Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

A Smart IoT-Based Fire Detection and Machine Learning Based Control System for Advancing Fire Safety

Balaji Singaram[1], Lakshmi. B[2], Dr.M.Preetha[3], V.K. RamyaBharathi[4], Dr.S.Muthumarilakshmi[5], Rakesh Kumar Giri[6]

[1]Software Developer, Compunnel Inc., Plainsboro, New Jersey, USA, 08536, balaji.singaramus@gmail.com
[2]Assistant Professor, Department of Computer Science and Technology, Madanapalle Institute of Technology and Science, Madanapalle, Andhra Pradesh, India, lakshmibreddy93@gmail.com
[3]Professor & Head, Department of Computer Science and Engineering,Prince Shri VenkateshwaraPadmavathy Engineering College, Chennai, India,smpreetha14@gmail.com
[4]Assistant Professor, Department of AI&DS, Panimalar Engineering College, Chennai, India, ramyabharathi96623@gmail.com
[5]Associate Professor,Department of CSE,Chennai Institute of Technology,Kundrathur, Chennai-69, India, muthu3041974@gmail.com
[6]Assistant Professor, Department of Computer Science & Engineering, Sunrise University, Rajasthan, rakesh274@gmail.com

In this study, detailed research has been introduced to enhance the fire safety and security of the chemical laboratories by using the integration of IoT and machine learning. The purpose of the research is to develop a strong framework to identify and take a quick response of any potential fire incidents or safety hazard properly in real time. Using different kinds of sensors, including temperature, smoke, and gas sensors in different locations of the laboratory area, this framework has collected real-time data and identifies the anomalies, which may cause fire or any safety issue. At last, the use of machine learning technologies, including SVM, ANN, DT, and RF helps to understand and analyze the nature of sensor data and help to make a suitable decision for the response. According to the experimental results, the performance of the SVM is excellent in this context, where a precision of 0.987, recall of 0.989, F1 score of 0.988, and AUC-ROC curve of 0.985 has been identified. In addition, the effectiveness of the ANN, DT, and RF is also satisfactory, which can be considered as an effective technology in the context of the fire safety application. By using SVM in the IoT fire detection system, the added advantage has been found in terms of the robustness, interpretability, and computational feasibility, which increases its success ratio. Results of the present study show a significant potential of the IoT and ML, which can be used to redesign the fire safety and emergency response mechanism of the chemical laboratories. Using advanced optimization techniques and sensors, the scalability, efficiency, and reliability of the present framework can be increased.

Keywords: IoT, Fire Detection, Machine Learning, Chemical Laboratories, Safety.

1. Introduction

Fire safety and security of chemical laboratories draw particular concerns since the substances being evaluated and integrated into various mixtures are extremely volatile as a rule and may be considered potentially flammable. Though fire may be of relatively low probability, especially since prompt water-based extinguishing is not very common concerning such volatile substances, and the main threat of tangible damage to personnel is the chemical spill. However, accidents do occur, such as spills or overheating of mitric acid, resulting in a lab explosion. With valuable equipment and materials found in a chemical lab setting, the consequences may be dire for both personnel safety and the equipment itself, and even environmental area[1]–[3].

Regarding safety, the traditional fire detection systems, while generally useful, possess precise, relevant, and timely reacting, integral to the intricate and complex networks of a chemical laboratory. Either relying on manual detection or utilizing sensors, fire detection is often inadequate, imprecise, and too slow. The incapability of traditional fire detection systems to provide relevant and useful safety support, IoT and machine learning technologies may be optimally used for fire safety and security. With chemical labs considered some of the main beneficiaries of IoT algorithms, proper protection of equipment and personnel in the labs without any mistakes in emergency calling and procedures are almost assured. For example, the IoT employs various sensors to register, for example, temperature or gas concentration, and transmits this information over the internal network, which is then analyzed and acted upon with machine learning algorithms, such as Support Vector Machines, Artificial Neural Network, DT and Random Forests[4]–[6].

Detection of fire relies on the method use of technologies. The existing fire detection systems deployed in the chemical laboratories rely on conventional approaches such as smoke detectors and heat sensors. As the best safety system for the protection of laboratories, these methods apart from being the best approach towards safety they include manual monitoring. The uses of heat, smoke, or sensors are exposed to challenges that are highly related to the use of manual observation. Although the manual system of monitoring the fire is considered, the best method of fighting the source. However, it take much of the lab assistant time to observing the possible sources. In this reference, since human-observed patterns are not uniform as expected, they detect the fire with exaggerated zeal which results in overreactions leading to unnecessary alarm_settings in the disposal [7]–[9]. Therefore, manual observation is time-consuming and demands more in terms of human observation that cannot be maintained highly effectively on normal and healthy work. Manual observation is a risk that delays the response to initiate fire fighting to reduce the causes for possible fire alarms. Traditional sensor-based-lab monitoring devices might fail to detect the slight, subtle, and small changes in the environment leading to inefficiencies of the fire detection systems-initiation. In response to the natural manual fire detection system, the analysts and machine development experts and App developments that can interconnect systems for effective laboratory safety[10], [11]. In my opinion, they include the introduction of the IoT sensors for effective appraisal of environmental conditions.

The emergence of machine learning algorithms in IoT-based fire detection systems introduces a novel framework in the field of fire safety and security. Machine learning models such as SVM or support vector machines, ANN or artificial neural networks, DTs or decision trees, and RF or random forests facilitate the ability to analyze immense datasets of intricate measurements and provide reliable insights and predictions. For instance, SVM has demonstrated excellent performance in binary classification tasks assessing which hyperplanes optimally separate data points[12]–[14]. Thus, these algorithms can be utilized to distinguish between class 1, lab normal, and class 2, causality unusual, operations. Moreover, ANN can provide reliable predictions due to their capacity to detect nonlinear patterns [15]–[17]. In comparison with other models, DT and RF outperform in terms of simplicity, interpretability, and ability to conduct ensemble learning, whereas the latter is crucial when conducting robust classification tasks. Numerous research endeavors have examined the framework of IoT and machine learning for fire safety and security in different industries such as manufacturing, healthcare, and transportation. It has been established that IoT-based fire detection systems facilitate response time improvement, false alarms minimization, and overall safety outcome advancement. For instance, researchers have successfully designed IoT-smoke detection systems that adopt machine learning algorithms to predict fire. These installations differentiate among different types of smoke particles and then proceed to provide predictions of fire. Similarly, IoT-precursors-based gas sensing networks have been previously deployed at industry locations to detect hazardous gas leaks. Machine learning would then be employed to provide real-time monitoring and prediction of the occurrence of gas leakages[18]–[20].

While IoT and machine learning technologies provide many opportunities for enhancing fire safety and security solutions, numerous challenges should be considered. One of the major challenges relevant to IoT is the heterogeneous nature of sensors and communication technologies used as part of these systems. In other words, the IoT devices utilized as part of the network can use different communication protocols for interacting with the internet or other devices. This being the case, the system design process should take account of the issues related to scalability, interoperability, and management of data. When it comes to machine learning, the algorithms used for this purpose should address multiple concerns related to the safety and privacy of data, the interpretability of such models, and their potential biases[21], [22].

Another important consideration is that the efficiency of IoT-based solutions for fire detection is influenced by the sensor type, location, and time, as well as the certain features of the network and system used in this case. Therefore, the advantages and limitations of the existing solutions should be carefully evaluated as part of a testing and validation procedure to identify the focus on the improvement. In general, the future work and efforts should be focused on the development of the most advanced sensor technologies, the creation of the most sophisticated machine learning technologies, and the improvement to any other related solutions. Furthermore, IoT solutions can be integrated with other promising technologies, like edge computing or blockchain, to enhance the scalability, efficiency, reliability, etc., of the existing and novel fire detection and response mechanisms.

2. Problem Statement and Objectives

Chemistry laboratories require specifically-oriented security systems that would prevent the immense risks and hazards of handling hazardous materials and various chemical processes. Though traditional ways of conducting security work in laboratories have proven to be somewhat effective, they are still not able to offer real-time monitoring and detect the anomalies, such as fire breakout or unauthorized access. Moreover, modern laboratories have increasingly more entry points with numerous environmentally-sensitive pieces of equipment and, therefore, follow more complex patterns and multilayer structures that are difficult to monitor and control manually. The proposed research would help to eliminate these limitations by developing a Smart IoT-Based Fire Detection and Machine Learning-Based Control System for Chemical Laboratories.

The security system, in this case, must be based on the Internet of Things technology and, more specifically, on the instant monitoring of the environmental factors in the laboratory where temperature, humidity or gas content might signal the fire hazard or another kind of safety-related anomaly. At the same time, the use of machine learning algorithms would also allow this system to learn the patterns of the monitored data and react independently to no less potential threat-related anomaly, such as an unscheduled visit or otherwise unusual behavior. Its proactive component ensures quick and timely response to any security threats and eliminates the hazards not only for the laboratory personnel but also the equipment and resources that might be otherwise lost due to the accident or inappropriate actions of untrained personnel. Additionally, such a security system is also more effective for large-scale deployment in the sense of providing an average centralized system for the control and monitoring.

3. Methodology

The central concept of IoT-based security and safety is the deployment of multiple sensors in the chemical laboratory. They can be of several types: temperature sensors, fire and smoke sensors, and gas sensors. The working of the system are shown in figure 1. They should be dispersed throughout the laboratory in different locations to ensure that the coverage is as comprehensive and all-inclusive as possible. The temperature sensors are likely the most important, as they should always be on. If these sensors collectively indicate that the temperature has risen in the location to a degree that is far above the safe level established by normal operation, it means that the laboratory is either on fire or that some piece of equipment is overheating. Fire and smoke sensors are vital because they pick up the cause of a fire or smoke, which usually gives them a few seconds or minutes to send the signal of danger and action to the security system. Finally, gas sensors can detect some of the more dangerous gases that can be formed during chemical reactions or leaks: their concentration can be too high, and the laboratory staff or the facility’s building can be endangered.

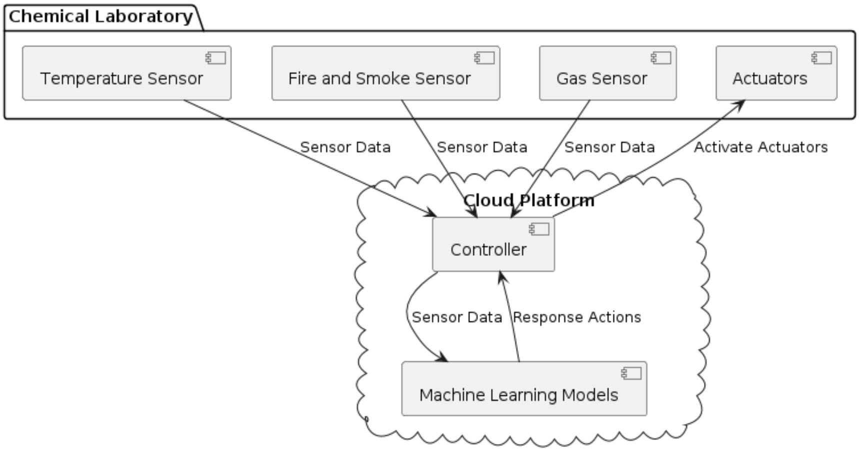

Fig. 1. Working of the Proposed Model

All information is then used in the IoT security system. The information from all sensors is sent to a central controller. The central controller is physically present in the laboratory and collects all the data while also analyzing and sending it further along to the cloud system. It is the most critical part of the IoT security system. The cloud system is used for data storage and analysis and for the remote monitoring of the sensor's system. The analysis at the cloud side can also be more complex. It is the last central idea of the IoT security system. One of the central ideas of the already-built IoT Security system is the inclusion of machine learning models in risk detection. How complex machine learning will be depends on the complexity of the task. For instance, they analyze the information being sent from all sensors in the lab right now. They then decide if the current situation shows any dangers to the security and safety of the laboratory. If the sensors ever show danger of the area going over the safe limit, the machine learning will send a signal to the fire system. The sprinklers will activate everywhere or evacuation settings will be enabled to remove the personnel from the safest place.

4. Dataset and Machine Learning Models

The present study utilizes a variety of machine learning models, such as Artificial Neural Networks, Support Vector Machines, Decision Trees, and Random Forests, with the aim of improving the efficiency of the security system developed for the chemical laboratory. The models are trained using the three types of sensor readings collected by diverse sensors placed in different locations of the laboratory. Online and real-time environmental sensor readings have been taken to register a proper distribution and representation of the environment and security threats. These readings are the input data, and the response of the sensors, such as the activation of water sprinklers or sounding an alarm and evacuating the laboratory has been recorded in the training dataset, serving as the output or target variable.

The dataset includes a total of 1400 readings and is separated into two sets for training the models and their later evaluation: 70 percent of the dataset have been used for training, and 30 percent to test the trained models. Such a proportion allows the machine learning models to understand the data and the patterns and relationships in the data and make the corresponding target response. The 30 percent of the data have not been used for training the model and therefore an unbiased evaluation of the performance and generalization of the models have been made.

5. Preprocessing of Dataset

Preprocessing of the dataset is crucial for making the machine learning models that have to be applied in the created security system for the given chemical laboratory reliable and efficient. The processing procedure done in this research are shown in figure 2. It is understood that the dataset has to experience a wide array of preprocessing, as its particular steps are intended to clean, change, and otherwise prepare the data for analysis during the training of testing phases. Different problems are addressed, including missing values of any feature, outliers that range the data significantly, the presence of noise in the data and other concerns. One of the initial steps towards the corresponding preprocessing is the missing value imputation with the mean, median or mode.

In the real world, it often happens that the system is not able to get the necessary reading from the given sensor due to malfunctioning of the device or errors in communication between the sensor and the system or any other reasons related to their work. The analogous values have to be identified and replaced with the estimate. Some sophisticated methods like interpolation and modeling can be applied to be followed, yet the most reliable way to impute the missing data is the imputation in mean, median, or mode. In any particular case, the approach makes the real dataset as full as it is rather than the model which stops once it detects that some values are not provided in the dataset.

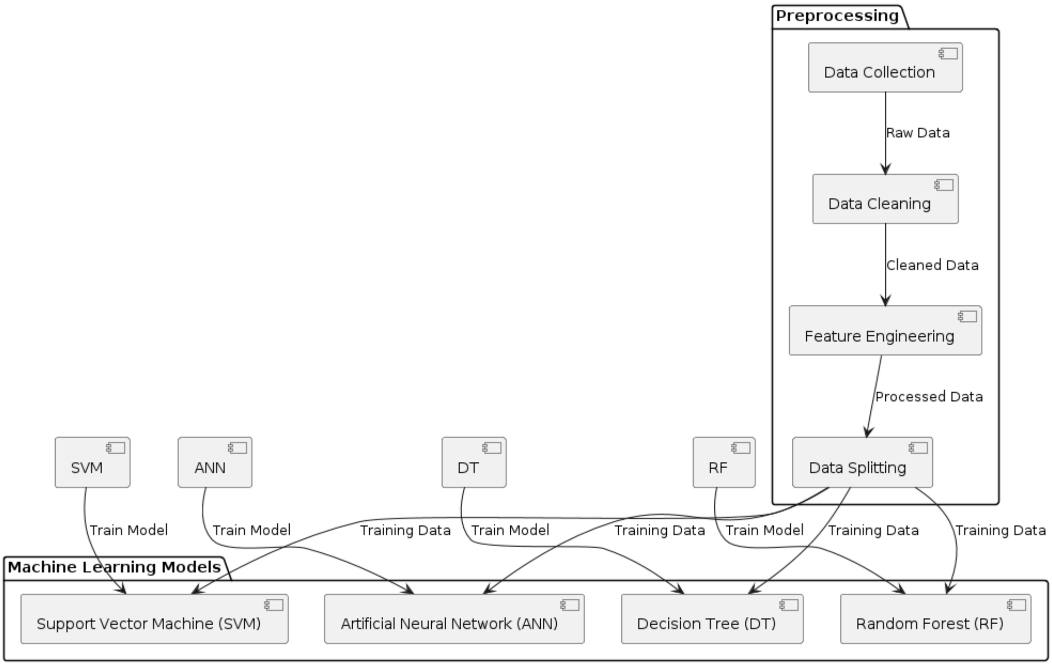

Fig. 2. Processing of Dataset

The corresponding problem has to be resolved, as the corresponding missing values can contain the target perception of the feature in question. Another problem that has to be addressed during dataset preprocessing is dealing with outliers. They have a significant impact on the mean value of the given feature and hence should be removed from the dataset. The simplest approaches towards the corresponding problem can be the usage of z-score or IQR analysis. In addition, the given feature has to be scaled or normalized. It means that all features have to share the same value and magnitude. It is particularly vital for such ML models that are highly dependent on the size of the input features, like support vector machines, for instance. In addition, normalization approaches such as L1 or L2 are equally implemented to normalize feature vectors, thus ensuring that they have unit scales and similar directions. Along with handling missing values, treating outliers, and reducing dimensionality, the dataset is modified into a format that is more appropriate for model training and prediction and better compatible with the theoretical concepts of the algorithms. More specifically, PCA, or feature selection, among other dimensionality reduction approaches, could be used to determine the most significant features and exclude irrelevant ones. In such a way, dimensionality reduction reduces computational complexity and planners phenomenon of the curse of dimensionality, which negatively impacts computational efficiency.

Additionally, categorical information in the dataset is transformed into numerical formatting, using tools such as one-hot encoding or label encoding. Such approaches help ML programs to analyze and predict results more efficiently and make categorical information more compatible with the model training process. Lastly, the dataset is divided into training, validation, and testing datasets to increase the opportunities of evaluating a model and optimize its performance during the training process. In addition, cross-validation methods, such as k-fold cross-validation or stratified sampling, are used to evaluate the generalization performance of the ML models and reveal preliminary symptoms of underfitting and overfitting.

6. Machine Learning Models

Artificial Neural Network is one of the machine learning algorithms used in this research to analyze sensor data and predict safety or security risks in the chemical lab. ANNs are types of computational models created to replicate the structure and function of biological neural networks in the human brain. ANNs are built by connecting nodes or neurons at several layers consisting of an input layer, an output layer, and one or more hidden layers. Weights of the links between nodes take place in the training stage where the model learns from the input data to prevent predictive error. ANNs play an important role in predicting potential safety or security risk by delineating the nonlinear and sophisticated causes and effects contained in the data. The use of the ANNs enables the lab workers to take proactive response while security risks are minimized.

Support Vector Machines, also known as SVMs, are a type of supervised learning models. They are particularly effective in classification and regression tasks. SVMs find optimal hyperplanes to separate data points into different classes. The data points, also referred to as vectors, are multi-dimensional and the classes can be defined as different categories. In this research project, the SVM model is employed to classify sensor data into categories that represent normal, safe operation and different types of anomalous events, which are usually indicative of security breaches and safety hazards. Therefore, the sensors act as vectors in multi-dimensional space and the SVM model structures the decision boundary, also known as the hyperplane, in effective ways in the high-dimensional feature space.

One frequent example of a machine learning algorithm is Decision Trees or DTs. This algorithm is highly interpretable and easy for use since it asks about the value of input features and can distinguish class labels that should be assigned to them loosely speaking. The appeal to DT predominantly relies on its ability to outline a decision boundary between all classes that should be considered in the laboratory and depict features that may contribute to security threats or safety hazards. Overall, DTs split a feature space into decision nodes depending on whether this split is initialized on the basis of feature entropy or Gini impurity, which is aimed at successfully classifying sensor data into all relevant classes by constructing sequences of simple decision rules.

Random Forests are ensemble learning methods that rely on a collection of decision trees for better and more accurate predictions of outcomes. Therefore, the current study utilizes the ability of RFs to rely on the combined predictive capabilities of decision trees for improving the performance of the security system that the chemical laboratory uses. Specifically, the set of decision trees created by the given methodology is based on taking random samples of the dataset and, subsequently, aggregating the prediction outcomes that the series of decision trees provides by voting or averaging. As a result, the current approach relies on the deployment of a model that does not run the risk of overfitting because of the fact that the decision trees are both different and completely independent of each other. Furthermore, the use of RFs offers valuable insights concerning the significance level of each variable that informs the model, thus helping interpret the nature of security threats or safety hazards present in the laboratory. As a result, leveraging the possibility to predict risks in advance and avert any accidents or threats to the security of the facility and the personnel inside represent a set of benefits that the use of RFs promotes in the chemical laboratory.

7. Result and Discussion

The table 1 provides the sample of sensor readings that were obtained as part of the conducted research. The real-time data was received from the installed IoT system in the laboratory environment. It represents the sensors data deployed at a various location from the morning to the evening. According to that, the overall condition of the environment is presented by a variation of the monitored parameters, including temperature, humidity, gas levels, and fire/smoke detection. This information demonstrates the dynamic environment state in the laboratory. Overall, this data will be used for our analysis, model training and decision-making inside of our security system.

Table 1. Sensor Readings

Time	Temperature (°C)	Humidity (%)	Gas Level (PPM)	Fire/Smoke Detection
08:00 AM	22.5	55	250	No
09:00 AM	23.0	56	260	No

10:00 AM	23.5	57	255	No
11:00 AM	24.0	58	270	No
12:00 PM	24.5	59	275	No
01:00 PM	25.0	60	280	No
02:00 PM	25.5	61	290	No
03:00 PM	26.0	62	295	No
04:00 PM	26.5	63	300	No
05:00 PM	27.0	64	305	No
06:00 PM	27.5	65	310	No
07:00 PM	28.0	66	315	No

After developing, training, and validating the machine learning models under discussion, rigorous testing is conducted to ascertain their predictive performance. In identifying responses to security threats or safety hazards in a chemical laboratory, the model testing process revealed that SVM is the one that has the highest accuracy. Its ability to predict responses accurately is about 98.98%, which is crucial in realizing the model's full potential. For an SVM, two parallel hyperplanes are developed in a dataset so that the maximum margin is generated, leading to the separation of one class of data points from others. In the current application, the model can accurately predict different events and separate them, meaning that the classifiers separate the normal operating conditions from all other cases.

The ANN model emerged second, with an accuracy of 95.23%. From these results, it appears that this model can accurately predict events because it can use a nonlinear activation function in the dataset to separate the normal and the worst-case operating conditions. ANNs can recognize complex patterns in datasets and predict without any significant problem. The last model is DT that registers an accuracy level of 91.5%, which is slightly lower than the performance of RF because of their reduced ability to predict accurately. Nevertheless, for minimizing decision-making problems, it should be noted that the DT's simplicity and the basic rules of decision-making in security-whole system synthesized them automatically but accurately. Therefore, to some extent, the lower RF performance level is expected because DT is one of the learners within it. From these results, the modeling technique seems to be in the order of their relevance such that SVM is the most important in its contribution, followed by others. The roles of the four models were justified, and they meet the basic requirements of optimizing security and safety in a chemical laboratory and the result are shown in figure 3.

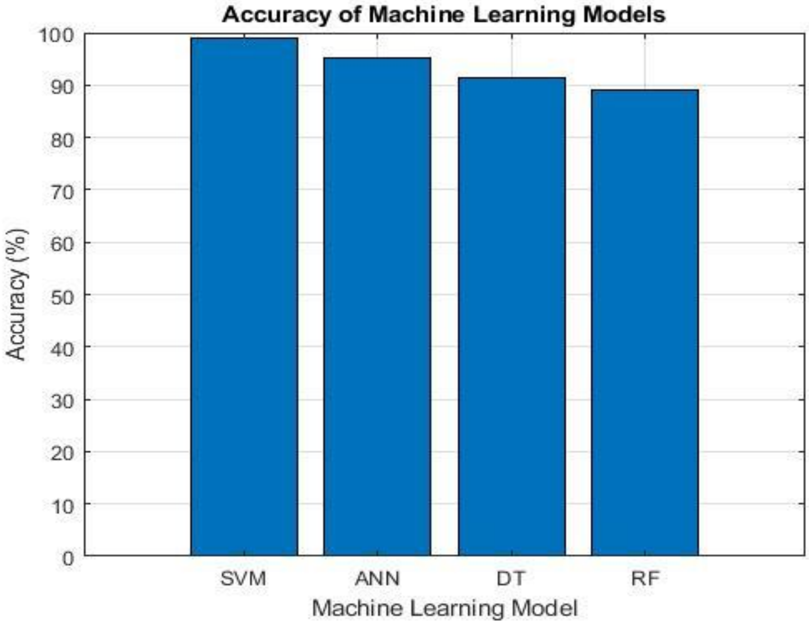

Fig. 3. Accuracy of Each Model

The performance score of each model are shown in figure 4. The precision score of 0.987 for SVM indicates the percent of all instances that were classified as positive and that actually are members of the positive category such that 98.7% of instances classified as positive by the SVM model are true positives. Evidently, the precision asses the model's proficiency in making positive predictions, and accordingly minimising false positives. A recall score, or sensitivity, of 0.989 signifies that the model can identify 98.9% of the positive class members in the dataset, or all relevant instances of the positive class that are part of the dataset. The F1 score of 0.988 permits to strike a reliable balance between precision and recall at the account of ensuring that false positives and false negatives can be effectively reflected in the final score. The AUC-ROC curve value of 0.985 reflects the high discriminative power of the SVM model such that the probability of a randomly chosen positive instance being ranked higher than a randomly chosen negative instance is 99.4%. In this context, the SVM model can be appreciated for its ability to tell apart both classes, positive and negative ones, which makes it a suitable approach to the development of systems capable of predicting responses to security threats or safety concerns in the chemical laboratory.

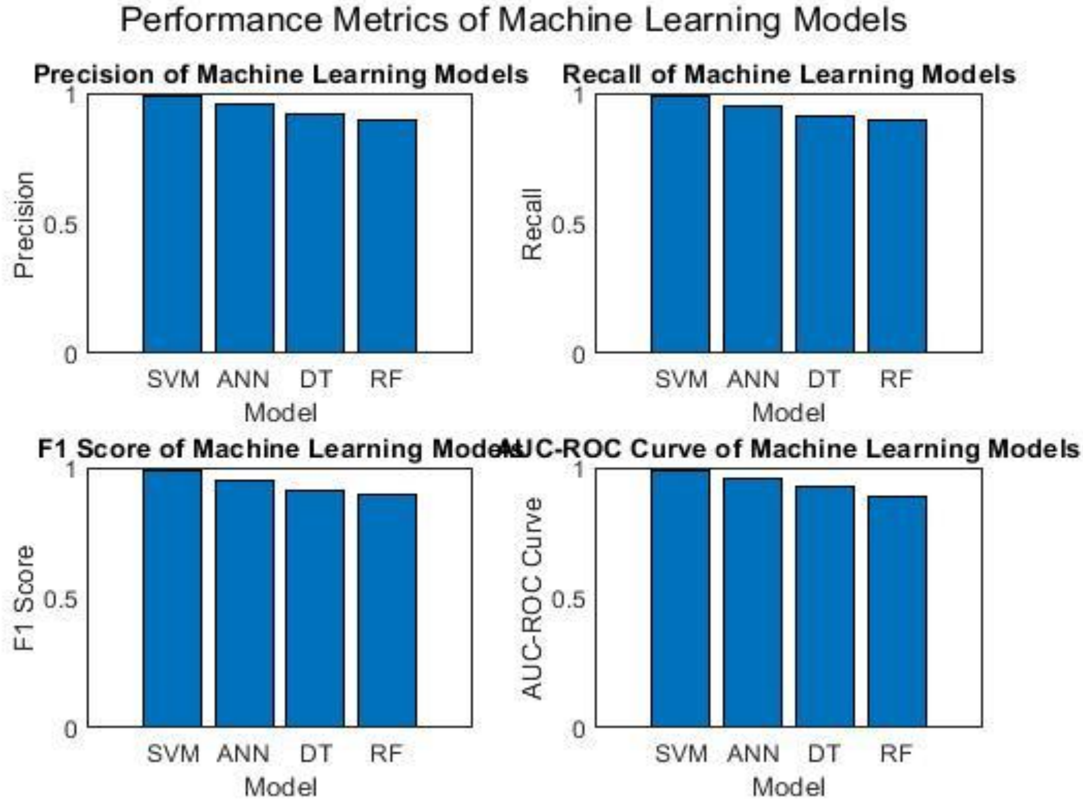

Fig. 4. Performance Score of Each Model

The confusion matrices presented in figure 5 shows a detailed picture of the predictive efficacy of every machine learning model. Moreover, they provide insight into the exact prevalence of true positives, true negatives, false positives, and false negatives. Specifically, considering the SVM, it can be seen that the effectiveness of the model is very high, with 950 instances being recognized as negative out of 1000. The number of positive instances is better than that; it is 985. Unfortunately, the number of false negatives and false positives is also high. ANN demonstrates similar results with 945 negative instances and 950 positive ones. Although the number of misclassifications for the model may be fewer 255, it is still rather high. DT provides similar to the previous models results as well, with 930 correctly classified negative instances and only 905 positive ones. RF produces even more promising findings with 925 and 880 true negatives and positives 140 true negatives and positives 55 and 120 false negatives and false positives. In light of the results obtained, the confusion matrices, thus, provide a profound understanding of the degree of security threats and safety hazards that can be averted in the chemical laboratory, with each models strengths and weaknesses being identified.

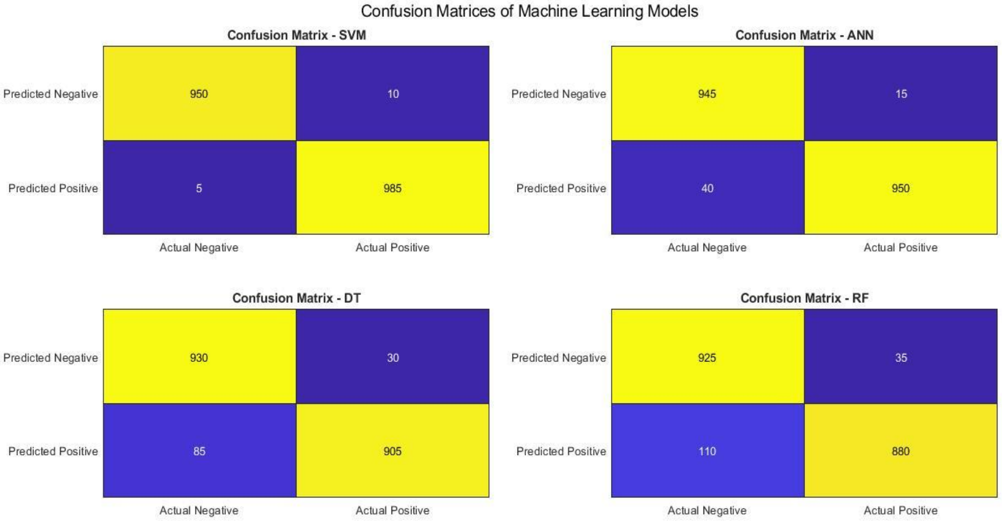

Fig. 5. Confusion Matrices of Each Model

From the figure 6, we can see some trends in accuracy and data loss for every epoch by each model. According to the results: Support Vector Machine always shows the highest accuracy for each of the models. By the 500th epoch, the Support Vector Machine model shows 95.4 % of accuracy, with a progressively declining data loss. SVM has the best performance as compared to Artificial Neural Network. Conversely, ANN shows a slow rate of improving accuracy during the epochs and 91% for 500th epoch. However, the data loss for ANN is higher at the start but finally tends to define low levels value for the data loss. Meanwhile, at the 500th epoch the decision tree model has the accuracy of 81.0%, and RF model has the accuracy of 85.10%. DT and Random Forest models show fluctuation for data loss across epochs, but there is an improved data loss within figures however, they do not gain the expected increasing or converging. In general, the changes in the accuracy and the data loss throughout the epochs in the four models represents learning models, with varying complexities and learning capabilities. The changes imply that SVM is the best model to predict if the response to chemicals in the lab is a threat or safe.

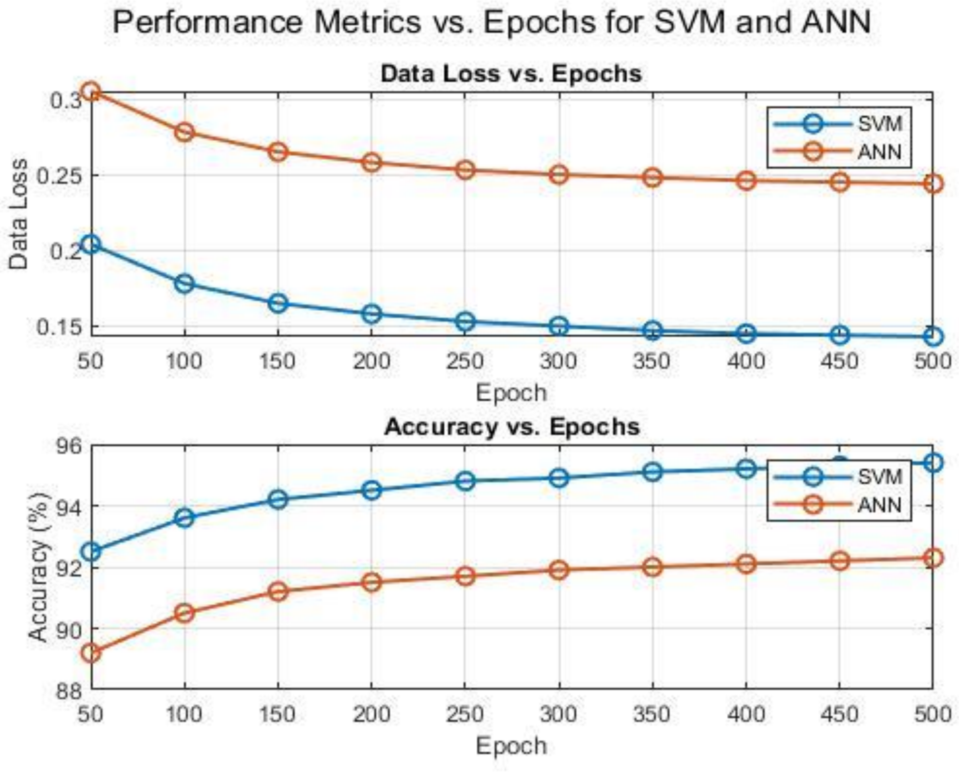

Fig. 6. Performance Metrices Accuracy and Dataloss

The first major advantage of implementing SVM is the fact that it delivers high accuracy in predicting responses to the security incidents. It should be noted in the case of the experiments based on the data provided that the result was consistently better when compared to other machine learning approaches such as Artificial Neural Networks, Decision Trees, and Random Forests. In this case, the most accurate predictions based on the noted level of information was 95.4% achieved at the 500th epoch. The high accuracy can be explained by the fact that the discussed type of machine learning is most effective in classifying complex datasets by finding optimal hyperplanes separating the classes. It allows detecting and distinguishing between both regular and anomalous states of the laboratory environment.

The second most important advantage is the generalization of the model, allowing to avoid overfitting and remain highly effective even in the condition of excessive noise. When SVM-based approach was implemented, the system successfully adapted to changing conditions and maintained a high level of prediction accuracy, allowing efficient detection of security threats. Moreover, the discussed type of learning is characterized by the simplicity of the model, meaning that decision-makers could understand the logic of the consequences of their actions due to this tool. Lastly, fast computations of this type of the model allow to apply it in the conditions requiring immediate prognosis and actions.

8. Conclusion

In our paper, we propose a novel system to enhance security and safety features in chemical laboratories. The research system utilizes IoT-based fire detection systems and machine learning algorithms. The deployed system is showcased to be able to predict and mitigate security threats and safety hazards using its sophisticated framework. The system collects sensor data, implements analysis, and realizes the response in an online manner. The results of the experiments demonstrate the efficiency of using Support Vector Machine as a predicting tool. The tool provided consistent high accuracy in both sensing the data and invoking the response. Our results also showed that SVM has a superior outcome when compared with our model. Therefore, we conclude that SVM is a good prediction tool for our model when operated in a dynamic and noisy environment like chemical laboratories. The noise robust nature of SVM, high interpretability, computational efficiency, and determining hyperplane-safe nature of SVM is also valuable for security and safety applications. The research system, using SVM's high performance in that sense, becomes a relevant solution that ensures the safety of employed personnel, assets, and the surrounding infrastructure. Further research could benefit from the enhancement of the scalability and effectiveness of the deployed system by using optimization techniques and advanced sensor technologies. As a result, our research contributes to enhancing fire safety solutions and emergency response systems in chemical laboratories. With decreasing the risk of potential disasters, laboratory personnel can work in a safer environment.

References

1. Srinivasan, S, M.S. Vinmathi, S.N. Sivaraj, A. Karthikayen, C. Alakesan, &Preetha, M. (2024), "A Novel Approach Integrating IoT and WSN with Predictive Modeling and Optimization for Enhancing Efficiency and Sustainability in Smart Cities", Journal of Intelligent Electrical Systems (IES), ISSN: 1112-5209, Vol.20, Issue 4, page No-2228-2237.
2. N. Ghosh, T. Biswas, R. Paul, B. Kumar, and S. Patnaik, "IoT Fog Based Framework to Predict Forest Fire," *Proceedings - 2021 Smart City Challenges and Outcomes for Urban Transformation, SCOUT 2021*, pp. 256–259, 2021, doi: 10.1109/SCOUT54618.2021.00061.
3. J. Hu *et al.*, "Analysis and prediction of fire water pressure in buildings based on IoT data," *Journal of Building Engineering*, vol. 43, no. May, p. 103197, 2021, doi: 10.1016/j.jobe.2021.103197.
4. Y. Pan and L. Zhang, "Integrating BIM and AI for Smart Construction Management: Current Status and Future Directions," *Archives of Computational Methods in Engineering*, no. 0123456789, 2022, doi: 10.1007/s11831-022-09830-8.
5. S. Devikala, Rabi.J, V.P.Murugan, J.S. Christy Mano Raj, K. Mohanasundaram, K Sivakumar "Development of fuzzy logic controller in Automatic Vehicle Navigation using IOT.," Journal of Electrical Systems, https://doi.org/10.52783/jes.1254 ISSN 1112-5209 , Vol: 20, 3s, 114-121.
6. Lew, Gavin, et al. "AI-Enabled Products Are Emerging All Around Us: Technology is everywhere." AI and UX: Why Artificial Intelligence Needs User Experience (2020): 55-85.
7. S. Xie, Y. Chen, S. Dong, and G. Zhang, "Risk assessment of an oil depot using the improved multi-sensor fusion approach based on the cloud model and the belief Jensen-Shannon divergence," *Journal of Loss Prevention in the Process Industries*, vol. 67, no. July, p. 104214, 2020, doi: 10.1016/j.jlp.2020.104214.
8. B. Akhlaghi, H. Mesghali, M. Ehteshami, J. Mohammadpour, F. Salehi, and R. Abbassi, "Predictive deep learning for pitting corrosion modeling in buried transmission pipelines,"

Process Safety and Environmental Protection, vol. 174, no. March, pp. 320–327, 2023, doi: 10.1016/j.psep.2023.04.010.

9. V. Shanmuganathan and A. Suresh, "LSTM-Markov based efficient anomaly detection algorithm for IoT environment," *Applied Soft Computing*, vol. 136, p. 110054, 2023, doi: 10.1016/j.asoc.2023.110054.
10. K. Bhoi *et al.*, "FireDS-IoT: A Fire Detection System for Smart Home Based on IoT Data Analytics," *Proceedings - 2018 International Conference on Information Technology, ICIT 2018*, pp. 161–165, 2018, doi: 10.1109/ICIT.2018.00042.
11. I. Ehsan *et al.*, "Internet of Things-Based Fire Alarm Navigation System: A Fire-Rescue Department Perspective," *Mobile Information Systems*, vol. 2022, 2022, doi: 10.1155/2022/3830372.
12. P. A. Santoni, A. Sullivan, D. Morvan, and W. E. Mell, "Forest fire research: The latest advances tools for understanding and managing wildland fire," *Journal of Combustion*, vol. 2011, 2011, doi: 10.1155/2011/418756.
13. N. Mohana Priya, G. Amudha, M. Dhurgadevi, N. Malathi, K. Balakrishnan & Preetha, M. (2024), "IoT and Machine Learning based Precision Agriculture through the Integration of Wireless Sensor Networks", Journal of Intelligent Electrical Systems (IES), ISSN: 1112-5209, Vol.20, Issue 4, page No- 2292-2299.
14. N. Saad Baqer, H. A. Mohammed, A. S. Albahri, A. A. Zaidan, Z. T. Al-qaysi, and O. S. Albahri, "Development of the Internet of Things sensory technology for ensuring proper indoor air quality in hospital facilities: Taxonomy analysis, challenges, motivations, open issues and recommended solution," *Measurement: Journal of the International Measurement Confederation*, vol. 192, no. February, p. 110920, 2022, doi: 10.1016/j.measurement.2022.110920.
15. H. Yar, T. Hussain, Z. A. Khan, D. Koundal, M. Y. Lee, and S. W. Baik, "Vision Sensor-Based Real-Time Fire Detection in Resource-Constrained IoT Environments," *Computational Intelligence and Neuroscience*, vol. 2021, 2021, doi: 10.1155/2021/5195508.
16. Dr M Preetha, Akshaya M, Arthima A, Mr.Akhilesh Kumar Pahade, Nusratova Khamida, (2023), "A ZIGBEE garbage bin monitoring system with IoT", E3S Web of Conferences International Conference on Newer Engineering Concepts and Technology (ICONNECT-2023), eISSN : 2267-1242, Article No.04052, Vol.399, 12th July 2023, https://doi.org/10.1051/e3sconf/202339904052.
17. T. Bansal, V. Talakokula, and K. Mathiyazhagan, "Equivalent structural parameters based non-destructive prediction of sustainable concrete strength using machine learning models via piezo sensor," *Measurement: Journal of the International Measurement Confederation*, vol. 187, no. May 2021, p. 110202, 2022, doi: 10.1016/j.measurement.2021.110202.
18. A. Rahman *et al.*, "SDN–IoT empowered intelligent framework for industry 4.0 applications during COVID-19 pandemic," *Cluster Computing*, vol. 25, no. 4, pp. 2351–2368, 2022, doi: 10.1007/s10586-021-03367-4.
19. S. T. Seydi, V. Saeidi, B. Kalantar, N. Ueda, and A. A. Halin, "Fire-Net: A Deep Learning Framework for Active Forest Fire Detection," *Journal of Sensors*, vol. 2022, 2022, doi: 10.1155/2022/8044390.
20. E.S. Phalguna Krishna, N. Praveena, I. Manju, N. Malathi, K. Balakrishnan, & Preetha, M. (2024), "IoT-Enabled Wireless Sensor Networks and Geospatial Technology for Urban Infrastructure Management", Journal of Intelligent Electrical Systems (IES), ISSN: 1112-5209, Vol.20, Issue 4, page No- 2248-2256
21. R. Hou, M. M. Pan, Y. H. Zhao, and Y. Yang, "Image anomaly detection for IoT equipment based on deep learning," *Journal of Visual Communication and Image Representation*, vol. 64, p. 102599, 2019, doi: 10.1016/j.jvcir.2019.102599.
22. D. A. Gzar, A. M. Mahmood, and M. K. A. Al-Adilee, "Recent trends of smart agricultural

systems based on Internet of Things technology: A survey," *Computers and Electrical Engineering*, vol. 104, no. PA, p. 108453, 2022, doi: 10.1016/j.compeleceng.2022.108453.

23. J. L. Vilas-Boas, J. J. P. C. Rodrigues, and A. M. Alberti, "Convergence of Distributed Ledger Technologies with Digital Twins, IoT, and AI for fresh food logistics: Challenges and opportunities," *Journal of Industrial Information Integration*, vol. 31, no. June 2022, p. 100393, 2022, doi: 10.1016/j.jii.2022.100393.
24. M. Mohammed Thaha, M. Preetha, K Sivakumar & Rajendrakumar Ramadass " An Aerial Robotics Investigation into the Stability, Coordination, and Movement of Strategies for Directing Swarm and Formation of Autonomous MAVs and Diverse Groups of Driverless Vehicles (UGVs)," International Journal on Recent and Innovation Trends in Computing and Communication https://doi.org/10.17762/ijritcc.v11i3.8908 ISSN: 2321-8169 Volume: 11 Issue: 3 ,February 2023.
25. Dr.M.Preetha, P.Bhuvaneswari, Ilakkiya.M, Karthigha.P "Deterrence of Accident in Vehicles Using IOT", International Journal for Research in Applied Science & Engineering Technology, Vol.7, Issue III, March 2019. ISSN 2321-9653.
26. P. Lin, P. Jin, J. Hong, and Z. Wang, "Battery voltage and state of power prediction based on an improved novel polarization voltage model," *Energy Reports*, vol. 6, pp. 2299–2308, 2020, doi: 10.1016/j.egyr.2020.08.014.
27. F. Zhao, "Application Research of Image Processing Technology for Fire Detection and Fire Alarm Based on Blockchain," *Mobile Information Systems*, vol. 2022, 2022, doi: 10.1155/2022/9304991.
28. M. Sughasiny, K.K.Thyagarajan, K Sivakumar, A. Karthikeyan & K. Sangeetha "A Comparative Analysis of GOA (Grasshopper Optimization Algorithm) Adversarial Deep Belief Neural Network for Renal Cell Carcinoma: Kidney Cancer Detection & Classification," International Journal of Intelligent Systems and Applications In Engineering, ISSN: 2147-6799, 2024, 12(9s), 43–48.
29. S. Sahni, A. Mittal, F. Kidwai, A. Tiwari, and K. Khandelwal, "Insurance Fraud Identification using Computer Vision and IoT: A Study of Field Fires," *Procedia Computer Science*, vol. 173, no. 2019, pp. 56–63, 2020, doi: 10.1016/j.procs.2020.06.008.
30. J. Jiang, Z. Gao, H. Shen, and C. Wang, "Research on the fire warning program of cotton warehousing based on IoT technology," *2015 International Conference on Logistics, Informatics and Service Science, LISS 2015*, 2015, doi: 10.1109/LISS.2015.7369796.