effectiveness and efficiency of the organization. Thus, nonprofits, whether small or big, can use these technologies to improve and maximize their positive impact and ensure transparency and responsibility of their work [14]–[16].

Concerning the problem of fraud detection and prevention, it should be noted that about nonprofit organizations, and since these volunteers depend on the trust of donors in this issue, there differences in the conditions of their work and implementation of the most technologies. Several cases showed that IoTs and ML algorithms are suitable for recognizing fraud. According to the study demonstrated that the IoTs generated a huge amount of data because sensors were positioned at different levels of financial transactions and that the ML algorithm could trigger these data iot, clustering the data in the data center, and the model generated the best result. As such case described the application of gradient boosting machines to the detection and prevention of fraud. The GBM settled the challenge of active supervision, as the model acquired suspicious activity that might have provided non-profits with necessary real time notices of the event [17]–[19].

Machine learning algorithms are of great importance to the nonprofit in the context of considering fraud scenarios. Thus, Random Forest is broadly used in this type of organization for the above-mentioned purpose since it allows for incorporating a large database and pinpointing significant variables that are the sources of fraud risk. The technique processes multiple decision trees to predict which transactions are more likely to be fraudulent, for example, on the bases of the amount of transaction, frequency, and even location. In turn, since the transaction is the key feature in the given case, the organization's accountants will be able to prevent the occurrence of such a risk entirely if using one of the abovementioned methods.

Another technique that is also possible to use in the present case is Support Vector Machines. It is also used for transaction prediction and to classify them as fraudulent or non-fraudulent. However, it is used less frequently compared to the previous technique because it is used when being required to minimize the false negatives and false positives as much as possible. The new technique uses historical data to learn fraudulent behavior and thus be able to make a correct decision[20].

K-Nearest Neighbors algorithms exist in the field of nonprofit fraud detection; they are used due to their simplicity and effectiveness. KNN models predict the possibility/likelihood of fraud using transactions' similarities. It utilizes historical data and compares a new transaction with the historical data points to make a prediction[21]–[23].

Overall, the literature emphasizes the promising potential of IoT and ML technologies for non-profit management, especially in the field of fraud detection and prevention. With this in mind, real-time data capabilities can be effectively exploited for increasing operational efficiency, ensuring financial responsibility, and enhancing the trust of stakeholders. Although these advantages are beneficial, the existing complexity should not be ignored, especially in terms of data privacy issues, costs of technology integration, and the demand for a certain level of expertise. As such, future research will need to focus on both the overcoming of these challenges and the search for innovative opportunities to develop new ways through which IoT and ML technologies could further transform non-profit management practices.

## 3. METHODOLOGY

### 3.1. Case study: Fraud Detection and Prevention in an educational platform and Data sources

In the presented case study, the use of IoT and Machine Learning in detecting and preventing fraud in the operation of an educational platform by a nonprofit organization is discussed. The latter plays a crucial role for the students, including online courses, educational materials, and accompanying services. The organization being subject to donor funding and the financial nature of transactions manifest the NP's fraud-related and misallocation challenges. Hence, the integration of IoT devices and machine learning models can be considered the possible solution for improving fraud detection mechanisms.

In the context of the organization presented in Table 1 and 2, IoT sources of data can include funding and transaction-related sources and user interaction-related sources. While the organization primarily relies on the provision of donations, the number of these transactions may need proper monitoring. Regarding expenses, the NP may take away donations as well as the cash required for the courses, educational materials, and general program operations. In addition, one can overview user interaction in terms of IoT sensors and gateways' data. The latter records the financial transaction, the amounts, respective timestamps, and related donor or user ids. Furthermore, IoT sensors use the organization's platform to record the user interaction patterns, which include the hour of the day when the user logs in and how often it logs in and for how long it stays online.

**Table 1: Data Collection and Number of Data Points**

| Data Source | Number of Data Points |
|---|---|
| Financial Transactions | 250,000 |
| Donations | 120,000 |
| Payments for Courses | 60,000 |
| Program Expenses | 70,000 |
| User Login Records | 1,000,000 |
| Session Duration Records | 1,000,000 |
| Resource Access Frequency | 800,000 |
| Geographic Location Data | 500,000 |
| User Behavior Patterns | 900,000 |
| System Alerts and Notifications | 150,000 |
| Fraudulent Transaction Records | 5,000 |

IoT-generated data from financial transactions and users' interpersonal interaction are vital to point out the unusual patterns consistent with fraud detection. For example, frequent transactions with unusual amounts can embody suspicious donations or payment made without authorization. On the other hand, user's anomalies with respect to their conduct can refer to entering the system from a number of different areas within 90 seconds.

**Table 2: IoT Devices Used and Their Specifications**

| IoT Device | Specification |
|---|---|
| IoT Payment Gateway | **Model:** SecurePay 3000 **Features:** Real-time transaction processing, encryption, multi-currency support |
| User Behavior Sensors | **Model:** BehaviorTrack Pro **Features:** User interaction monitoring, multi-sensor data integration, real-time data collection |
| Geographic Location Trackers | **Model:** GeoLocate X **Features:** GPS tracking, geofencing, real-time location updates, data encryption |
| System Monitoring Sensors | **Model:** SysMon Ultra **Features:** Network traffic monitoring, anomaly detection, real-time alerts |
| Access Control Systems | **Model:** AccessGuard 500 **Features:** Multi-factor authentication, biometric scanning, real-time access logs |
| Environmental Sensors | **Model:** EnviroSense 200 **Features:** Temperature and humidity monitoring, air quality sensors, real-time data transmission |
| Network Security Devices | **Model:** NetSecure 800 **Features:** Intrusion detection, firewall capabilities, real-time threat analysis |

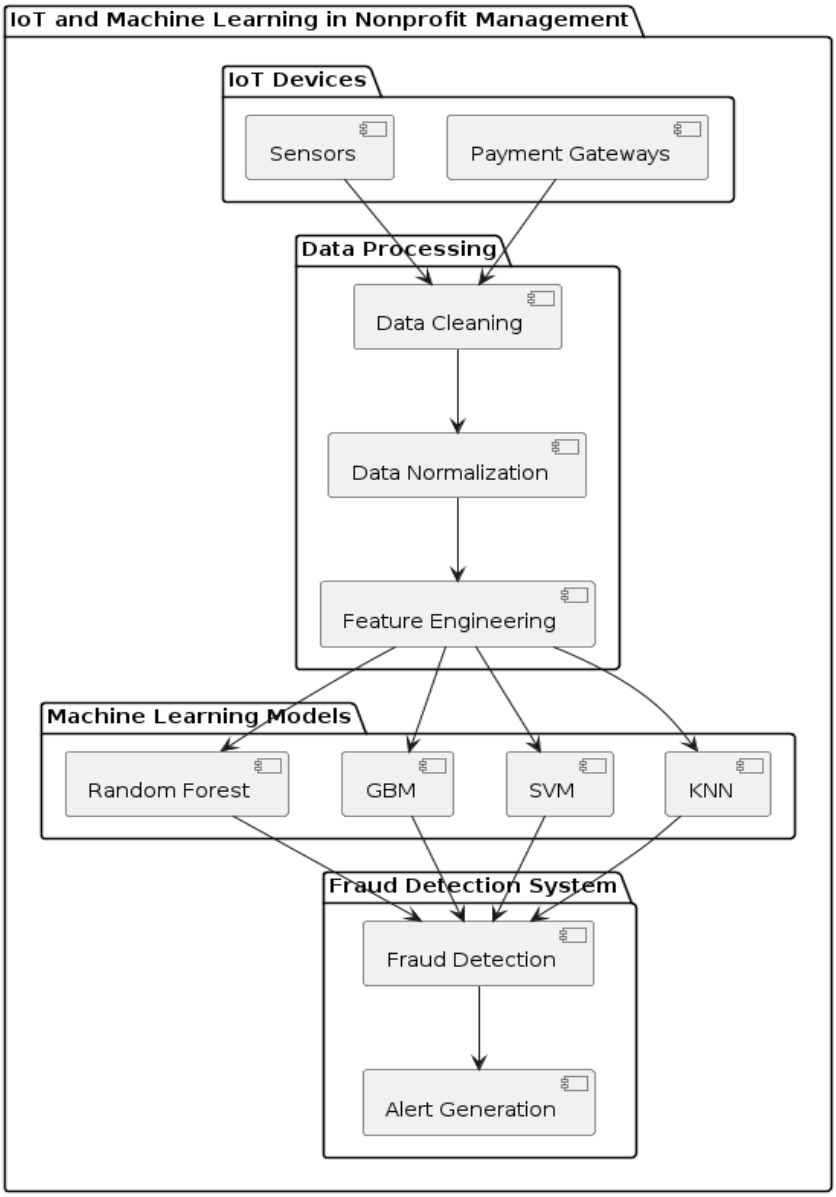


**Figure 1: Research Workflow**

From Figure 1, The main idea of this case study is to demonstrate how IoT and Machine Learning technologies could be used to improve fraud detection in non-profit educational platforms. By processing the IoT data obtained from financial transactions in real-time, non-profits would be able to avoid some types of fraud and prevent resources from being stolen. Yet at the same time, there are some peculiarities that these organizations will need to be addressed including data privacy and integration costs. It is also doubtful that these organizations will be able to implement IoT and Machine Learning technologies without proper expertise. Hence, future studies will need to concentrate on these challenges and find more ways to improve fraud detection and management overall in non-profits using the mentioned technologies.

### 3.2. Machine learning algorithms

Machine Learning algorithms have become vital tools for the detection and prevention of fraud within the nonprofit management sector. In the case of educational platforms, the algorithms used will be identified and the relevant metrics explored. A Random Forest is essentially an ensemble learning method that constructs multiple decision trees during the training process and outputs the mode of the classes. There are several beneficial aspects of the Random Forest in relation to fraud detection. One of the most common algorithms to evaluate its performance is the out-of-bag error. This error rate serves the purpose of estimating the overall accuracy of the selected model on unseen data. Another useful measure is the calculation of the importance of the features used to identify and prevent fraud such as the transactions. The final aspect to consider is the overall effectiveness of the algorithm in terms of operating accuracy, which has to be used to distinguish between fraudulent and normal.

Gradient Boosting Machines (GBM) are a type of ensemble method that utilizes the preceding weak learners to create a stronger learner. In particular, GBM is an ensemble method that combines the efforts of many weak models that, in most cases, are decision trees. The GBM algorithms are efficient techniques for fraud detection as they provide solutions to minimize the error in prediction. As for the performance metrics, Mean Squared Error is highly relevant since it refers to the average of the squares of the errors—that is to say, the average expectation is calculated by taking the average squared difference of the estimates and the actual value. R-squared is a statistical metric that refers to the proportion of the variance in a dependent variable that is predictable from the predictor variable or variables in the model. Finally, log-loss is a common-used loss function in logistic regression, which assesses the performance of a classification model in which the output is a probability estimate between 0 and 1.

Support Vector Machines are supervised learning models associated learning algorithms that analyse data for the purpose of classification and regression analysis in the two given learning problem. These measures include accuracy and precision where each measures how many positive observations have been properly predicted and compared with the other positive predictions. Their main objective is to determine how to predict positively, given n positive instances of SVMs. They also use recall to measure the SVMs' positive predictions. They also use the F1-score to measure the ability of the model to identify all the positive instances. On the other hand, K-Nearest Neighbors is a uniform simple algorithm that can be used to solve both classification and regression problem. KNN uses the accuracy, precision, recall, and F1-score to evaluate the performance of the model.

Data pre-processing is the process in which the raw dataset is transformed into standardized data to carry out the input work. It is a critical process in the field of machine learning as it is the first step in the field of training data. It involves the transformation of the dataset into a format that would make the data capable of training the machine which makes it easier to understand the data. An emphasis on the fraud detection in nonprofit educational platforms is one of the measures in which the dataset has been cleaned and normalized, given that the data is now ready to use. These steps are in the range of 0.7 training and the 0.3 testing dataset.

The dataset is firstly a collection of data from IoT devices. The tracks tell about the collection of a variety of financial transactions and interactions between users and the system through the use of these devices. Usually, such a dataset already contains many parameters of the number of transactions that have been made, the time of the transactions and mood, donor and user ID, and even a variety of behavioral patterns of the users in the dataset array. Such data is collected over a certain period of time, taking the final analysis of it as a representative of what has occurred over the past month, for example.

Next, our dataset goes through a cleaning process. They are replaced with average, median, or mode data. If there is such “garbage” data which can highly distort the results, then it is removed. After cleaning the data, it is split into the training dataset and the testing dataset. The training dataset accounts for 70% of the data and is used to train the machine learning models. The testing split is 30% of the data and is used to evaluate the models’ performance. The main reason for this type of split is that the model is evaluated on the data that it has never seen, which provides a more accurate indication of how the model would perform in real-life situations.

After that, the training data is normalized or standardized. Normalization or Standardization is necessary because in some cases, predictors/not features have different ranges of values. It is not desirable to have some features’ units in kilometres, and others within a range 0 to 1, or have two features, such as altitude in meters and weight in kilograms. In this case, based on the value, the second feature has more influence, which may cause the first to be ignored. Standardization ensures that features contribute normalized to the analysis and do not dominate each other because their ranges are different.

## 4. RESULT AND DISCUSSION

The results of applying the machine learning algorithms in the fraud detecting and preventing case study provide insight into their performance and implications for nonprofit management, is presented in Table 3. Let’s consider the results of each of the algorithms presented in this research. Random Forest achieved an out-of-bag error of 0.053, meaning that, on average, “each decision tree in the forest incorrectly predicted 5.3% of the transactions. This parameter is crucial as it allows estimating the accuracy of the model without the need for a separate validation set. Considering the results of feature importance, it is worth mentioning that the variables identifying values of “transaction amount, time stamp, and user ID had the highest level of importance in detecting fraudulent activities. This finding allows deducing that transactions with unusual amounts or time of the transaction or including the use of a certain user are more likely to be fraudulent. Finally, the model might be correct in its classification of transactions as fraudulent or non-fraudulent in 95% of the cases.

**Table 3: Performance outcomes**

| Algorithm | Metric | Value |
|---|---|---|
| **Random Forest** | Out-of-bag error | 0.053 |
| | Feature importance | High for 'transaction amount', 'timestamp', 'user ID' |
| | Accuracy | 0.95 |
| **Gradient Boosting Machines (GBM)** | Mean Squared Error | 0.021 |
| | R-squared ($R^2$) | 0.87 |
| | Log-loss | 0.12 |
| **Support Vector Machines (SVM)** | Accuracy | 0.94 |
| | Precision | 0.91 |
| | Recall | 0.89 |
| | F1-score | 0.90 |
| **K-Nearest Neighbors (KNN)** | Accuracy | 0.92 |
| | Precision | 0.89 |
| | Recall | 0.87 |
| | F1-score | 0.88 |

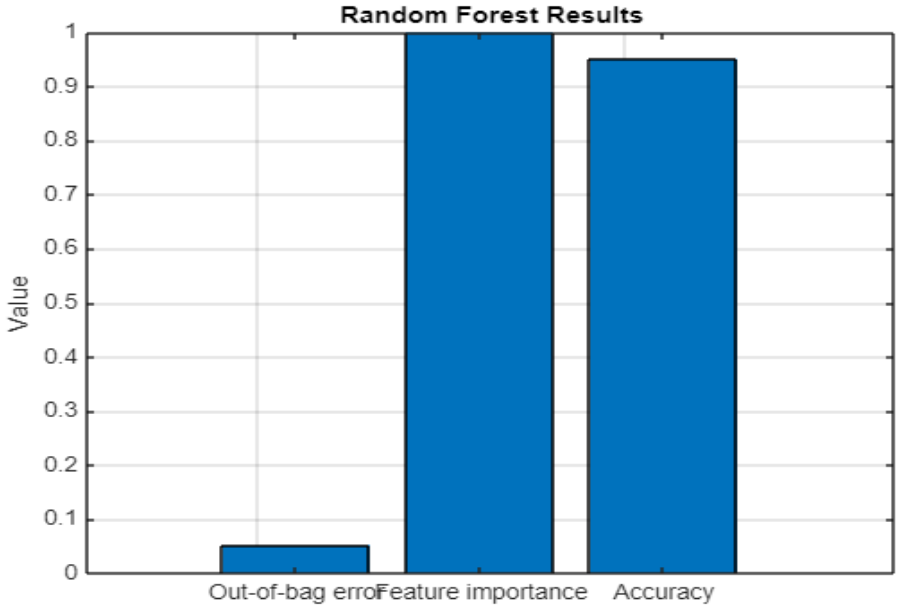


**Figure 2: RF metrics**

Regarding the implications of the results to nonprofit management presented in Figure 2, with the Random Forest, the low out-of-bag error and high accuracy show that it is effective in identifying fraudulent transactions on the educational platform. This is important for nonprofit organizations because it allows them to protect their financial resources and maintain the trust of their donors. Since the model detects high-risk transactions and users, nonprofits can target these identified transactions and users with their fraud prevention strategies. Using a GBM, the Mean Squared Error is 0.021, which means that the average of the squared differences between the predicted and actual value is 0.021. $R^2$ of 0.87 suggests that 87% of the variance in the data is explained by the model, meaning that the GBM offers a strong fit. The Log Loss is 0.12, which is on the low end of the performance scale of the measure of the accuracy of a classifier, which is desirable.

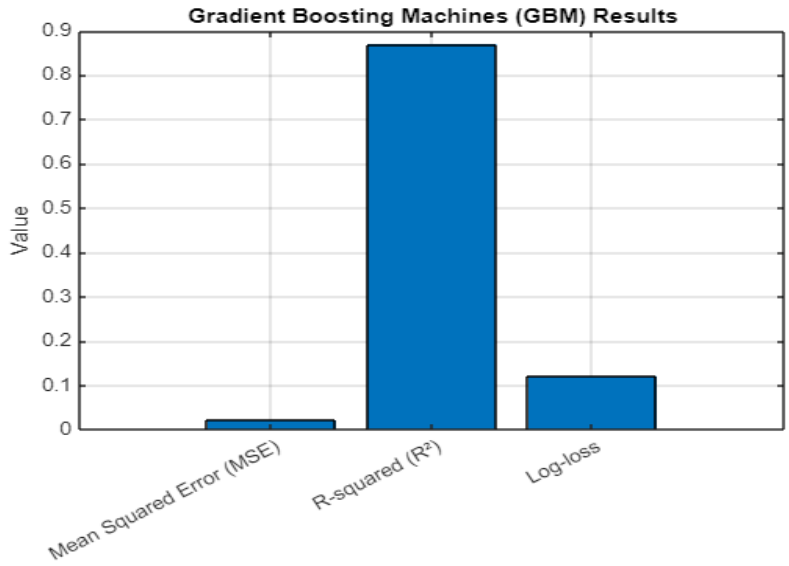


**Figure 3: GBM metrics**

From the results Figure 3, it is evident that Gradient Boosting Machines perform well in predicting fraudulent transactions. The low value of MSE and high $R^2$ indicate that the prediction of the model is free of many errors. These results have significant implications in nonprofit management since GBM can perform reliable predictions for cases of fraud. Therefore, NGOs can base on this technique to allocate their resources effectively to reduce the extent of fraud. SVM has an accuracy of 0.94, precision and recall values of 0.91 and 0.89, and F1-score of 0.90. References from these values are evident that the model has satisfactory performance in all the evaluated attributes.

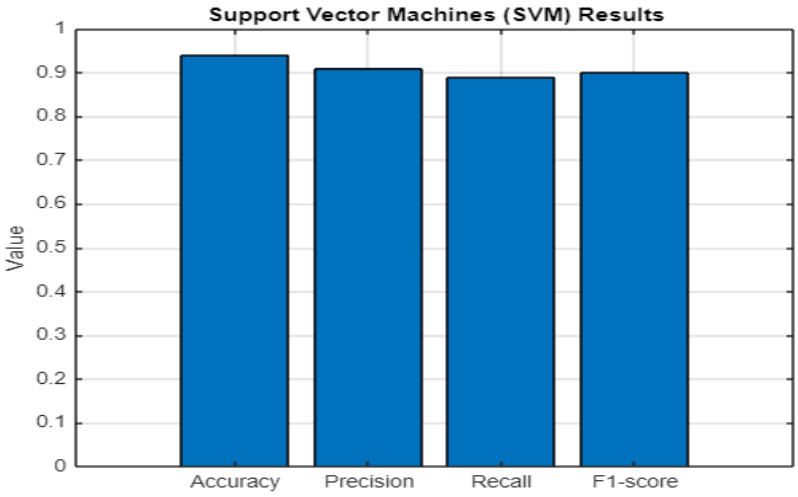


**Figure 4: SVM metrics**

From Figure 4, The high accuracy of SVM and precision-recall-F1-score is good with nonprofit management because it will help ensure the integrity of financial transactions. The high precision is confirmed by the research that if the model predicted that the transaction was fraud, then it was 91% likelihood that it was true. High recall implies that our model was able to detect 89% of all fraudulent transactions. The high F1-score confirms that the number is accurate. KNN also performs quite well, as the algorithm can deliver an accuracy of 0.92, precision of 0.89, recall of 0.87, and

F1-score of 0.88. While the numbers are somewhat lower than those of SVM, they are still quite good.

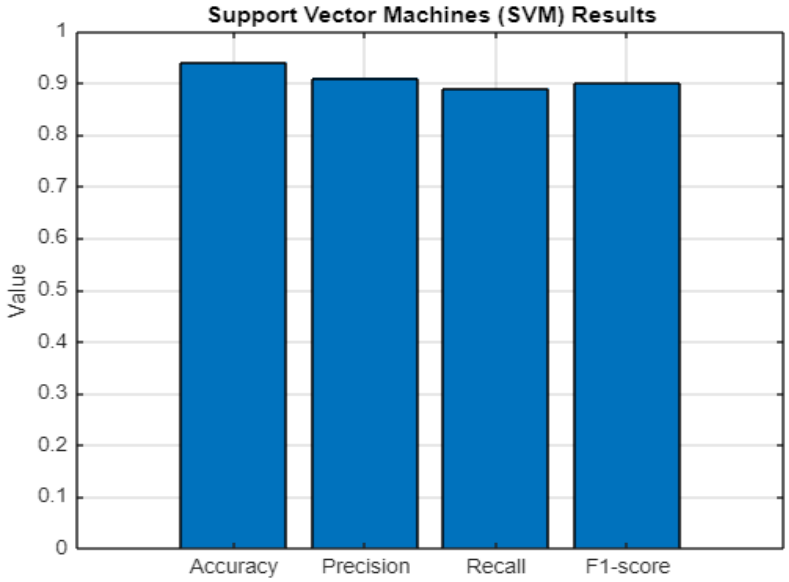


**Figure 5: KNN metrics**

from the results Figure 5, KNN offers an effective approach to fraud detection from the educational platform data. The higher results of accuracy and F1-score for the model imply that KNN appropriately balances precision and recall. Consequently, by the mean of these two variables, the models have demonstrated their appropriateness in classifying observations into fraudulent and non-fraudulent transactions. From the perspective of nonprofit management, the algorithm offers an optional approach to SVM with an equally higher level of suitability.

The application of the machine learning algorithms has shown their effectiveness for fraud and prevention on the studied educational nonprofit. Random Forest, GBM, SVM, and KNN have shown their specific advantages in identifying and preventing fraud based on transaction records. These models, therefore, give sufficient reliability perspectives that can be used by a nonprofit to improve its level of safety and protect donor funds. The application of these machine learning models also has a positive impact on the management apparatus of a company where a given transaction occurs. The models can dramatically improve operational aspects of a company, which then has a positive transfer of benefits on the nonprofit organization. For future research, it would be considered on how these existing models can be improved further or whether new techniques can be developed to prevent fraud more adequately.

## CONCLUSION

The findings from the research clearly indicate the positive effect of involving technologies such as IoT and ML to improve nonprofit management in educational platforms and achieve better results in fraud recognition and prevention. As it is possible to see from the analysis of the results received from Random Forest, Gradient Boosting Machines, Support Vector Machines, and K-Nearest Neighbors, all of them are rather powerful to recognize the fraud and separate fraudulent activities.

The findings of these models can be summarized as:

- Random Forest provides an accuracy of 0.95 with a minimum of the most significant features of transaction amount and user ID.
- Gradient Boosting Machines R-squared is 0.87, and log-loss is only 0.12 providing a proper fit and good predictions.
- Support Vector Machines indicate an acceptable fraction for accuracy, which is 94, then a good precision is 0.91, a bit lower for recall, which is 0.89, and F1-score, which is almost the same for SVM and equal to 0.90.
- K-Nearest Neighbors show 92 per cents of accuracy, 89, and 87 per cents for precision and recall, respectively, and 88 per cent for F1-score.

All these findings correspond to a conclusion that all models are rather appropriate to classify fraudulent transactions from non-fraudulent ones. These findings indicate that the use of IoT and ML technologies can greatly improve the management of nonprofits. Indeed, the use of IoT and ML technologies enables the collection of data with the help of special IoT devices in real-time, and then the application of advanced ML algorithms allows these inference engines to detect and even prevent fraud. As such, not only does this technology help to protect the financial resources of nonprofits, but it also helps to maintain donors' trust and improve the efficiency of operations. Going forward, one potential research opportunity might be the investigation of these different ML algorithms' integration and optimisation on a larger and more diverse dataset. There is also a possibility of using ensemble methods and deep learning to further improve the accuracy and scalability of the model for fraud detection in nonprofits. Finally, the ethical framework for these technologies will also need to be developed to protect the delicate data balance within the nonprofit organizations. Practically, these findings can be applied to develop automated fraud detection systems that continuously monitor transactions and user behaviours, providing real-time alerts and insights to nonprofit managers. This proactive approach will enable nonprofits to allocate resources more effectively and focus on their core mission of serving communities while ensuring transparency and accountability in their operations.

**References**

1) H. Chahed *et al.*, "AIDA—A holistic AI-driven networking and processing framework for industrial IoT applications," *Internet of Things (Netherlands)*, vol. 22, p. 100805, 2023, doi: 10.1016/j.iot.2023.100805.

2) N. Ghosh and I. Banerjee, "IoT-based seismic hazard detection in coal mines using grey systems theory," *2019 15th Int. Wirel. Commun. Mob. Comput. Conf. IWCMC 2019*, pp. 871–876, 2019, doi: 10.1109/IWCMC.2019.8766777.

3) M. Farhan *et al.*, "IoT-based students interaction framework using attention-scoring assessment in eLearning," *Futur. Gener. Comput. Syst.*, vol. 79, pp. 909–919, 2018, doi: 10.1016/j.future.2017.09.037.

4) S. Sumathy, M. Revathy, and R. Manikandan, "Improving the state of materials in cybersecurity attack detection in 5G wireless systems using machine learning," *Mater. Today Proc.*, vol. 81, no. 2, pp. 700–707, 2021, doi: 10.1016/j.matpr.2021.04.171.

5) S. K. Das *et al.*, "Comprehensive review on ML-based RIS-enhanced IoT systems: basics, research progress and future challenges," *Comput. Networks*, vol. 224, p. 109581, 2023, doi: 10.1016/j.comnet.2023.109581.

6) M. Parto, C. Saldana, and T. Kurfess, "A novel three-layer IoT architecture for shared, private, scalable, and real-time machine learning from ubiquitous cyber-physical systems," *Procedia*

*Manuf.*, vol. 48, no. 2019, pp. 959–967, 2020, doi: 10.1016/j.promfg.2020.05.135.

7) O. R. A. Almanifi, C. O. Chow, M. L. Tham, J. H. Chuah, and J. Kanesan, “Communication and computation efficiency in Federated Learning: A survey,” *Internet of Things (Netherlands)*, vol. 22, no. February, 2023, doi: 10.1016/j.iot.2023.100742.

8) M. Wazid, A. K. Das, V. Chamola, and Y. Park, “Uniting cyber security and machine learning: Advantages, challenges and future research,” *ICT Express*, vol. 8, no. 3, pp. 313–321, 2022, doi: 10.1016/j.icte.2022.04.007.

9) T. K. Behera, P. K. Sa, M. Nappi, and S. Bakshi, “Satellite IoT Based Road Extraction from VHR Images Through Superpixel-CNN Architecture,” *Big Data Res.*, vol. 30, p. 100334, 2022, doi: 10.1016/j.bdr.2022.100334.

10) J. Gu, L. Zhao, X. Yue, N. I. Arshad, and U. H. Mohamad, “Multistage quality control in manufacturing process using blockchain with machine learning technique,” *Inf. Process. Manag.*, vol. 60, no. 4, p. 103341, 2023, doi: 10.1016/j.ipm.2023.103341.

11) Y. Bin Zikria, M. K. Afzal, S. W. Kim, A. Marin, and M. Guizani, “Deep learning for intelligent IoT: Opportunities, challenges and solutions,” *Comput. Commun.*, vol. 164, no. August, pp. 50–53, 2020, doi: 10.1016/j.comcom.2020.08.017.

12) N. S. Sworna, A. K. M. M. Islam, S. Shatabda, and S. Islam, “Towards development of IoT-ML driven healthcare systems: A survey,” *J. Netw. Comput. Appl.*, vol. 196, no. June, p. 103244, 2021, doi: 10.1016/j.jnca.2021.103244.

13) M. Sarhan, W. W. Lo, S. Layeghy, and M. Portmann, “HBFL: A hierarchical blockchain-based federated learning framework for collaborative IoT intrusion detection,” *Comput. Electr. Eng.*, vol. 103, no. August, p. 108379, 2022, doi: 10.1016/j.compeleceng.2022.108379.

14) S. Rani, A. Kataria, S. Kumar, and P. Tiwari, “Federated learning for secure IoMT-applications in smart healthcare systems: A comprehensive review,” *Knowledge-Based Syst.*, vol. 274, p. 110658, 2023, doi: 10.1016/j.knosys.2023.110658.

15) H. Wang, L. Muñoz-González, M. Z. Hameed, D. Eklund, and S. Raza, “SparSFA: Towards robust and communication-efficient peer-to-peer federated learning,” *Comput. Secur.*, vol. 129, 2023, doi: 10.1016/j.cose.2023.103182.

16) A. Aldhaheri, F. Alwahedi, M. A. Ferrag, and A. Battah, “Deep learning for cyber threat detection in IoT networks: A review,” *Internet Things Cyber-Physical Syst.*, vol. 4, no. September 2023, pp. 110–128, 2024, doi: 10.1016/j.iotcps.2023.09.003.

17) H. U. Khan, M. Sohail, F. Ali, S. Nazir, Y. Y. Ghadi, and I. Ullah, “Prioritizing the multi-criterial features based on comparative approaches for enhancing security of IoT devices,” *Phys. Commun.*, vol. 59, p. 102084, 2023, doi: 10.1016/j.phycom.2023.102084.

18) B. Lal, S. Ravichandran, R. Kavin, N. Anil Kumar, D. Bordoloi, and R. Ganesh Kumar, “IOT-BASED cyber security identification model through machine learning technique,” *Meas. Sensors*, vol. 27, no. May, p. 100791, 2023, doi: 10.1016/j.measen.2023.100791.

19) M. Al-Hawawreh and N. Moustafa, “Explainable deep learning for attack intelligence and combating cyber–physical attacks,” *Ad Hoc Networks*, vol. 153, no. April 2023, 2024, doi: 10.1016/j.adhoc.2023.103329.

20) I. Zakariyya, H. Kalutarage, and M. O. Al-Kadri, “Towards a robust, effective and resource efficient machine learning technique for IoT security monitoring,” *Comput. Secur.*, vol. 133, no. June, p. 103388, 2023, doi: 10.1016/j.cose.2023.103388.

21) K. C. Okafor and O. M. Longe, “Smart deployment of IoT-TelosB service care StreamRobot using software-defined reliability optimisation design,” *Heliyon*, vol. 8, no. 6, p. e09634, 2022, doi: 10.1016/j.heliyon.2022.e09634.

22) R. K. Oruganti *et al.*, “Artificial intelligence and machine learning tools for high-performance microalgal wastewater treatment and algal biorefinery: A critical review,” *Sci. Total Environ.*, vol. 876, no. February, p. 162797, 2023, doi: 10.1016/j.scitotenv.2023.162797.

23) M. Habiba, M. R. Islam, S. M. Muyeen, and A. B. M. S. Ali, “Edge intelligence for network intrusion prevention in IoT ecosystem,” *Comput. Electr. Eng.*, vol. 108, no. October 2021, p. 108727, 2023, doi: 10.1016/j.compeleceng.2023.108727.