Advances in Artificial Intelligence and Machine Learning; Research 4 (3) 2490-2498 Received 9-06-2024; Accepted 18-08-2024; Published 25-08-2024

Enhancing IoT Security Development and Evaluation of a Predictive Machine Learning Model for Attack Detection

Atdhe Buja atdhe.buja@academyict.net
ICT Academy, Prishtina, Kosovo.

Melinda Pacolli pacollimelinda@gmail.com
ECPD, Prishtina Kosovo.

Donika Bajrami donika.bajrami@academyict.net
ICT Academy, Prishtina, Kosovo.

Philip Polstra ppolstra@commonwealthu.edu
Bloomsburg University of Pennsylvania, PA, USA.

Akihiko Mutoh mutoh@tsukijihongwanji.jp
Tsukijihongwanji, Tokyo, Japan.

Corresponding Author: Atdhe Buja

Abstract

The research aims to develop and evaluate a model for Internet of Things (IoT) attack identification utilizing IoT data from the Global Cyber Alliance's (GCA) Automated IoT Defense Ecosystem (AIDE). In the growing landscape of IoT security, the need for enhanced predictive solutions is vital. Our research leverages an enormous dataset, overall historical data from various IoT devices and network interactions, to develop a model to identify potential security threats. The key to our methodology concerns exploratory data analysis, which is focused on understanding complex patterns and anomalies in IoT data. This step is vital for feature engineering, where we meticulously select and transform data attributes to advance the model's predictive strength. The data pre-processing stage further improves the dataset, ensuring the model training and testing on high-quality, relevant data. Model development is a composite process in this research. We tried out a few machine-learning algorithms, finally selecting the one that exhibited outstanding performance in preliminary tests. The chosen model endured strict training, with a basis on balancing accuracy and validity to effectively predict IoT attacks in various scenarios. The evaluation of our model is as durable as its development. We utilized a range of metrics, including accuracy, precision, recall, and F1 score, to evaluate the model's behavior overall. The results show that our model not only attains high accuracy but also maintains a notable level of precision in predicting IoT attacks, which is crucial in minimizing false positives. In conclusion, our research contributes to the enhancement of IoT security by providing a very effective predictive model for IoT attack detection.

Citation: Atdhe Buja, et al. Enhancing IoT Security Development and Evaluation of a Predictive Machine Learning Model for Attack Detection. Advances in Artificial Intelligence and Machine Learning. 2024;4(3):145.

Keywords: IoT Security, Predictive model, Machine learning, Cybersecurity, Cyber-attacks.

1. INTRODUCTION

The rise of Internet of Things (IoT) sensors has changed industry sectors by allowing unseen scale of connectivity and automation. Still, this rise in connectivity also comes with security risks and threats. IoT sensor devices many cases have limitations in computing power and lack security integrity, and confidentiality which brought targeted cyber-attacks. As the increase of cyber-attacks continues, they have been unaffordable to protect IoT systems, and there is a need for proactive predictive models that can identify potential threats.

The research objective is to develop and evaluate a predictive Machine Learning (ML) model intended to identify IoT attacks utilizing data from the Global Cyber Alliance's Automated IoT Defense Ecosystem (AIDE) [1]. This model will benefit massive amounts of data generated by IoT devices and network communications. Our [2, 3], and other previous research have carried significant outcomes to IoT security. Agreeing to [4], assuring the security and privacy of IoT is foremost, knowing their broad adoption and the sensitivity of the data they handle. [5] highlights the need for enhanced threat detection systems able to identify and mitigate potential attacks in real-time. In the industry, organizations Global Cyber Alliance (GCA) are diligently engaged in advancing IoT security through initiatives like the AIDE platform.

This paper contributes to various vital aspects of the field of IoT security:

- Predictive model development utilizing the thorough methodology and a machine learning model to predict IoT attacks, detection patterns, and anomalies typical of security threats.
- Model performance evaluation
- Feature engineering and data preprocessing
- Inference for IoT security

Sections are organized that way, we begin a methodology defining our way to data collection, preprocessing, feature selection, and model design [6, 7]. Then, we move on to the feature selection and engineering, and [6], show the features selected for model development and evaluation of performance. Finally, we talk through the impact of our findings and provide advice for enhancing IoT security posture.

2. METHODOLOGY

The methodology engaged in this research sticks to a solid scientific basis to ensure the strength and solidity of the research findings [2, 8]. The methodology follows a comprehensive data science lifecycle and cybersecurity, as well as data preprocessing, feature selection, and engineering. Making use of the GCA Automated IoT Defense Ecosystem (AIDE) [4], dataset, the study identifies the

key features relevant to IoT security, model development, and evaluation. Feature engineering is carefully selected to advance the model's predictive accuracy. The model development and evaluation relate to the examination of several Machine Learning (ML) algorithms, and analysis from previous research work [3, 6]. Further down is an overview of the steps taken.

2.1 Data Acquisition and Preprocessing

We used actual IoT data from a running honey farm in partnership with the Global Cyber Alliance's (GCA) Automated IoT Defense Ecosystem (AIDE) [1]. This dataset contains thorough information on varied IoT devices and network relations, providing a great source of data for training and evaluating our predictive model. The AIDE dataset contained significant data (54,835,849 records) for a particular period (1st May 2023 – 31st July 2023). Each record in the dataset carries information on certain events related to IoT attacks. Python's adaptability and flexibility allow the development of custom scripts for automation and establish optimal performance and resource utilization. The data preprocessing assures the dataset's quality and suitability. We took some steps to address missing values, normalized numerical features and encoding, and data balancing. At last, the handled dataset was saved to a CSV file. By following this process, we were up to have a model design, and development to make sure the fine performance of model evaluation.

2.2 Feature Engineering

Feature engineering is a vital step where we identify and select data attributes to advance the model's predictive control. We select features based on insights gained from analysis and the composition of the dataset. This process of intricate feature selection (duration of attack, successful login indicator, geo-distance, command frequency, credentials tried, protocol encoding) to acquire the leading aspects of IoT attack actions. Custom Python scripts were created to automate the process, and along with this visualization, libraries were utilized (scikit-learn, pandas, geopy, seaborn).

3. MODEL DEVELOPMENT AND EVALUATION

In this section, we focused on straining the model design and enhancing Machine Learning (ML) and Artificial Intelligence (AI) model progress, training, testing, and evaluation processes. The model development stage considers doing tests on various machine-learning algorithms (logistic regression and random forests). The previous research work has brought to that point of having a preliminary model design [6]. The selected model was then trained and tested, focusing on balancing accuracy and universality to predict IoT attacks correctly over various scenarios.

The objective leads the research work:

- Develop a predictive ML model of Internet of Things (IoT) attack tracking and identification.

In our research, we use machine-learning algorithms, and metrics to evaluate the model's performance to gain a high grade in IoT attack successful identification.

3.1 Model Development

The model development stage in our study intends to build a well-predictive model for identifying possible IoT attacks. Random Forests (RF), Support Vector Machines (SVM), and Gradient Boosting (GB) machine learning algorithms were used to result in a broad variety which shows results in a better model. We split the dataset into training and testing sets (80/20 ratio) to ensure an upright evaluation. This separation into sets enables the model to learn from a portion of the data and to validate its performance. The model training process includes serving the training set into the ML algorithms. This model is handled by building multiple decision trees throughout training and outputting the mode of the classes for classification tasks. FIGURE 1 shows the flowchart of the model training process, including steps of data preprocessing, parameter tuning, and final model training.

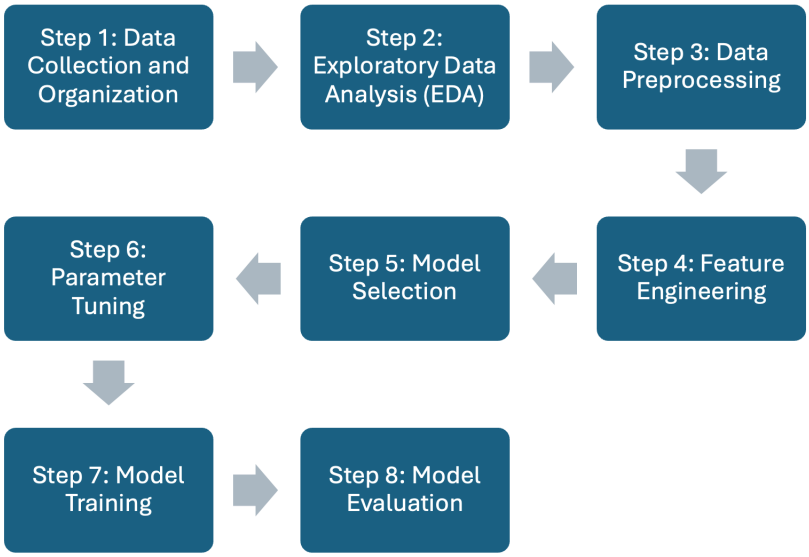

Figure 1: The model training process.

Feature importance analysis shows insights into which features supply noticeably to predictions of the model. The credentials tried (approximately 0.68) feature is the first, meaning that the number of unique credentials tried in every session is too critical in predicting IoT attacks. This hints that attackers frequently try multiple login credentials to gain unauthorized access, making this suspicious activity. The command frequency (approximately 0.25) feature is the second and represents unique commands used in every session. A often frequency of unique commands can flag tries to exploit vulnerabilities, benefiting noticeably the model's predictive strength. Duration of attack (approximately 0.06) features have a role in predicting IoT attacks. Geo-distance (approximately 0.01) shows the distance between the attacker and a target (IoT device or system). Protocol encoded (approximately 0.01) shows the protocol utilized (SSH or Telnet) in the communication, which is less critical and contributes to the model's predictions implying is not meaningful in identifying attacks. This feature importance analysis emphasizes that the model greatly depends on some features (number of credentials tried and the command count) to produce predictions.

3.2 Model Predictions and Evaluation

Following developing the mode, then we continued to the evaluation stage which assesses the model's performance through metrics to make sure for its solidity. We used various metrics (accuracy, precision, recall, f1 score, and roc auc score) to thoroughly evaluate the model. The reason we used those metrics provide us with insights on the sets of true/false results from the total number of assessed cases (accuracy); the ratio of true/false positives meaning the model's accuracy in the prediction of successful IoT attacks (precision); imitating the model's capability to identify actual attack examples (recall); the balanced mean (precision and recall), and model's strength in identifying between attack and non-attack examples (roc auc score). FIGURE 2 shows the RF model evaluation metrics (accuracy, precision, recall, f1 score, and roc auc score) with their values. The high accuracy (99.977%) and precision (99.991%) mean that the model is too effective in properly identifying IoT attacks with the slightest false positives. The fine recall (99.970%) assures that nearly all actual attacks are properly identified, minimizing the risk of unseen threats. The exceptional F1 score (99.980%) and ROC AUC score (99.979%) verify the model's experience in preserving a balance between knowing true positives and minimizing false positives, making it a precious tool for advancing IoT security. This predictive RF model can advance IoT security by providing solid real-time detection of potential attacks, allowing proactive responses. The model's top performance indicates its ability for practical implementation in IoT environments, enhancing the overall security and durability of IoT networks.

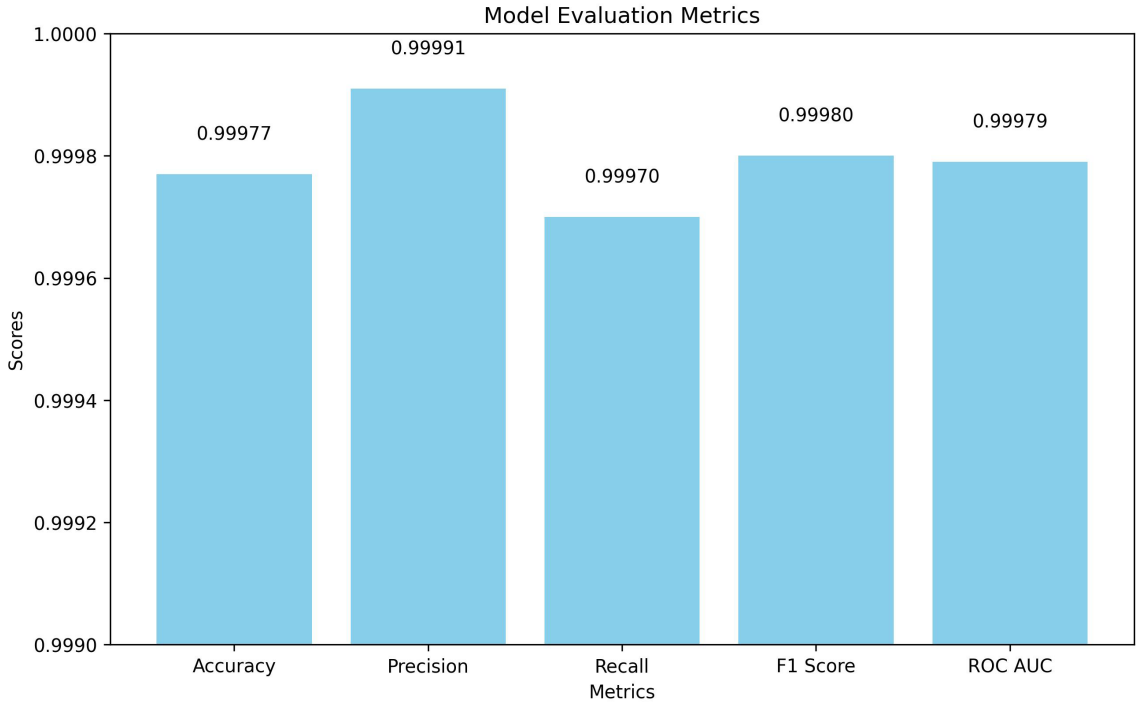

Figure 2: The RF model evaluation metrics.

Additionally, FIGURE 3 shows the confusion matrix of the distribution of True Negatives (TN), False Positives (FP), False Negatives (FN), and True Positives (TP). TN (3,288,803) represents the cases where the model properly predicted the negative class (no attack). FP (445) cases where the

model inaccurately predicted the positive class (attack) when it was negative. FN (1,390) cases where the model inaccurately predicted the negative class (no attack) when it was positive. TP (4,681,135) cases where the model properly predicted the positive class (attack).

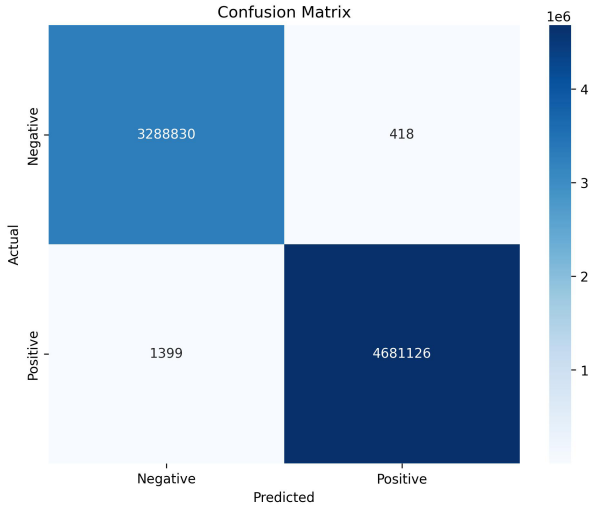

Figure 3: Confusion matrix.

The confusion matrix and metrics results mean that the model performs immensely well in predicting IoT attacks. The high metrics (accuracy, precision, recall, F1 score, and ROC AUC score) show that the model is both precise and solid. It correctly recognizes actual attacks with minimal false positives and false negatives, making it a precious tool for advancing IoT security.

Support vector machines (SVM) utilized through stochastic gradient descent (SGD) approximation, show odd performance in identifying IoT attacks. With a high accuracy (99.89%) the model displays the capability to properly classify instances in the dataset. The precision (99.88%) means that the model has a high capability to identify true positive attacks with minimal false positives. The recall (99.91%) emphasizes the model's sensitivity in detecting all actual attacks, in that way reducing the likelihood of passed-over threats. The F1 (99.89%) confirms the balanced and robust nature of the SVM model in accurately and reliably identifying IoT attacks.

The Gradient Boosting (GB) model displays even dominant performance compared to the SVM. An accuracy (99.97%) completes the classification of IoT attack instances. The model's precision (99.97%) means a low rate of false positives, which is vital for restoring high security and trust in IoT systems. The recall (99.97%) matters the model's ability to detect all real attack instances, in that way ensuring thorough threat coverage. The F1 (99.97%) imitates the model's general performance in restoring the balance between precision and recall. This dominant set of metrics exhibits that the GB model is immensely reliable and effective in predicting IoT attacks, making it a valuable tool for advancing IoT security. FIGURE 4 introduces a comparison of the performance metrics for three machine learning models (SVM, Gradient Boosting, and Random Forest). Broadly, all three models demonstrate high performance in identifying IoT attacks, the RF model just outperforms the SVM and GB models across most metrics.

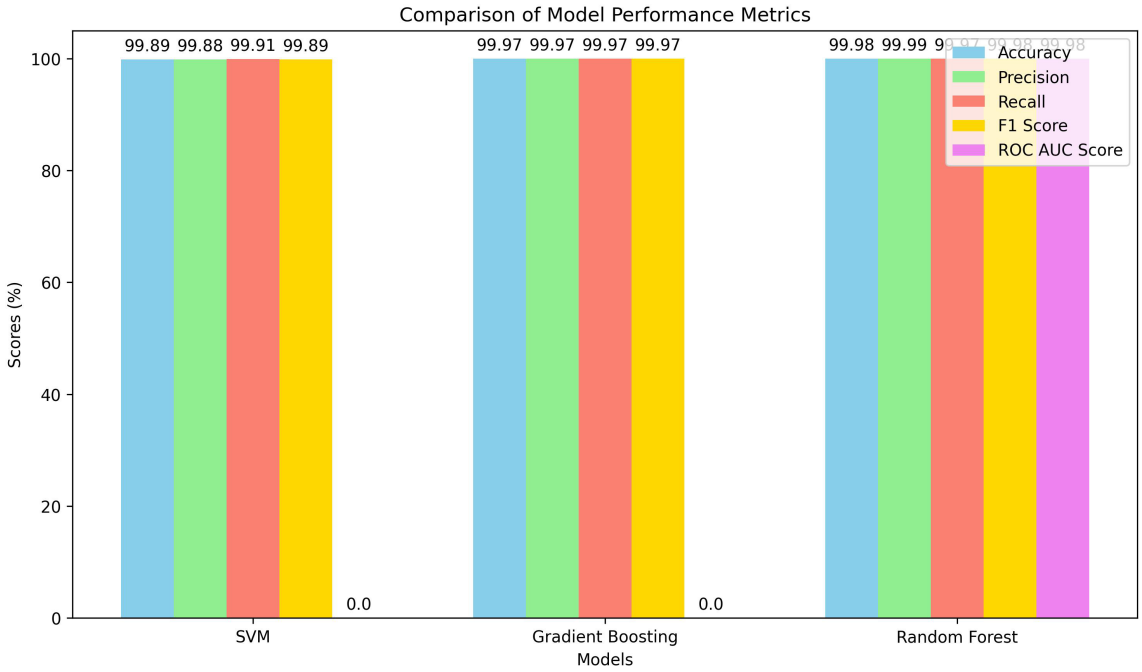

Figure 4: Comparison of model performance metrics.

4. DISCUSSION

The study engaged a comprehensive methodology to ensure the integrity and reliability of the research findings. The development and evaluation of our predictive ML model for IoT attack identification have shown valuable results, exhibiting the model's potential to advance IoT security. This section deep dive into the indications of our findings, the meaning of feature importance, and the impact on IoT security frameworks.

The dominant performance of our predictive model, as meant by metrics emphasizes the effectiveness of ML in identifying IoT attacks. These results confirm the model's ability to precisely discern between harmless and malicious activities within IoT networks. The performance metrics establish the model's solidity and precision in real-world use cases, where well-timed and precise identification of IoT attacks is critical. The confusion matrix results show that the model can correctly minimize false positives and negatives, in that way decreasing the risk of needless alerts and undetected threats. This balance is vital for preserving the integrity of IoT systems while assuring robust security.

The feature importance analysis delivers insights into which sides of the data are most characteristic of IoT attacks. The feature ('credentials_tried') appeared as the most critical, this shows that the number of unique credentials tried in a session is a warning of malicious activity (brute-force methods, trying multiple credentials to gain unauthorized access). The feature ('command_count') plays a meaningful role a high frequency of unique commands in a session can flag tries to exploit vulnerabilities. The features ('duration', and 'geo_distance') have less impact on the model, but the feature ('protocol_encoded') describing the communication protocol used (SSH or Telnet)

guides us in identifying potential attack vectors against IoT systems. Feature importance supports understanding model refining and gives guidance for Cybersecurity professionals to advance better security protocols and defenses based on the most meaningful indicators of compromise (IoCs).

The incorporation of advanced ML models in IoT security describes a meaningful step in addressing the increasing threat landscape. By leveraging historical data from the Global Cyber Alliance's Automated IoT Defense Ecosystem (AIDE), our model shows the practical implementation of ML in real-world use cases. The dominant performance and accuracy of the model indicate that it can be deployed in IoT environments, delivering a solution for threat detection.

5. CONCLUSION

This research pursues to develop and evaluate a predictive ML model efficient for proactively identifying attacks using IoT data from the Global Cyber Alliance's Automated IoT Defense Ecosystem (AIDE). Our model benefits from a thorough dataset including details on IoT device activities and network communication, leading to the identification of patterns and anomalies of potential security threats. The foremost contribution is in ways of development of a well-predictive ML model, thorough feature engineering, and productive model evaluation. Using ML algorithms (RF) we developed a predictive model that exhibits outstanding performance in identifying IoT attacks. The detailed feature analysis shows insights into feature importance ('credentials_tried' and 'command_count') for future model refinement and security protocol enhancement. The utilization of productive evaluation metrics followed by confusion matrix analysis sealed the maintained balance on the detection of threats.

The findings of this research have an impact on advancing IoT security. By having a solid and expandible solution for real-time threat detection, the ML model can be implemented in IoT environments to protect against cyber-attacks. The insights gathered from this research supply a better understanding of IoT security, through practical advice for Cybersecurity professionals in evolving to more effective countermeasures. Future research will examine directions to further advance ML model capabilities, integrating more data sources, nonstop learning, and exploring improved algorithms.

In summary, our research provides a high-performance predictive ML model for IoT attack identification, showing the practical potential of ML to advance IoT security. The model's capability to precisely identify attacks with minimal false positives and negatives makes it suitable for real-time threat detection and proactive countermeasures. As IoT devices expand, the insights and methodologies used in this research will be fundamental in enhancing IoT security and protecting critical infrastructures against cyber threats.

6. ACKNOWLEDGMENT

We would like to thank Global Cyber Alliance (GCA) https://globalcyberalliance.org/ for sharing the data with us. The ICT Academy https://www.academyict.net supported the work under the Research & Innovation Department in partnership with GCA.

References

[1] https://globalcyberalliance.org/aide/

[2] Singh R, Ujjwal RL. Feature Selection Methods for Iot Intrusion Detection System: Comparative Study. Comp Intell. 2023:227-236.

[3] Buja A, Pacolli M, Bajrami D, Polstra P, Mutoh A. Innovative Machine Learning Model Design for Predictive Iot Security Attacks. Adv Artif Intell Mach Learn;4:2394-2407.

[4] Sicari S, Rizzardi A, Grieco LA, Coen-Porisini A. Security, Privacy and Trust in Internet of Things: The Road Ahead. Computer Networks. 2015;76:146-164.

[5] Alrawais A, Alhothaily A, Hu C, Cheng X. Fog Computing for the Internet of Things: Security and Privacy Issues. IEEE Internet Comput. Mar. 2017;21:34-42.

[6] Buja A, Pacolli M, Bajrami D, Polstra P, Mutoh A. Time-Series Analysis on Aide Iot Attack Data Unraveling Trends and Patterns for Enhanced Security. J Adv Artif Intell Mach Learn;4:2233-2243.

[7] Li J, Othman MS, Chen H, Yusuf LM. Optimizing IoT Intrusion Detection System: Feature Selection Versus Feature Extraction in Machine Learning. J Big Data. 2024;11.

[8] https://research-methodology.net/research-methodology/research-types/applied-research/