Enhancing Detection and Counteraction of Routing Attacks on SCADA Networks in the Internet of Things through Advanced Artificial Intelligence Approaches

***Abdul Ahmed Abdul[1], Bashir Shehu[2], Abubakar Muhammad Abbas[3]**

[1]Infomation Technology Department,
Shamrock Innovations.

[2]Computer Science Department,
Ahmadu Bello University.

[3]Computer Science Department,
Bayero University Kano.

Corresponding Author:

Abstract

As SCADA (Supervisory Control and Data Acquisition) systems become more closely interconnected with the Internet of Things (IoT), they are also becoming more susceptible to routing attacks. These attacks can disrupt data transmission, manipulate routing tables, and potentially hijack control signals, causing significant damage to industrial processes. To effectively address these threats, advanced artificial intelligence (AI) approaches can be employed to enhance detection and counteraction capabilities. This paper explores the potential of AI-powered solutions for detecting, assessing, and mitigating routing attacks in SCADA networks in the IoT; This paper proposes and evaluates the use of gated recurrent units (GRU), convolutional neural networks (CNN), and multilayer perceptron classifiers (MLP) for detecting routing attacks in IoT networks. The classifiers are evaluated using accuracy, precision, recall, F1-score, and Matthew Correlation Coefficient (MCC). The results show that GRU outperforms both CNN and MLP in terms of all evaluation metrics. The paper also discusses the importance of feature selection and class-balancing strategies for generating reliable results. The study highlights the promise of deep learning techniques for routing attack detection and suggests that applying recent advancements in machine learning approaches for security will significantly progress this discipline.

Keywords: Routing Protocol for Low Power and Lossy Networks, Gated Recurrent Unit, Multi-layer Perceptron, Matthew Correlation Coefficient, F1-Score, Convolution Neural Network, Supervisory Control and Data Acquisition SCADA, Routing Attacks, Internet of Things.

INTRODUCTION

The increasing ubiquity of Internet of Things (IoT) devices in businesses, along with their steady expansion and significant financial outlays, confirms that IoT will remain relevant for the foreseeable future. A survey conducted in 2021 by IoT Analytics, a well-known German market research firm, found that the worldwide IoT market grew by 22% to reach USD 158 billion in annual investments. As of the end of 2022, it is estimated that there will be 14.5 billion connected IoT devices worldwide (Wegner, 2022). Even when the COVID-19 pandemic somewhat slowed down the growth of the Internet of Things, high-speed 5G networks are becoming more widely available and reasonably priced, and this will greatly improve connectivity and spark a new wave of IoT growth. With the integration of more IoT devices into organizational and mobile networks, the probability of these devices infiltrating networks supporting critical infrastructure sectors, as identified by the Cybersecurity & Infrastructure Security Agency (CISA), becomes more pronounced. The manufacturing, communications, commercial facilities, energy, financial services, agriculture, healthcare, IT, transportation, and water sectors are all classified as critical infrastructure sectors by CISA (Cybersecurity and Infrastructure Security Agency, 2022). IoT has enormous potential to change the world, but it also has significant security risks that put society and vital infrastructure at risk. Furthermore, the integration of the Internet of Things (IoT) and Supervisory Control and Data Acquisition (SCADA) systems have transformed industrial processes by allowing for real-time control, monitoring, and optimization. However, this integration has also introduced new security vulnerabilities and risks, making SCADA networks in the IoT increasingly susceptible to routing attacks. Routing attacks target the underlying communication infrastructure, disrupting data transmission, manipulating routing tables, and potentially hijacking control signals (Silverman et al., 2019).

In addition, IoT services are available in several industries, including manufacturing, energy, retail, healthcare, building management, and transportation. New issues with device management, data volume, storage, communication, computing, security, and privacy arise from the enormous scale of IoT networks. Many facets of the Internet of Things, including architecture, communication, protocols, applications, security, and privacy, have been extensively researched (Sha et al., 2018).But maintaining security, privacy, and customer happiness is crucial to the commercialization of IoT technologies (Hussain et al., 2020). Potential attackers face a wider range of threats with the integration of enabling technologies like as Software-Defined Networking (SDN), Cloud Computing (CC), and fog computing (Hussain et al., 2020). The sheer amount of data generated by Internet of Things devices may make standard techniques of data collecting, storage, and processing insufficient. The proliferation of intelligent devices and their mobility make the Internet of Things vulnerable to attacks from a variety of intelligent devices with constrained

computational resources, including low power, processor capacity, storage capacity, and connectivity limitations. IoT is vulnerable to routing attacks because of these constraints; sinkhole and selective forwarding attacks stand out as being especially dangerous (Choudhary & Meena, 2022). In a selective forwarding attack, one or more network nodes are compromised by a hostile node known as the attacker, who then chooses to drop a specific number of packets. In addition to filtering particular protocols, such as forwarding all RPL (Routing Protocol for Low Power and Lossy Networks) control messages while dropping the remainder packets in the route, this kind of attack tries to disrupt routing routes. The effects of selective forwarding attacks worsen when they are coupled with other attacks, such as sinkhole attacks. A sinkhole attack compromises data reception at the collecting point and undermines the integrity and dependability of sent data by the attacker trying to draw in the most traffic in a certain area.

Furthermore, the massive volume of data produced by Internet of Things devices offers chances for behavior analysis, assessments, forecasts, and pattern identification. However, in this context, new mechanisms are needed to unlock the value of IoT-generated data because of the heterogeneity of IoT-generated data, which presents hurdles for current data processing systems. Artificial Intelligence (AI) emerges as a highly suitable computational paradigm to embed intelligence in IoT devices (Hussain et al., 2020). AI empowers machines and devices to derive valuable insights from device- or human-generated data, enabling automated responses based on knowledge—an integral aspect of IoT solutions. Although AI is being used for a variety of tasks, including density estimation, regression, and classification, the main focus of this research is on how AI may help IoT networks with security and privacy (Hussain et al., 2020).

However, Routing attacks within IoT networks carry significant implications, leading to potential data loss, network downtime, and unauthorized access to sensitive information. The spectrum of dangers posed by possible attackers has expanded with the incorporation of supporting technologies like Software-Defined Networking (SDN), Cloud Computing (CC), and fog computing into the Internet of Things (IoT). Conventional data collection, storage, and processing methods face issues in handling the significant amount of data created by Internet of Things devices. Furthermore, the inherent limitations of IoT devices, including low computational resources and connectivity issues, render them susceptible to various routing attacks, with selective forwarding and sinkhole attacks emerging as particularly severe. These attacks disrupt routing paths, jeopardize the reliability and integrity of data, and can have dire consequences when executed.

The diversity in IoT-generated data compounds challenges for existing data processing mechanisms. Traditional approaches to detecting and preventing routing attacks in IoT networks have proven inadequate in

terms of accuracy, efficiency, and adaptability to evolving attack strategies. Many of these methods rely on static rule-based systems or signature-based detection techniques, struggling to keep pace with the dynamic nature of IoT networks and the advancing sophistication of attacks. Moreover, the sheer scale and heterogeneity of IoT networks, coupled with the resource constraints of IoT devices, make implementing robust security measures a formidable task.

To harness the valuable data produced by IoT devices effectively, innovative mechanisms are imperative. Recognized as a fitting computational paradigm, Artificial Intelligence (AI) plays a pivotal role in providing embedded intelligence in IoT devices. Artificial Intelligence (AI) enables robots and intelligent gadgets to extract valuable knowledge from data and modify their actions accordingly. AI has been effectively used in a variety of fields, including computer vision, fraud detection, bioinformatics, and authentication. In the context of the Internet of Things, AI is strategically used to provide intelligent security and privacy services.

RELATED WORKS

Li et al., (2021) use fault-discrimination information (FDI) to present an enhanced Stacking ensemble learning-based sensor fault detection approach for energy-related building systems. The study intends to create a data-driven model for sensor fault detection in building HVAC (heating, ventilation, and air conditioning) systems that has improved fault detection performance and a decreased false alarm rate. To create an ensemble learning detection approach with a relatively good generalization ability utilizing a stacking training manner, the proposed method uses four separate single models: principal component analysis, one-class support vector machine, K-Means clustering, and autoencoder; by deducting the statistics from each model's threshold, the fault-discrimination data is taken from the original samples. According to the data, their suggested approach performs better than the four individual models and conventional stacking when the added biases are between -4 °C and −2 °C and between 3.7 °C and 4 °C. On average, their suggested approach reduces the false positive rate by 5.76% and raises the Area under the ROC curve by 2.85%. Zhu et al., (2023)propose an Internet of Things (IoT) security detection method and system for sensing situations, along with a storage medium. The method involves discovering online equipment in the IoT, identifying asset information of the equipment, monitoring the state of the device, analyzing network behaviour to obtain early warning information, visually displaying the early warning information, and performing alarming or blocking according to the early warning information. Their system aims to solve the problems of poor effectiveness, low accuracy, and insufficient operability of IoT safety in the aspects of monitoring, early warning, and disposal. An extensive assessment of the literature on the application of AI techniques for cybersecurity attack detection in Internet of Things devices is given by (Mohamed et al., 2022). The study follows the PRISMA guidelines and

includes a thorough screening and selection process, as well as a detailed data extraction and classification of the selected studies. They also discuss the limitations and challenges of using AI for IoT cybersecurity. However, this study does not include studies written in other languages and only takes into account journal articles published between 2016 and 2021, which could restrict the review's applicability. Furthermore, a low level of accuracy is produced by some of the suggested frameworks in the chosen studies due to inadequate methodology and data analysis.

Alazab et al., (2023) suggest a novel Intrusion Detection System (IDS) for Internet of Things (IoT) infrastructure, which makes use of a feature set created especially to identify different kinds of routing assaults. The suggested solution is built on a hybrid intrusion detection system that uses a stacking ensemble method to combine two phases of detection for increased detection accuracy. The experimental results show that the hybrid IDS performs better in terms of accuracy and false alarm rate than other individual techniques and approaches published in earlier studies. The hybrid IDS uses an ensemble of C4.5 and one-class SVM in two cascaded phases. This study also covers the history of Routing Protocol for Low-Power and Lossy Networks (RPL) and how it was used in Internet of Things networks. A machine learning-based intrusion detection system is proposed by Raghavendra et al., (2022) to identify attacks on Internet of Things (IoT) networks that employ the Routing Protocol for Low-Power and Lossy Networks (RPL). The proposed system uses a combination of supervised and unsupervised learning techniques to detect attacks on the RPL protocol. The authors evaluate the performance of the system using a dataset of RPL traffic and show that it achieves high accuracy in detecting attacks while maintaining low false positive rates. The results suggest that the proposed system can be an effective tool for securing IoT networks against RPL-based attacks.

Zhang et al., (2022) offer a real-time abnormal operation pattern detection approach to create energy systems based on association rule bases. Expert systems and association rule mining are used in this strategy to create rule bases for both regular and aberrant operation patterns. Then, using the defined rule bases, an expert system for the real-time detection of anomalous operation patterns is developed. The suggested method is used to assess the performance of a real chiller plant. The findings indicate that the method is successful in detecting 15 types of known abnormal operation patterns and 11 types of unknown abnormal operation patterns. Irum et al., (2020) discuss the detection and prevention techniques against Distributed Denial of Service (DDoS) attacks in the Internet of Things (IoT) environment. This study provides a comparative analysis and analysis of different methods for preventing and detecting DDoS assaults on the Internet of Things. The report offers recommendations and goes into the reasons for the assessment based on certain evaluation criteria. The study makes the case that defensive measures against DDoS assaults should include preventive

procedures and that different strategies employ rate-limiting and filtering techniques to more reliably identify and stop DDoS attacks. Future work in the IoT arena, such as investigating the most recent AI and machine learning-based detection and prevention methods, is also covered in this study. They concluded that the proliferation of IoT devices has increased the likelihood of networks being vulnerable to the notorious DDoS attacks, but there are numerous methods for identifying and shielding networks from these attacks. Janani & Ramamoorthy, (2022) propose a threat analysis model to control IoT network routing attacks through a deep learning approach. To detect and categorize such assaults, the suggested model makes use of Long Short-Term Memory, Mayfly optimization technique, and ADASYN oversampling techniques. The suggested model is fresh and brings something fresh to the body of research already in existence.

METHODOLOGY

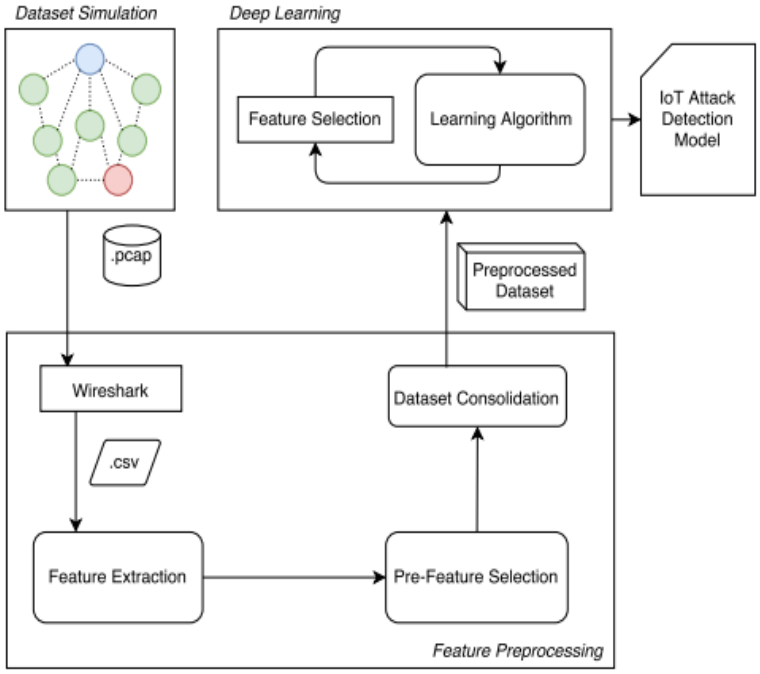

Figure 1: Designed Methodology Approach

This paper's technique is shown in Figure 1 above. The most crucial and first step before beginning the analysis is the data presentation. This paper suggests using artificial intelligence classifiers to identify routing hazards in Internet of Things networks. For this solution, we used the data set of simulated RPL attacks created using the Wireshark software tool. Also, as depicted above the methodology for the paper is described thus:

1. Dataset Simulation:
    - This is the initial step where the dataset for training and evaluating the deep learning model is generated (simulated).
    - The dataset simulation process involves creating

synthetic data that represents various IoT device behaviors, including both normal and anomalous (attack) patterns.
- This simulated dataset serves as the input for the subsequent feature preprocessing and deep learning stages.

2. Feature Preprocessing:
   - The preprocessing stage involves multiple steps to prepare the dataset for the deep learning model.
   - Wireshark is used as a tool for feature extraction from the dataset. Wireshark is a network traffic analysis tool that can extract relevant features, such as network packets, protocols, and communication patterns, from the IoT device data.
   - The extracted features are then passed through a "Feature Extraction" step, where additional feature engineering or transformation may be performed to create a more suitable input for the deep learning model.
   - The preprocessed dataset is then consolidated, potentially combining data from multiple sources or performing data normalization to ensure consistency and quality.
   - Finally, a "Pre-Feature Selection" step is performed, which involves selecting the most informative features from the consolidated dataset to be used as input to the deep learning model.
3. Deep Learning:
   - The deep learning component is the core of the methodology and consists of several key steps.
   - First, the "Feature Selection" step identifies the most relevant features from the preprocessed dataset that will be used as input to the deep learning model.
   - The "Learning Algorithm" is then applied to the selected features to train the deep learning model. The specific learning algorithm is not explicitly named in the figure, but it could be a neural network, or another deep learning architecture suitable for IoT attack detection.
   - The output of the deep learning process is the "IoT Attack Detection Model," which is the final model capable of detecting and classifying IoT attacks based on the learned patterns from the dataset.
4. Dataset Consolidation:
   - This step is mentioned separately in the figure,

indicating that it may be performed as a standalone process or in parallel with the feature preprocessing and deep learning stages.

- The dataset consolidation involves combining multiple datasets, potentially from different sources (e.g., simulated data, real-world IoT device data, or a combination of both), to create a comprehensive dataset for training and evaluating the deep learning model.

Moreover, the open-source Contiki/Cooja simulator was used to produce data through simulations that are comparable to real-life scenarios, while publicly available IoT attack data sets are not readily available. The raw packet capture (PCAP) files produced by the Cooja simulation are first transformed into CSV files so that text-based processing may begin. After that, the CSV files are loaded into our system's feature pre-processing module. The traffic flow data in the CSV files is used to calculate the features. A feature extraction procedure is first carried out. All datasets are then subjected to feature normalization to lessen the adverse effects of marginal values. Several features are eliminated during the pre-feature selection stage due to feature importance analysis amounting to a dataset of ~ 600,000. Following feature pre-processing, each scenario's relevant datasets are blended and labeled. This leads to the creation of the preprocessed dataset randomly, which includes both benign and attack data. An algorithm for deep learning and machine learning is fed to these datasets. IoT Attack Detection Models are generated by training deep layers with regularization and dropout algorithms and adjusting their weights. IoT devices have limited power consumption and resource availability. Due to these limitations, IoT security solutions should be effective and lightweight, placing as much of the processing and communication load on the end devices as feasible. Since our proposal just needs network packet traces which may be obtained outside by network recording equipment or specially designated nodes for the detection and prediction of attacks, it places the least amount of strain on the Internet of Things.

Furthermore, Gated Recurrent Units (GRU), Convolutional Neural Networks (CNN), and Multilayer Perceptron classifiers (MLP) are tested using the assault dataset. Accuracy, Precision, Recall, F1-score, and Matthew Correlation Coefficient (MCC) are the metrics used to compare the classifiers. More specifically, data preparation is utilized in artificial intelligence to reduce and clean data while also handling missing values to increase accuracy.

Moreover, the following four metrics, which capture samples that were properly and wrongly classified for each class, were used to evaluate the models in addition to the conventional performance measures:

- *True positive* (TP): Total number of positive samples that are appropriately coded as positive.
- *False positive* (FP): The number of positive samples that are mistakenly categorized as negatives.
- *False negative* (FN): The number of negative samples that are mistakenly identified as positive samples.
- *True negative* (TN): The count of negative samples that are accurately categorised as such.

The confusion matrix in Table 1 can be used to display the prior cases and convey all of the classification's results.

Table 1: Confusion Matrix

	Normal	Anomaly
Normal	True Positive (TP)	False Negative (FN)
Anomaly	False Positive (FP)	True Negative (TN)

According to Sokolova & Lapalme, (2009), accuracy serves as a gauge for the classifier's overall efficacy. This indicator displays the percentage of total instances that are successfully classified. Deng et al., (2016) define accuracy as follows:

$$Accuracy = \frac{TP + TN}{TP + FP + TN + FN}$$

1. Accuracy

A measure of precision indicates the percentage of accurately predicted affirmative cases. The statistic displays the frequency with which the model correctly predicts the target class—in this case, routing assaults in the Internet of Things networks. Precision, according to Deng et al., (2016), is computed as follows and indicates how accurately a particular class can be predicted.

$$Precision = \frac{TP}{TP + FP}$$

2. Precision

According to Sokolova & Lapalme, (2009), recall is a metric that indicates how well a classifier determines cases that are classified as positive. It demonstrates the binary classifier's capacity to recognize occurrences of a particular class(Deng et al., 2016). The formula for recall is as follows:

$$Recall = \frac{TP}{TP + FN}$$

3. Recall

The F-score is frequently used to assess a classifier's performance. The F-score, which is commonly defined as the harmonic mean of recall and precision, is a metric that accounts for both precision and recall. When the F-score is closer to 1, a better recall and precision combination is obtained. (Vafeiadis et al., 2015)

$$F - Score = \frac{2 * Precision * Recall}{Precision + Recall}$$

4. F-Score

Furthermore, there are numerous approaches to assess a method's performance in terms of classification. Accuracy is impartial towards all classes. While measurements like precision and recall distinguish

between the number of correct labels for each class, accuracy does not.

Moreover, the confusion matrix is summarized by the Matthews correlation coefficient (MCC), a single-value statistic that is similar to the F1 score. The four entries of a confusion matrix, often called an error matrix, are False Positives (FP), False Negatives (FN), True Positives (TP), and True Negatives (TN). It is easy to determine the primary advantage of utilizing MCC rather than F1 score simply by looking at their formulas:

$$MCC = \frac{TN \times TP - FP \times FN}{\sqrt{(TN+FN)(FP+TP)(TN+FP)(FN+TP)}}$$

5. Matthews Correlation

Also, the number of True Negatives is ignored by the F1 score. On the other hand, MCC provides care for each of the four confusion matrix entries.

RESULT ANALYSIS

Table 2: Evaluation Result of Deep Learning Variant

Model Name	Feature Selection	Accuracy	Loss	MCC	F1-Score
MLP	SVD	0.8923	0.0896	0.7729028948115314	0.8848725512929048
CNN	SVD	0.8750	0.0944	0.9071901917239312	0.8800893295998806
GRU	SVD	0.9892	0.0087	0.9998922471846449	0.9999461206894987

The best-performing algorithm overall is gated recurrent unit (GRU) which is seen in the three algorithms used and, in table 2 above. Generally, the best-performing metric set for the algorithms is the MCC. One of the benefits of MCC is the ease with which rules can be extracted and interpreted from a model built with it. The MCC result is therefore especially interesting for this research, as they are interested in models that they can understand and interpret easily. GRU comes up as the best algorithm. This is also true for other models used for which f-measure, recall, precision, and accuracy are the evaluation metrics to ascertain the evaluation done with MCC; GRU still outperforms other models after evaluating with state-of-the-art evaluation techniques.

Furthermore, we compare the performance of our proposed models (MLP, CNN, GRU) to the baseline model ensemble C4.5 decision tree using accuracy and F1-score evaluation metrics. From Table 2 above we deduce that GRU outperforms the other models as such will be used as our baseline for comparing with state-of-the-art and base paper model evaluation. Table 2 illustrates the tasks where our GRU model with SVD feature selection outperformed the other approaches we utilized as a baseline for this study. Based on the average performance across all projects, our GRU surpassed the ensemble C4.5 model by about 0.057. Further analysis of the findings reveals that our GRU model outperformed cutting-edge machine learning models for different datasets used in terms of F-

measure, Accuracy, and MCC since we were able to evaluate the model and get an optimal score of close to 1.

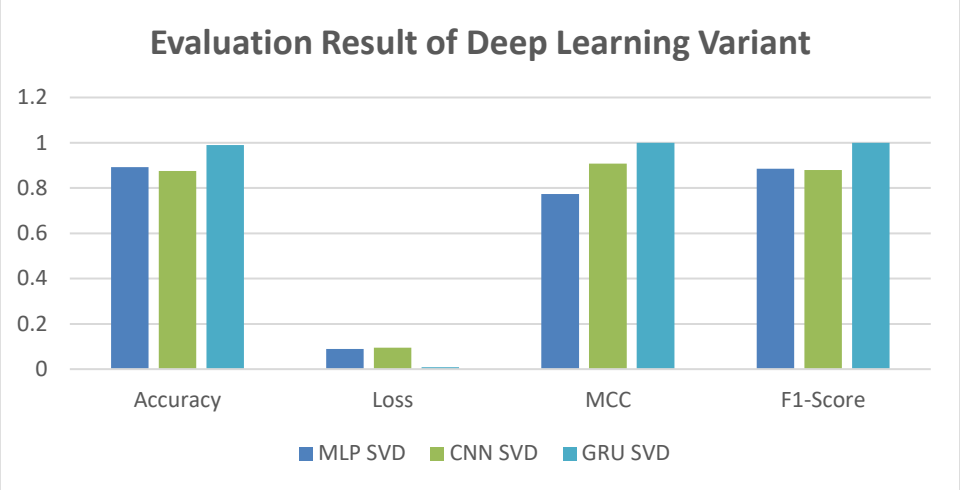

Figure 2: Model Result

More significantly, from Figure 2, it is clear that the GRU model outperforms the MLP and CNN models across all the evaluation metrics. The GRU model demonstrates the highest accuracy, lowest loss, and strongest correlation between predictions and true values (as indicated by the MCC). The consistently superior performance of the GRU model suggests that it is the most effective deep learning variant among the three presented. Also, the values of MCC, which are more accurate at quantifying a model's performance on imbalanced data, show the greatest performance disparity. These outcomes unequivocally show our model's superiority, particularly for large and unbalanced datasets. In contrast, accuracy values for various models are very high and quite similar, demonstrating accuracy's insensitivity to the problem of class imbalance. In other words, a model can attain high accuracy values by simply classifying unlabelled nodes as the majority class. These findings show conclusively that our methodology is effective in addressing label scarcity of the simulated dataset and class imbalance difficulties while fully utilizing information propagation.

CONCLUSION

The integration of the Internet of Things (IoT) with Supervisory Control and Data Acquisition (SCADA) systems has brought about significant advancements in industrial processes. However, this convergence also introduces security challenges, particularly in the form of routing attacks. As IoT continues to grow exponentially, the security of these interconnected devices becomes crucial, especially in sectors classified as critical infrastructure. The study demonstrates that all features, except the number of integrations, may be regarded as good explanatory features and that severe feature reduction does not aid in the detection of incorrect data points. It has also been demonstrated that the models perform better when

the class distribution in the dataset is balanced using oversampling approaches.

However, the study underlines the significance of feature selection and class balancing strategies in generating reliable results and highlights the promise of deep learning techniques for routing attack detections. Recent developments in artificial intelligence, including the usage of multi-layered neural networks and deep learning algorithms, have created effective methods that use learning algorithms to represent patterns in a way that captures behaviors and structural information. Applying the following will considerably progress this discipline, especially in light of recent advancements in the machine learning approaches for the security problem.

- Using transformers in modelling building.
- Continuous Monitoring and Training of datasets.
- Leveraging the trending advancement in machine learning techniques in natural language processing by leveraging retrieval augmentation generation (RAG).

REFERENCE

Alazab, A., Khraisat, A., Singh, S., Bevinakoppa, S., & Mahdi, O. A. (2023). Routing Attacks Detection in 6LoWPAN-Based Internet of Things. *Electronics*, *12*(6). https://doi.org/10.3390/electronics12061320

Choudhary, Dr. S., & Meena, G. (2022). Internet of Things: Protocols, Applications and Security Issues. *Procedia Computer Science*, *215*, 274–288. https://doi.org/https://doi.org/10.1016/j.procs.2022.12.030

Cybersecurity and Infrastructure Security Agency. (2022). *Cyber Incident Reporting Framework*.

Deng, X., Liu, Q., Deng, Y., & Mahadevan, S. (2016). An improved method to construct basic probability assignment based on the confusion matrix for classification problem. *Information Sciences*, *340*. https://doi.org/10.1016/j.ins.2016.01.033

Hussain, F., Hussain, R., Hassan, S. A., & Hossain, E. (2020). Machine Learning in IoT Security: Current Solutions and Future Challenges. *IEEE Communications Surveys & Tutorials*, *22*(3), 1686–1721. https://doi.org/10.1109/COMST.2020.2986444

Irum, A., Khan, M. A., Noor, A., & Shabir, B. (2020). *DDoS Detection and Prevention In Internet of Things*.

Janani, K., & Ramamoorthy, S. (2022). Threat analysis model to control IoT network routing attacks through deep learning approach. *Connection Science*, *34*(1), 2714–2754. https://doi.org/10.1080/09540091.2022.2149698

Li, G., Zheng, Y., Liu, J., Zhou, Z., Xu, C., Fang, X., & Yao, Q. (2021). An improved stacking ensemble learning-based sensor fault detection method for building energy systems using fault-discrimination information. *Journal of Building Engineering*, *43*, 102812.

https://doi.org/https://doi.org/10.1016/j.jobe.2021.102812

Mohamed, Y., Abdullahi, M., Alhussian, H., Alwadain, A., Aziz, N., & Jadid Abdulkadir, S. (2022). electronics Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review. *Electronics*, *11*, 1–27. https://doi.org/10.3390/electronics11020198

Raghavendra, T., Anand, M., Munuswamy, S., Thangaramya, K., Kumar Svn, S., & Arputharaj, K. (2022). An Intelligent RPL attack detection using Machine Learning-Based Intrusion Detection System for Internet of Things. *Procedia Computer Science*, *215*, 61–70. https://doi.org/10.1016/j.procs.2022.12.007

Sha, K., Wei, W., Andrew Yang, T., Wang, Z., & Shi, W. (2018). On security challenges and open issues in Internet of Things. *Future Generation Computer Systems*, *83*, 326–337. https://doi.org/https://doi.org/10.1016/j.future.2018.01.059

Silverman, D., Hu, Y.-H., & Ann Hoppa, M. (2019). *A Study on Vulnerabilities and Threats to SCADA Devices*.

Sokolova, M., & Lapalme, G. (2009). A systematic analysis of performance measures for classification tasks. *Information Processing & Management*, *45*(4), 427–437. https://doi.org/https://doi.org/10.1016/j.ipm.2009.03.002

Vafeiadis, T., Diamantaras, K. I., Sarigiannidis, G., & Chatzisavvas, K. Ch. (2015). A comparison of machine learning techniques for customer churn prediction. *Simulation Modelling Practice and Theory*, *55*, 1–9. https://doi.org/https://doi.org/10.1016/j.simpat.2015.03.003

Wegner, P. (2022). *INSIGHTS RELEASE*. www.iot-analytics.com

Zhang, C., Zhao, Y., Zhou, Y., Zhang, X., & Li, T. (2022). A real-time abnormal operation pattern detection method for building energy systems based on association rule bases. *Building Simulation*, *15*(1), 69–81. https://doi.org/10.1007/s12273-021-0791-x

Zhu, Z., Zhang, L., Liu, J., & Ying, X. (2023). IoT Security Detection Method Based on Multifeature and Multineural Network Fusion. *Security and Communication Networks*, *2023*, 2801421. https://doi.org/10.1155/2023/2801421