An Artificial Intelligent (AI) Automated Compliance Framework for Securing Critical Infrastructure

Mamilla Divya[1], Dr. M. Mallikarjuna Rao[2], D. Venkatesh[3]

[1,2,3] Computer Science and Engineering, PVKK Institute of Technology

---***---

Abstract - The project is called as An AI-Based Automated Compliance Framework to secure the critical infrastructure. The project will provide an automated system of securing critical infrastructure with a machine learning/ Artificial Intelligence-based tool that will provide a timely and correct compliance mechanism (activated by the identified network attacks activity) and predictive models. These predictive models will be machine learning that will be used to process the network traffic data to predict detected active network threats, such as CROSS-SITE SCRIPING (XSS), DDoS, Man-in-the-Middle (MITM), Structured Query Language (SQL Injection), etc. In order to allow the users to utilize the framework and upload their network traffic data to the service, visualize and analyze compliance recommendations based on the security framework, an artificial intelligent User Interface (Flask/MySQL/joblib) was developed. The final output of this project is to adorn an automated process of compliance/security that will facilitate timely and fitting detection, analysis and response of new security threats to critical infrastructure.

Keywords: Automated Compliance Framework, Artificial Intelligence, Critical Infrastructure Security, Network Attack Detection, Machine Learning, Model training, predictive models, real-time predictive analytics, security.

1. INTRODUCTION

The important infrastructure such as power systems, water systems and transportation systems has turned out to be a matter of concern in the contemporary digital and globalized world. Advanced cyberattacks are also targeting such critical systems that may result in service disruption, financial losses, and a risk to the national security [1]. The traditional security systems rely on rules and human processing which is difficult to justify the requirement to detect new and dynamic cyber threats in real time. In this project, it will be possible to propose an AI- and machine learning-based compliance model, which can be implemented to enhance the security of vital infrastructure. The framework can also identify network traffic to identify the cyber threats that include Distributed Denial of Service (DDoS), SQL Injection, Cross-site Scripting (XSS) and Man-in-the-Middle (MITM) attack. Machine learning models (a Random Forest, Support Vector Regression, and Logistic Regression), are used to do real-time threat classification and prediction [2]. Based on the perceived risks, the system proposes the proper compliance measures that entail input validation, filtering of traffic, round-the-clock monitoring and multi-factor authentication. The architecture is implemented as a secure, safe, and web-based application that is written using Flask and MySQL and offers an alternative effective and convenient means of the traditional security strategies.

a) Objective of Project:

The main aim of the given venture is to develop and deploy an automated compliance and security system that would enable the protection of critical infrastructures against a vast variety of cyber-attacks, relying on the solutions that are grounded on artificial intelligence and machine learning. The framework will be displayed in a continuous monitoring of network operations, determination of potential risk areas, and assist the companies to react to the necessary security requirements, standards and institutional policies. They will be using historical data of network traffic to train machine learning models that will identify and label cyberattacks like Cross-Site Scripting (XSS), Distributed Denial of Service (DDoS), Man in Middle (MITM) and SQL Injection (SQLi). Depending on the risks identified, the system will provide feasible compliance recommendations, such as the input validation, multi-factor authentication, the sifting out of the suspicious traffic, and constant lurking over the system. The preventative practice will enable organizations to stop the attack, react to it more speedily, and stay connected to the regulations in all significant services.

b) Motivation:

With the development of digital technologies in the government and industries, the critical systems are increasingly exposed to enhanced cyberattacks. Incidents such as the DDoS attacks on social services and MITM attack on the financial services present the need to have more advanced cybersecurity practices. The traditional security and compliance procedures require a lot of manual work and, therefore, are rather inefficient, slow, and prone to errors. In addition, network traffic is getting bigger and more intricate, and conventional ways of monitoring cannot identify the threat in time. With the help of machine learning, organizations have the opportunity to automate the threat detection process, enhance the efficiency of the compliance process, reduce the response time, and will make critical infrastructure more resistant to emerging cyber threats.

2. RELATED WORK

One of the applications of AI is an extensive point of focus in recent studies of cybersecurity in the context of defending critical infrastructure against cyber threats. Examples of predictive machine learning models that have been studied widely to analyze network traffic and identify active threats include Cross Site Scripting (XSS), Distributed Denial of Service (DDoS), SQL Injection, and Man in the Middle attacks are: Random Forest, Support Vector Regression, and Logistic Regression [3]. It has been found that network security predictive analytics is more accurate and faster to detect than the protection signature-based practices [4]. The threat classification of real time set ups has also been improved by ensemble techniques and hybrid learning techniques [5].

It has been suggested to implement automated compliance systems based on machine learning that will evaluate and implement security policies on the fly and minimize manual interventions and enhance responsiveness [6]. The structures of AI-based approaches coupled with real time surveillance have facilitated the development of adaptive security controls with responses to observed abnormalities [7]. The identification of unknown or changing attack patterns can be done reliably by real time threat detection systems which combine a network feature extraction with ML classification [8]. They are supervised learning models which are trained on labeled attack samples to distinguish between benign and malicious traffic [9].

Moreover, the combination of user-friendly interfaces and back-end services, which can be created on top of applications such as Flask and databases such as MySQL, makes security platforms more usable and accessible to stakeholders who can engage with forecasting results and compliance suggestions [10]. With technologies like joblib, machine learning models can be efficiently serialized and can also be inferred in real time [11]. The study has also highlighted the importance of scalable AI systems that are able to support high throughput network environments without compromising its performance [12]. The importance of the combination of AI driven detection and automated response mechanisms as a way of minimizing the mean time to detect and respond is emphasized in critical infrastructure security studies [13],[14].

3. PROPOSED METHODOLOGY

Major machine learning models that can be deployed to a classification or regression problem are multi-layer perceptron (MLP), decision tree, XGBoost, gradient boosting, K-Nearest Neighbors (KNN), logistic regression and random forest. The tabular data is learnt by the various models differently.

The neural network known as MLP learns by processing input data through multiple sets of neurons. Every neuron uses the weighted combination of inputs and an activation function and the weights change according to prediction errors. MLP is good in the modeling of non-linear patterns in the data, which are complex. Decision Trees divide the data according to features values in order to minimize uncertainties at every node. This is repeated until a stopping criterion is satisfied resulting in a tree-like structure of the decision-making process. These trees are simple to interpret and visualize and are likely to overfit.

XGBoost and Gradient Boosting are the ensemble techniques, which combine building trees in a row. Every tree is conditioned to correct the mistakes of the former. XGBoost is further optimized with regularization to minimize overfitting and accelerate training. These are robust models when dealing with different forms of data as well as complex patterns. KNN is a straightforward algorithm in which the model makes a classification of a point according to the majority of the closest points. It is useful in situations in which the boundaries of decisions are non-linear but may be computationally intensive in case of a big dataset.

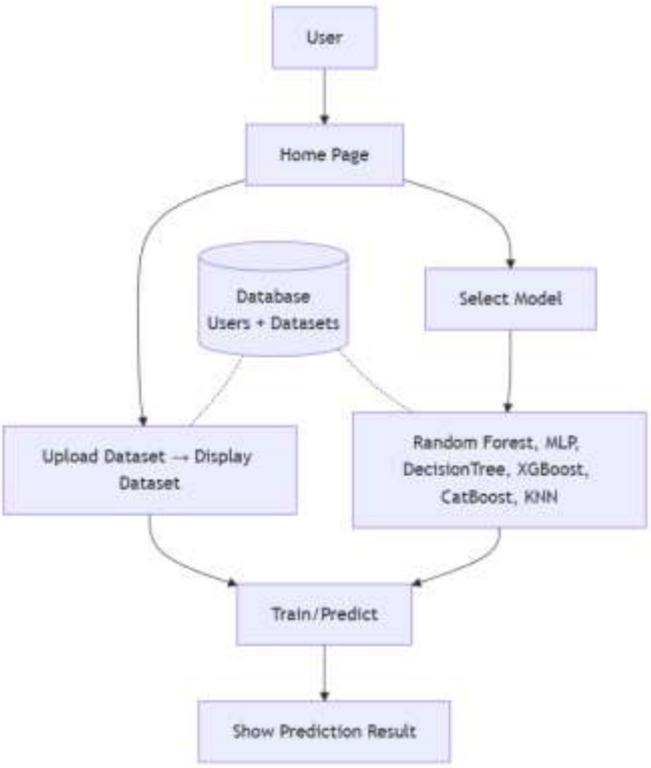

User
Home Page
Database
Users + Datasets
Select Model
Upload Dataset → Display Dataset
Random Forest, MLP, DecisionTree, XGBoost, CatBoost, KNN
Train/Predict
Show Prediction Result

Figure 1 Architecture Diagram

The Logistic Regression is a linear binary classification model. It estimates the likelihood of an example to belong to a particular group by weighted accumulation of the entry characteristics with the help of a logistic operation. Although it is simple, it functions effectively with a separation data that is linear. Random Forest: It is a set of Decision Trees and each tree is trained on a random sample of both features and of data points. Combination of all the trees increases the accuracy and strength of the predictions compared to single trees.

Such models have been chosen due to their strengths in various situations. MLP and Random Forests are adaptable and they can work with complex data, whereas Decision Trees are interpretable. High performance bias and variance reduction is achieved by boosting and KNN can be used on non-linear problems and Logistic Regression is simple to be used where binary classification is required. Collectively, they constitute a toolkit that is diverse in solving machine learning problems.

4. RESULTS AND DISCUSSSION

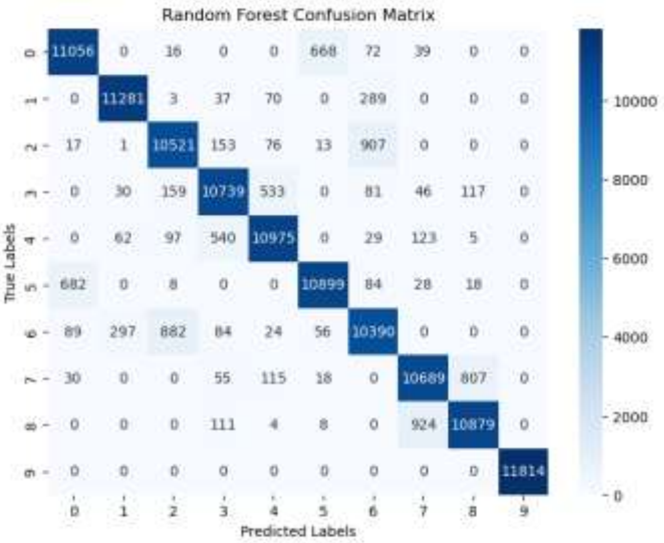


Figure 2 Randon Forest Confusion Matrix

Based on Figure 2, the accuracy of most of the classes is high with the diagonal values indicating the correctly predicted cases of each of the classes. The model is really high in most of the classes and a huge percentage of the true labels are being predicted right. As an example, the number of correct predictions in class 0 (11,056) is high, whereas relatively more misclassifications are observed in such classes as 3 and 5, with the off-diagonal values being 159 and 540, respectively. Comprehensively, the model is well performing and has a low misclassification.

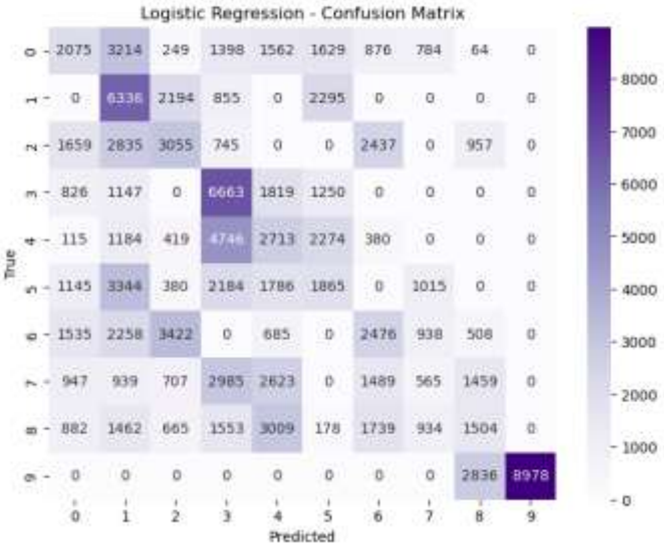


Figure 3 Logistic regression Confusion Matrix

Based on Figure 3, the confusion matrix demonstrates a good level of performance, especially on classes 1, 4 and 9 which showed a high number of corrects (6,336,4,746 and 8,978, correspondingly). Nonetheless, some of the classes have significant misclassifications, including class 0, in which 3,214 cases were incorrectly classified as class 1, and class 5, where the misclassification to class 3 and 8 can be observed. The model works well on the higher frequency classes, but is not so prevalent as some of the misclassifications are higher in the frequencies where the model predicts with the greatest accuracy.

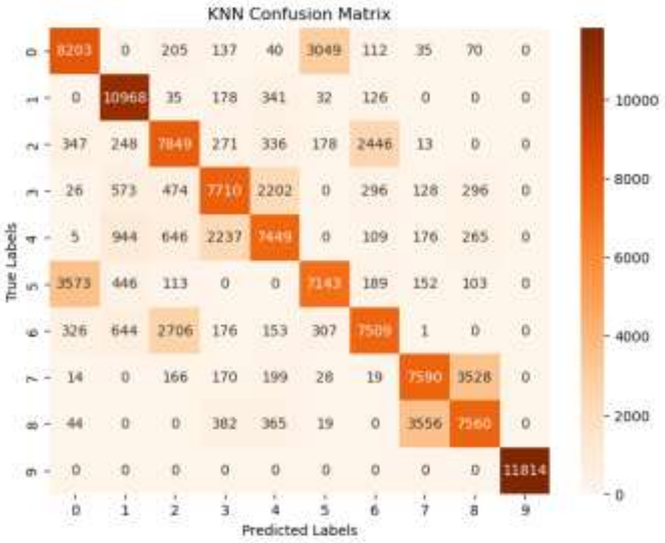


Figure 4 KNN Confusion Matrix

Based on Figure 4, the confusion matrix reveals that the model is performing well on most of the classes especially on the class 9 with 11,814 accurate predictions. Misclassifications are however witnessed in classes 0, 3 and 4 with instances being classified as wrong classes, e.g., the class 0 being misclassified as class 4 and 5. Nevertheless, the model is effective in the high-frequency classes such as 1, 7 and 9 and the off-diagonal numbers in other classes implies that there are relatively low misclassification rates. In general, KNN demonstrates good results on the dataset.

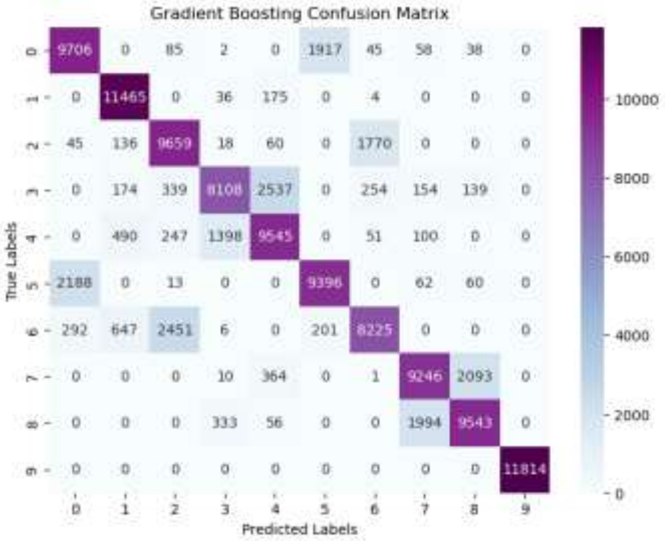


Figure 5 Gradient Boosting Confusion Matrix

Based on Figure 5 above indicates that the model has a high degree of performance, more so with the class 9 which has 11,814 instances of the model that are correctly classified. Nonetheless, classes 0, 3, and 4 have certain misclassifications including standout misclassifications of 1,917 in class 0 and 2,537 in class 3. These are minor errors that still exist but these were not very numerous in contrast to the number of correct predictions. All in all, the model is very accurate with a small error in lower frequency classes which means that the model is very strong enough to deal with different patterns in the data.

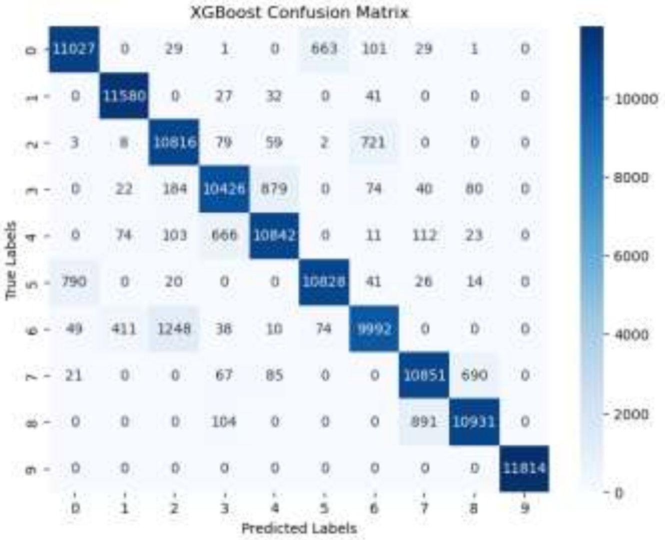


Figure 6 Xgboost Confusion Matrix

Based on Figure 6, exhibits excellent performance especially in class 9 where there are 11,814 correct predictions. Most of the classes are also dealt with properly by the model with the class 1 and class 3 being the most accurate (11,580 and 10,426 correct predictions, respectively). There are however certain misclassifications in the class 0, 2 and 4, where cases are incorrectly predicted in classes 0, 2 and 4 like 663 in the class 0 is wrongly predicted in the class 4. However, despite these misclassifications at a few occasions, the overall accuracy of the model is very high, with small errors in lower frequency classes, which shows that the model is effective at identifying patterns in the data.

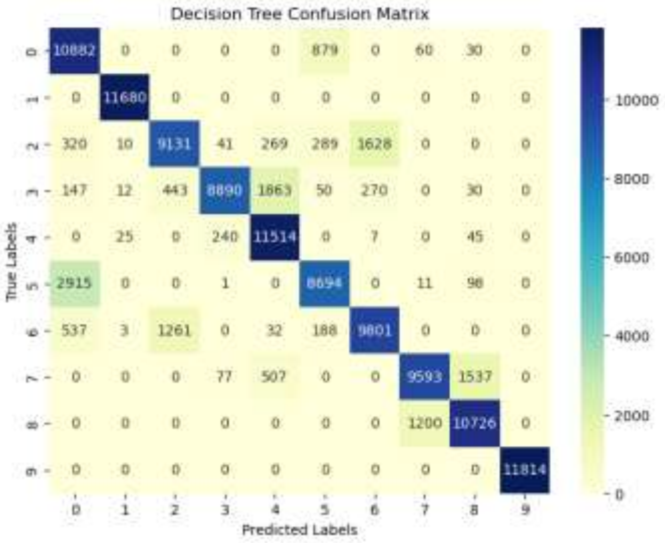


Figure 7 Decision Tree Confusion Matrix

According to Figure 7, a great performance, especially in terms of class 9, which represents 11,814 correct predictions of the model. Classes 1, 2 and 4 are also highly accurate with 11,680, 9,131 and 11,514 correct predictions respectively. There however exists significant misclassification in classes 0 and 7 with the cases of the class 0 misclassified as class 3 (879) and class 7 (60). The overall performance of the model is high, and there are only some slight misclassifications, which is why this model is capable of observing patterns and classifying most of the classes accurately.

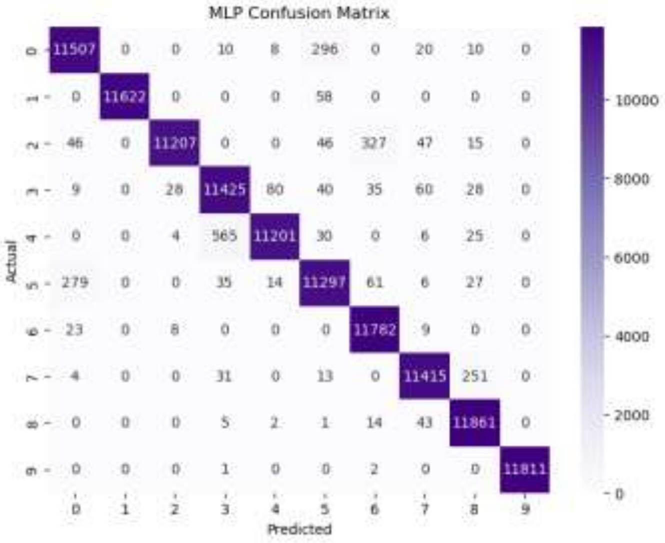


Figure 8 MLP Confusion Matrix

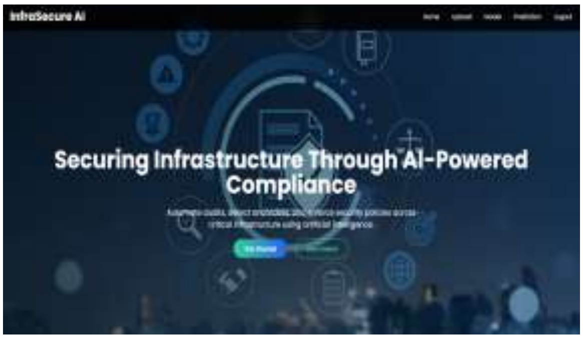
Based on Figure 8, it shows that it has good performance, particularly among the class 1 where it has 11,622 correct predictions. Accuracy in the model of class 0, 2, 3, 4 and 9 is also high with the majority of the diagonal value being correct prediction. There are however certain misclassifications like class 0, with 296 instances predicted to be class 4, and 5, with 61 misclassified instances. All in all, the model is a good one with some minor misclassification particularly in the low frequencies classes.

Table 1 Model Performance Table

Algorithm	**Accuracy**	**Precision**	**Recall**	**F1 Score**
Random Forest	0.93	0.93	0.93	0.93
Logistic Regression	0.31	0.31	0.31	0.29
Decision Tree	0.87	0.88	0.87	0.87
XGBoost	0.93	0.93	0.93	0.93
Gradient Boosting	0.82	0.82	0.82	0.82
KNN	0.71	0.71	0.71	0.71
MLP	0.99	0.98	0.98	0.98

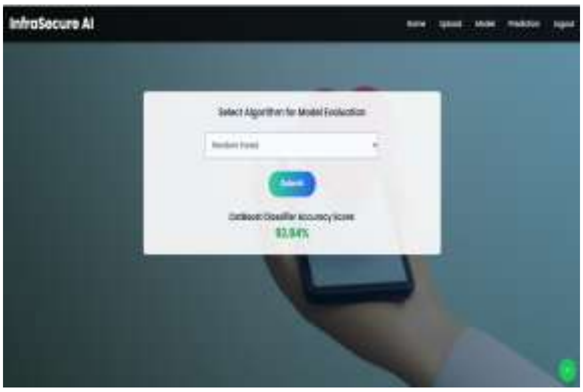
Table 1 shows that the output of the different machine learning algorithms on the measures of accuracy, precision, recall, and F1 score are rather different. Multi-Layer Perceptron (MLP) has the greatest performance since it has the highest accuracy of 0.99, has high performance in terms of accuracy, recall and F1 score of 0.98 and thus the most reliable at this dataset. The accuracy of even the Random Forest and XGBoost are 0.93 and high percentage of precision, recall and F1 score and that means, they are good at classifying data. Logistic regression on the other hand gives results that are much lower only 0.31 and this indicates that it is very poor. The moderate performance of decision tree and gradient boosting is 0.87 and 0.82 respectively. KNN has the worst performance in the tree models with 0.71 in all metrics. Overall, MLP is the most powerful model that will be applied to this task.

UI SAMPLES:



Home page

Upload page



Model page

Prediction Page

5.CONCLUSION & FUTURE ENHANCEMENT

Automated Compliance Framework on Critical Infrastructure Security indicates an intelligent and practical approach of making sure that the major systems are not compromised by the new cyber-attackers. Based on the machine learning algorithms such as the Random Forest, the Support Vector Regression and the Logistic Regression, the framework is able to detect the network traffic to detect attacks in the form of XSS, DDoS, mitigation in the middle and SQL Injection. The system also provides feasible compliance suggestions in addition to adequate threat identification, such as input validation, multi-factor authentication, traffic filtering, and round-the-clock monitoring, hence enabling the organization to take preventative measures early enough. The framework has been implemented on a secure web-based platform with Flask, MySQL, and Joblib which means that the framework can be deployed easily, scaled and that the models can be managed effectively. This automated strategy minimizes the use of manual security functions and enhances the speed and accuracy of responsiveness hence a cost-effective and dependable measure of protection of the critical infrastructure.

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to my guide and faculty members for their valuable guidance and continuous support in completing this research work titled “An Artificial Intelligence (AI) Automated Compliance Framework for Securing Critical Infrastructure.”

I also thank my institution and the Department of Computer Science for providing the necessary resources and support. Finally, I extend my heartfelt thanks to my friends and family for their encouragement and cooperation throughout the completion of this work.

REFERENCES

[1] A. Pinto, L. C. Herrera, Y. Donoso, and J. A. Gutierrez, “Survey on Intrusion Detection Systems Based on Machine Learning Techniques for the Protection of Critical Infrastructure,” *Sensors*, vol. 23, no. 5, pp. 2415, Feb. 2023, doi: 10.3390/s23052415.

[2] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, “Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study,” *Journal of Information Security*

and Applications, vol. 50, p. 102419, Feb. 2020, doi: 10.1016/j.jisa.2019.102419.

[3] M. Sannigrahi and R. Thandeeswaran, “Predictive Analysis of Network-Based Attacks by Hybrid Machine Learning Algorithms Utilizing Bayesian Optimization, Logistic Regression, and Random Forest Algorithm,” *IEEE Access*, vol. 12, pp. 142721–142732, 2024, doi: 10.1109/ACCESS.2024.3464866.

[4] M. Danish, “Enhancing Cyber Security Through Predictive Analytics: Real-Time Threat Detection and Response,” *International Journal of Advanced Computer Science and Applications*, vol. 16, no. 8, pp. 38–49, Aug. 2025, doi: 10.14569/IJACSA.2025.0160804.

[5] F. Alserhani and A. Aljared, “Evaluating Ensemble Learning Mechanisms for Predicting Advanced Cyber Attacks,” *Applied Sciences*, vol. 13, no. 24, pp. 13310, Dec. 2023, doi: 10.3390/app132413310.

[6] A. Mohammed, “AI in Cybersecurity: Enhancing Audits and Compliance Automation,” Accessed: Feb. 19, 2026.

[7] R. Sharma and J. Mahur, “Real-Time AI-Based Anomaly Detection in IoT Networks for Cybersecurity Threat Mitigation,” *Journal of Scientific Innovation and Advanced Research*, vol. 1, no. 5, 2025, Accessed: Feb. 19, 2026.

[8] M. Sarhan, S. Layeghy, N. Moustafa, M. Gallagher, and M. Portmann, “Feature extraction for machine learning-based intrusion detection in IoT networks,” *Digital Communications and Networks*, vol. 10, no. 1, pp. 205–216, Feb. 2024, doi: 10.1016/j.dcan.2022.08.012.

[9] S. Krishnan, A. Neyaz, and Q. Liu, “IoT Network Attack Detection using Supervised Machine Learning,” *International Journal of Artificial Intelligence and Expert Systems*, 2021, Accessed: Feb. 19, 2026.

[10] K. Mani and A. K. B. Shenoy, “Machine learning models in web applications: A comprehensive review,” *ICT Express*, vol. 11, no. 6, pp. 1110–1119, Dec. 2025, doi: 10.1016/j.icte.2025.09.001.

[11] P. Singh, “Deploy Machine Learning Models to Production: With Flask, Streamlit, Docker, and Kubernetes on Google Cloud Platform,” pp. 1–150, Jan. 2020, doi: 10.1007/978-1-4842-6546-8.

[12] K. C. Chaganti, “A Scalable, Lightweight AI-Driven Security Framework for IoT Ecosystems: Optimization and Game Theory Approaches,” *IEEE Access*, vol. 13, pp. 72235–72247, 2025, doi: 10.1109/ACCESS.2025.3558623.

[13] I. H. Sarker, “AI for Critical Infrastructure Protection and Resilience,” *AI-Driven Cybersecurity and Threat Intelligence*, pp. 153–172, 2024, doi: 10.1007/978-3-031-54497-2_9.

[14] M. A. Ameedeen, R. A. Hamid, T. H. H. Aldhyani, L. A. K. M. Al-Nassr, S. O. Olatunji, and P. Subramanian, “A Framework for Automated Big Data Analytics in Cybersecurity Threat Detection,” *Mesopotamian Journal of Big Data*, vol. 2024, pp. 175–184, Sep. 2024, doi: 10.58496/MJBD/2024/012.