IoT Intrusion Detection System for Modbus Networks with Explainable AI

Fayez Alharbi

Department or Information Technology, College of Computer and Information Sciences,
Majmaah University, Al-Majmaah, 11952, Saudi Arabia
Email: fs.alharbi@mu.edu.sa

***Abstract*—Industrial automation underwent changes through IoT technology advancements which created major security threats against widely used industrial communication protocols including Modicon Bus (Modbus). Investigating the deployment of advanced Machine Learning (ML) Models and Explainable AI (XAI) techniques represents this research's goal to enhance Intrusion Detection (ID) within IoT Modbus networks. A detailed assessment of IoT Modbus traffic included an evaluation between multiple models starting with Random Forest (RF) and including XGBoost, Gradient Boosting, AdaBoost, Logistic Regression and Support Vector Machines (SVM). RF displayed superior performance as an intrusion detection model by reaching a 98.32% accuracy level along with 98.41% precision and 98.32% recall metrics and 97.49% ROC AUC score. The strong precision rate of 93.91% together with ROC AUC value of 97.40% makes XGBoost a dependable model for use. Local Interpretable Model-agnostic Explanations (LIME) implemented increased the model's transparency by revealing the critical predictive features through decision-making explanations. The study demonstrates ensemble models bring superior results because XGBoost and RF models showed better performance than alternative models for detecting malicious activities. The system benefits from LIME integration because it delivers both transparent features explanations and clear insights about what aspects affect model predictions thus generating more system trust. Through this research IoT security boundaries advance while the study offers operational solutions to protect industrial control systems against active cyber threats in practical environments.**

***Keywords*—cybersecurity, Intrusion Detection (ID), Models and Explainable AI (XAI), Modbus protocol, data breaches**

I. Introduction

The modern system transformation through Intrusion Detection (ID) devices enables production lines to exchange information and automatically operate [1]. Modbus represents one of many widely used protocols facing critical security risks as the result of enhanced connectivity between industrial systems [2]. The network vulnerabilities create a risk of cyberattacks that result in operational disruptions and sensitive information exposure and safety-related incidents [3, 4]. Strong Intrusion Detection Systems (IDS) demand immediate implementation to detect and respond to security threats which continue to rise. The traditional IDSs approaches which primarily rely on rule-based systems and easy Machine Learning models [5−7] become less effective because of persistent changes in cyber threats [8]. Ensemble learning techniques demonstrate excellent potential for detecting complicated attack patterns through their ability to model intricate relationships and adapt to diverse datasets [8, 9]. This work presents an investigation of sophisticated Machine Learning (ML) models which optimize the identification of IoT Metbus traffic security incidents. A comprehensive IoT Modbus communication dataset has undergone proper preprocessing to yield valuable features that allow training [10] processes to proceed. A performance evaluation of Random Forest (RF), Gradient Boosting, AdaBoost, XGBoost, Logistic Regression along with Support Vector Machines (SVM) models follows. A combination of Models and XAI procedures brings Local Interpretable Model-agnostic Explanations (LIME) for understanding how decisions arise from model predictions [11]. This study delivers three important outcomes that include studying different ML models in IoT context, along with implementing XAI methods through LIME, and building a comprehensive evaluation and visualization framework for models. The integration of advanced ML methods and interpretability tools makes this study the basis for advancing IoT security knowledge and delivering operational solutions to industrial practitioners.

II. Literature Review

The increasing number of IoT devices in industrial automation requires the establishment of advanced IDS platforms for protecting enterprises from associated security threats [12, 13]. Research has investigated the use of ML methods to boost IoT network security for Modbus protocol systems. The review of current research examines ML models working together with XAI techniques when performing ID tasks on IoT Modbus networks. The first deep learning-based approach for industrial control system anomaly detection emerged in works by Kheddar *et al.* [14] and Anton *et al.* [15]. The

Manuscript received March 2, 2024; revised April 4, 2025; accepted April 15, 2025; published July 15, 2025.

authors integrated Convolutional Neural Networks (CNNs) with Long Short-Term Memory (LSTM) networks to create a system which detected irregularities in Modbus/Transmission Control Protocol (TCP) communication traffic. High detection accuracy was reported by the authors while they emphasized the limitations of interpretability found in deep learning models [15]. The application of ensemble learning techniques for IoT security was studied by Naimi and Belhi [16]. By performing a performance assessment constant XGBoost achieved better detection results than Gradient Boosting and RF for monitoring IoT network security activities. Authors presented evidence which demonstrated that ensemble approaches showed better accuracy together with robustness through RF. Illuminating these models' internal operations is crucial for trust building in the systems according to Naimi and Belhi [16]. Scientists have made XAI techniques in IoT security their main research priority. The authors of LIME [17] created a technique which provides contextual explanations about single predictions from any ML system. The interpretation model LIME facilitates the assessment of many different complex models across cybersecurity domains [17, 18]. The predictions of a RF model used for detecting intrusions in IoT networks received explanation through LIME during a study by Sarker *et al.* [19]. Through their study the authors proved that LIME successfully recognized the important factors responsible for model predictions to enhance transparency [19]. The field of intrusion detection systems received a major advancement through Khan *et al.'s* [20] creation of a hybrid IDS which combines rule-based methods with ML models. Their integrated solution united the best capabilities of both techniques to deliver accurate alerts and maintain easy interpretation. The research integrated SHapley Additive exPlanations (SHAP) to generate complete explanations showing how the model reached its forecasting decisions [21]. The application of ML-based IDS presents ongoing technical obstacles when deployed in actual IoT settings. The existing datasets face limitations since they demonstrate restricted diversity and omit comprehensive attack patterns according to Hussain *et al.* [22]. Devoted research by Hussain *et al.* [22] demonstrated the necessity to create extensive datasets which enhance the generalization capabilities of ML algorithms. The coupling of ML methods with XAI procedures has convincingly proven its strength for boosting security measures of IoT Modbus network systems. Additional research needs to tackle the important difficulties which affect model interpretability as well as dataset diversity and real-world applicability [23]. The proposed framework within this research adds to existing foundations with an ensemble learning method that combines LIME for delivering both strong detection precision and easy interpretability.

The literature demonstrates that ML combined with XAI shows promise for IoT security so researchers need to provide improved ensemble method comparisons and explainable system implementation in real-world scenarios. This research fills the identified knowledge gaps through an assessment of six ML models (RF, XGBoost, Gradient Boosting, AdaBoost, Logistic Regression, SVM) with LIME on a representative Modbus dataset while showing RF and XGBoost produce the best outcomes for industrial IoT deployment.

III. Materials and Methods

The research implements a defined systematic method to create a durable IDS which monitors Modbus communications within IoT applications. The intended outcome includes improving industrial control system security alongside visibility by merging comprehensive data preprocessing methods with multiple ML algorithms and XAI techniques. The IDS development process consists of four important phases: dataset preparation along with model development and evaluation and the final stage is resulting visualization. The framework presentation of research methodology appears in Fig. 1.

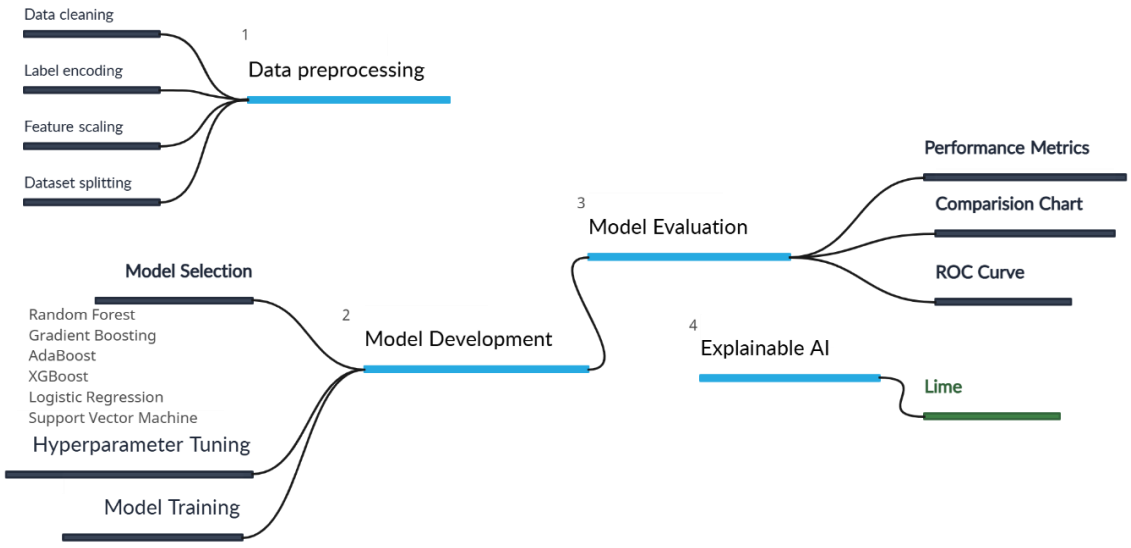

Fig. 1. Three-phase methodology: (1) Modbus data preprocessing, (2) Model development, and (3) Evaluation with XAI.

A. Dataset and Preprocessing

The research employs genuine Modbus network logs that contain recorded attacks together with standard operational traffic and documented attempts at port scanning and spoofing methods. This dataset proved optimal because it presented an accurate demonstration of real-world industrial IoT settings and demonstrated all Modbus protocols vulnerabilities while fixing the fake data flaws often found in synthetic alternatives. The data contains three primary features which consist of packet size anomalies alongside protocol sequence patterns and transaction identifier irregularities that classify events into different categories between normal traffic and attack types. Analysts excluded timestamp data collected during data acquisition since their main interest was in behavioral patterns rather than temporal data.

Feature selection established a method that integrated domain-specific knowledge with data-based verification procedures. Initial features selection originated from documented Modbus attack patterns such as the analysis of abnormal packet sizes and irregular transaction IDs which were obtained from MITRE ATT&CK ICS. Random Forest utilized Gini importance scores to measure feature importance after which it kept the variables that caused a minimum 5% decrease in impurity. The Recursive Feature Elimination (RFE) together with 5-Fold Cross-Validation (RFECV) allowed for optimizing the subset through a process which minimized redundancy and maximized detection accuracy (98.32%). The data required the following preprocessing approaches for model training together with evaluation:

- The process began with converting the categorical labels into numeric values so they could work with ML algorithms.
- StandardScaler was used to normalize feature magnitudes through feature scaling because Support Vector Machines benefit specifically from this process.
- A training subset comprised 80% of the data and the testing subset included 10% while the remaining 10% functioned as a validation subset during model evaluation.

B. Model Development

Multiple ML models were used to study their ability in detecting intrusions on IoT Modbus systems. The chosen models had proven their ability to detect complex patterns while demonstrating past success in related tasks. The following models were implemented:

- A combination of decision trees constitutes the RF model that aims to achieve better generalization and minimize overfitting.
- Gradient Boosting serves as a sequential ensemble algorithm that develops trees whenever previous iterations produce incorrect results.
- The adaptive boosting technique known as AdaBoost uses misclassified samples as its main focus for accuracy enhancement.
- XGBoost stands as an enhanced gradient boosting solution which achieves maximum computational performance when implemented.
- Logistic Regression presents itself as a linear model which provides results for binary along with multi-class classification problems.
- The SVM model represents an exceptional choice for working with high-dimensional data through its kernel-based approach.

The models received proper parameter settings through hyperparameter optimization procedures to reach their best possible performance outcomes.

The model parameters received final adjustment through GridSearchCV which implemented 5-fold cross-validation. The selected key parameters for RF were n_estimators (200) and max_depth (10) while learning_rate equaled 0.1 for XGBoost and an RBF kernel function worked best for SVM according to validation set scores.

C. Model Evaluation

The models received their performance evaluation through multiple varied metrics encompassing accuracy along with F1−Score precision and recall and ROC AUC. The selected metrics create a well-rounded evaluation system for model performance which accounts for the relationship between incorrect positive and negative results in the measurements [24]. The evaluation included confusion matrix visualization for observing different class classifications and the creation of ROC curves to detect model performance in normal and malicious activity differentiation.

D. XAI

The selection of LIME over other alternatives such as SHAP occurred because it demonstrated better efficiency for real-time industrial systems and provided localized interpretation capabilities. The local feature explanations generated by LIME are better suited for Modbus operators compared to the global information provided by SHAP. A framework integrating LIME allowed researchers to improve both the interpretability and clarity of the models during evaluation procedures. The local interpretive capability of LIME examines single predictions to reveal which features determine model predictions [25]. Transparency receives enhancement as this method reveals possible biases and weaknesses that exist within the models. The study utilizes LIME to make the decision process transparent because accessibility and understanding are essential requirements for IoT security system trust building.

E. Findings Reporting

Matplotlib and Seaborn visualized every result outcome which included performance metrics and confusion matrices and ROC curves. The research produced these precise illustrations because they helped researchers communicate their results better and document evidence effectively. This methodology provides a structured method for building IDSs specific

to IoT Modbus communications through the implementation of enhanced preprocessing with multiple ML approaches and interpretability techniques.

The following sections show experimental findings of the tested models to evaluate their performance levels according to introduction-defined objectives. The evaluation focuses on accuracy combined with F1−Score and ROC AUC metrics to demonstrate Modbus intrusion detection capabilities of each model together with LIME interpretation results.

IV. Result and Discussion

This part of the evaluation investigates the performance results of ML models through the methodology established in Section III for IoT Modbus intrusion detection. A comprehensive analysis takes place against the three objectives of this research: (1) assessing ML models' competitive value and (2) examining LIME explainability methods alongside (3) applying findings to enhance industrial IoT security. The experimental results showed how different ML systems functioned for detecting intrusions during Modbus IoT communication processes. The model that stands out as the most accurate detection system delivers 98.32% accuracy and an F1−Score of 98.27%. The model demonstrates excellent precision performance of 98.41% and recall at 98.32% while achieving 97.49% in ROC AUC which proves its ability to detect malicious traffic accurately. XGBoost produces results very similar to the top models because it shows high precision scores at 93.91% and ROC AUC results at 97.40% while maintaining robust performance characteristics. In contrast, Gradient Boosting, AdaBoost, Logistic Regression, and SVM show comparable performance, with accuracy and F1−Scores around 91.6%–91.7%. The precision values and ROC AUC of these models lag behind the results achieved by XGBoost and RF. The performance metrics from all models can be seen in Fig. 2 as a bar chart summary. The analysis demonstrates RF as the most reliable method for this application because it secures both threat detection and false alarm control effectively. XGBoost emerges as a strong backup alternative to defend against attacks. Ensemble methods effectively deal with IoT Modbus system security by combining high accuracy with reliable results according to research findings. The detailed results appear in Table I.

TABLE I. Confusion Matrix of the Developed Models

	Accuracy	F1−Score	Precision	Recall	ROC AUC
RF	0.983234	0.982721	0.984140	0.983234	0.974899
Gradient Boosting	0.916642	0.885217	0.934172	0.916642	0.933248
AdaBoost	0.916102	0.884625	0.887548	0.916102	0.929392
XGBoost	0.927715	0.909187	0.939072	0.927715	0.974008
Logistic Regression	0.916294	0.884065	0.863888	0.916294	0.924609
SVM	0.916294	0.884065	0.863888	0.916294	0.921730

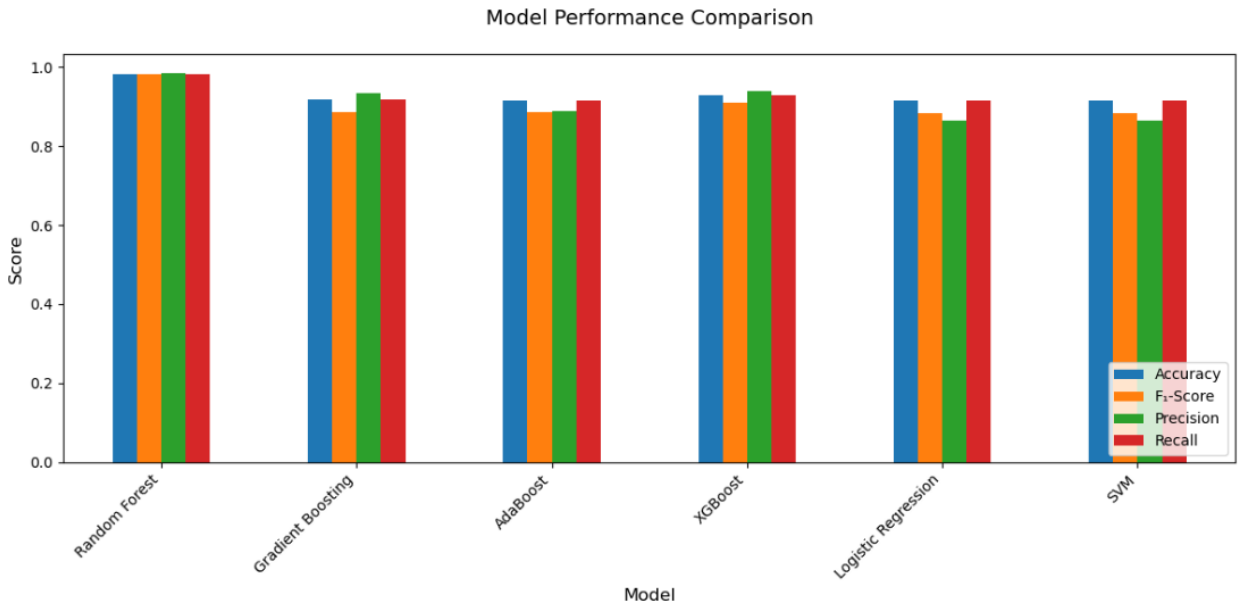

Fig. 2. Bar chart comparing the performance metrics of all models.

RF demonstrates superior intrusion detection capabilities according to the graph of ROC curve presented in Fig. 3. Single-class precision reaches perfect levels on the ROC curve for all four classes as measured by their AUC value at 1.00. The model operates at a perfect level where it produces no errors in distinguishing normal from malicious activities with both true positive rates and false positive rates for these classes in place. The model produces strong AUC scores of 0.90 and 0.96 for detecting intrusions in Class 4 and Class 5 samples. The scores record high accuracy rates even though they fall slightly below the other categories thus providing reliable detection of these particular intrusion types. The combined assessment of ROC analysis and bar chart visualization demonstrates RF's capability to handle multiple threat scenarios which occur in IoT Modbus

communications effectively. The robust model performance across various intrusion classes demonstrates its suitability as the leading solution for this task because it demonstrates strong effectiveness in practical implementations. RF maintains its superior position in the study due to ensemble voting that provides built-in resistance against noisy Modbus traffic and its modeling of non-linear feature interrelationships and its precise classification of minority classes through weighted splitting.

Through LIME results in Fig. 4 we obtain essential knowledge about RF model identification of IoT Modbus traffic patterns. The prediction probabilities analyzed through LIME reveal the model provides 5% confidence that the activity consists of backdoor password injection while other classes receive minimal probabilities below 1%. The model exhibits high conviction that the analyzed instance belongs to the non-injection activity class. LIME demonstrates the top influential features that led to the prediction decision. Three profile features named Feature_0, Feature_1 and Feature_2 are key for non-injection classification because their values demonstrate thresholds above 0.86, 0.87 respectively. The defined traffic characteristics follow standard operational patterns. The most important factor for detecting malicious activity in the injection class is Feature_4 because it carries a value of 1.86. The LIME explanations enhance both model transparency while revealing essential features behind the decision-making process. Professional practitioners who understand the most crucial model features would enhance their understanding of system behavior while detecting vulnerabilities and advancing system security [26–29]. The research effort supports the main objective of creating interpretive and trustworthy IDS systems for IoT Modbus communication security applications.

The spoofing attacks (Class 4) type exposed 8% of unclassified cases as normal traffic according to the analysis presented in Table I (Fig. 1). The detection capabilities of the model were strong with an AUC value of 0.90 (Fig. 3) yet these errors persist because benign packets share features with these attacks so the model needs improved threshold optimization or adversarial training with additional spoofing examples. Moreover, critical attacks remained undiscovered during the system operation.

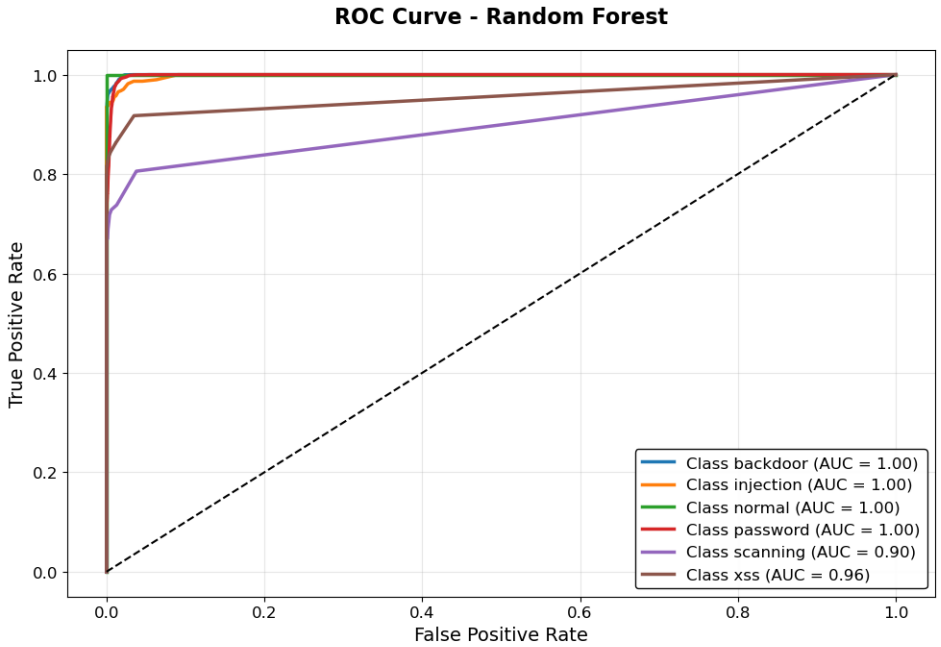

Fig. 3. The ROC curve of the top performing model (RF).

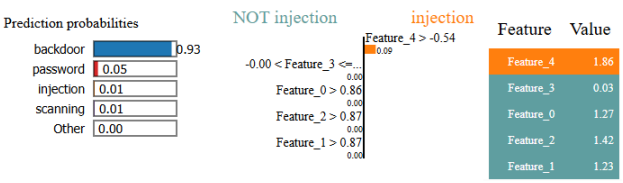

Fig. 4. Lime explanation for RF predictions.

The research results show that multiple ML algorithms prove effective for detecting intrusions across IoT Modbus communications. The performance metrics demonstrate that RF achieves the highest measurement of 98.32% for detection accuracy as well as optimal results across all evaluation metrics including precision and recall along with ROC AUC. Its near-perfect classification ability in most cases becomes evident in the ROC curve because it displays exceptional accuracy for differentiating normal from malicious traffic. XGBoost provides exceptional performance especially through its superior precision measurements and ROC AUC results which make it an effective alternative selection. The performance levels of Gradient Boosting, AdaBoost, Logistic Regression and SVM fall behind those of RF and XGBoost. The bar chart clearly presents this data by showing the performance results for comparison. RF decision-making becomes clear through LIME explanations that show which features determine its

predictive outcomes. When evaluating both models with a paired t-test performed on 500 validation sets scientists found no statistically relevant variations between RF and XGBoost ($p = 0.79$ and $p = 0.49$).

RF exceeds the performance of SVM and exhibits better explainability through LIME (Fig. 4) and Modbus traffic noise resistance which establishes it as the preferred model for industrial applications. The application of attack samples from different sources should be a focus of future research to validate these discovered trends. The clarity of the model increases because of these findings which deliver useful recommendations to enhance IoT security platforms. The study proves ensemble methodologies combined with XAI can create secure, explainable and dependable IDS systems for IoT Modbus protocols.

V. Conclusion

A new IDS system emerged from this study which solved IoT Modbus network security problems through development of an IDS with both strength and interpretability. RF outperformed multiple ML models when tested which led to its selection as the most suitable system for detecting malicious behavior because of its superior accuracy levels. The XGBoost model demonstrated high practical value because it combined effective precision and operational efficiency during testing. LIME implementation made the decision-making process of the model more understandable and actionable for practitioners to build trust in IoT security systems and pinpoint network vulnerabilities. This research confirms both ensemble models' effectiveness for IoT traffic challenges as well as the necessity of XAI to improve model visibility. The research benefits IoT security science through its contribution while delivering an operational model to defend industrial control systems from developing cyber-attacks. The application of advanced ML coupled with explainable approaches in this study establishes foundation research for secure and interpretable IDS deployment in the future. The study defines three research directions which include deploying real-time optimization methods in resource-limited IoT environments as well as testing against Modbus adversary attacks through spoofing and false data injection followed by creating hybrid architectures from our explainable ensemble systems and new sequence-based approaches represented by Modbus-NFA Behavior Distinguisher (MNBD). Project integration between MNBD's state-transition analysis and LIME's interpretability capabilities would help create faster IDS deployments for production settings.

Conflict of Interest

The author declares no conflict of interest.

Acknowledgment

The author extends the appreciation to the Deanship of Postgraduate Studies and Scientific Research at Majmaah University for funding this research work through project number R-2025-1749.

References

[1] G. Lazaridis, A. Drosou, P. Chatzimisios, and D. Tzovaras, "Unraveling the threat landscape of CPS: Modbus TCP Vulnerabilities in the Era of I4.0," in *Proc.* 2024 IEEE International Conference on Cyber Security and Resilience (CSR), 2024, vol. 8, no. 1, pp. 593–598. doi: 10.1109/CSR61664.2024.10679453

[2] Y. Sekaran, T. Debnath, T. A. Assadi *et al*., "Using machine learning to detect abnormalities on modbus/TCP networks," in *Proc. 4th Int. Conf. Inf. Manag. & Mach. Intell. (ICIMMI '22)*, 2023, vol. 8, no. 1, pp. 1–6. doi: 10.1145/3590837.359089

[3] B. K. Alotaibi, F. A. Khan, Y. Qawqzeh *et al*., "Performance and communication cost of deep neural networks in federated learning environments: An empirical study," *Int. J. Interact. Multimedia Artif. Intell.*, vol. 8, no. 1, pp. 1–10, 2024. doi: 10.9781/ijimai.2024.12.001

[4] Y. K. Qawqzeh, A. Alourani, and S. Ghwanmeh, "An improved breast cancer classification method using an enhanced adaboost classifier," *Int. J. Adv. Comput. Sci. Appl*., vol. 14, no. 1, pp. 473–478, 2023. doi: 10.14569/IJACSA.2023.0140151

[5] F. Alharbi, O. Lahcen, and J. A Ward, "Comparing sampling strategies for tackling imbalanced data in human activity recognition," *Sensors*, vol. 22, no. 4, 2022.

[6] F. Alharbi, L. Ouarbya, and J. A. Ward, "Synthetic sensor data for human activity recognition," in *Proc. 2020 International Joint Conference on Neural Networks (IJCNN)*, 2020, pp. 1−9.

[7] F. Alharbi and K. Farrahi, "A convolutional neural network for smoking activity recognition," in *Proc. 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom),* Ostrava, Czech Republic, 2018, pp. 1−6.

[8] K. K. Sabari, S. Shrivastava, and V. Sangeetha, "Anomaly-based intrusion detection Using GAN for industrial control systems," in *Proc. 2022 10th Int. Conf. Reliab., Infocom Technol. Optim. (ICRITO)*, 2022, vol. 8, no. 1, pp. 1–6. doi: 10.1109/ICRITO56286.2022.9964997

[9] T. Gueye, Y. Wang, M. Rehman *et al*., "A novel method to detect cyber-attacks in IoT/IIoT devices on the modbus protocol using deep learning," *Cluster Comput.*, vol. 26, no. 1, pp. 2947–2973, 2023. doi: 10.1007/s10586-023-04028-4

[10] M. M. Otoom, M. Jemmali, Y. Qawqzeh *et al*., "Comparative analysis of different machine learning models for estimating the population growth rate in data-limited areas," *Int. J. Comput. Sci. Netw. Secur*., vol. 19, no. 12, pp. 96–101, 2019.

[11] S. Gyawali, J. Huang, and Y. Jiang, "Leveraging explainable AI for actionable insights in IoT intrusion detection," in P*roc. 2024 19th Annu. Syst. Syst. Eng. Conf. (SoSE)*, 2024, vol. 8, no. 1, pp. 92–97. doi: 10.1109/SOSE62659.2024.10620966

[12] A. Abusitta, G. H. S. Carvalho, O. Abdel Wahab *et al*., "Deep learning-enabled anomaly detection for IoT systems," *Internet Things*, vol. 21, no. 1, pp. 1–10, 2023. doi: 10.2139/ssrn.4258930

[13] Y. K. Qawqzeh, M. B. Reaz, M. M. Ali, and K. B. Gan, "Assessment of atherosclerosis in erectile dysfunction subjects using second derivative of photoplethysmogram," *Sci. Res. Essays*, vol. 7, no. 1, pp. 1–10, 2012.

[14] H. Kheddar, Y. Himeur, and A. I. Awad, "Deep transfer learning for intrusion detection in industrial control networks: A comprehensive review," *J. Netw. Comput. Appl*., vol. 220, no. 1, pp. 1–10, 2023. doi: 10.1016/j.jnca.2023.103760

[15] S. D. Anton, S. Sinha, and H. Schotten, "Anomaly-based intrusion detection in industrial data with SVM and random forests," in *Proc. 27th Int. Conf. Softw., Telecommun. Comput. Netw. (SoftCOM)*, 2019, vol. 8, no. 1, pp. 1–10. doi: 10.23919/SOFTCOM.2019.8903672

[16] M. M. A. Naimi and A. Belhi, "Deep learning-based anomaly detection in industrial control system network traffic," *Smart Innov., Syst. Technol*., vol. 404, no. 1, pp. 1–10, 2024. doi: 10.1007/978-981-97-5810-4_11

[17] M. Ribeiro, S. Singh, and C. Guestrin, "Why should I trust you?: Explaining the predictions of any classifier," in *Proc. 2016 Conf.*

North Am. Chapter Assoc. Comput. Linguist.: Demonstrations, 2016, vol. 8, no. 1, pp. 97–101. doi: 10.1145/2939672.2939778

[18] Y. K. Qawqzeh, "Neural network-based diabetic type II high-risk prediction using photoplethysmogram waveform analysis," *Int. J. Adv. Comput. Sci. Appl*., vol. 10, no. 12, pp. 1–10, 2019. doi: 10.14569/IJACSA.2019.0101212

[19] I. H. Sarker, A. S. M. Kayes, S. Badsha *et al*., "Cybersecurity data science: An overview from machine learning perspective," *J. Big Data*, vol. 7, no. 1, pp. 1–20, 2020. doi: 10.1186/s40537-020-00318-5

[20] N. W. Khan, M. S. Alshehri, M. A. Khan *et al*., "A hybrid deep learning-based intrusion detection system for IoT networks," *Math. Biosci. Eng.*, vol. 20, no. 8, pp. 13491–13520, 2023. doi: 10.3934/mbe.2023602

[21] Y. K. Qawqzeh, A. M. A. Mohd, M. Reaz, and O. Maskon, "Photoplethysmography analysis of artery properties in patients presenting with established erectile dysfunction," in *Proc. Int. Conf. Comput. Sci. Netw. Technol*., 2010, vol. 8, no. 1, pp. 165–168. doi: 10.1109/ICECTECH.2010.5480006

[22] F. Hussain, S. G. Abbas, G. A. Shah, and I. M. Pires, "A comprehensive survey on machine learning-based intrusion detection systems for IoT networks," *Sensors*, vol. 21, no. 16, pp. 1–20, 2021. doi: 10.1155/2023/8981988

[23] V. Holubenko, D. Gaspar, R. Leal et al., "Autonomous intrusion detection for IoT: A decentralized and privacy-preserving approach," *Int. J. Inf. Secur*., vol. 24, no. 7, pp. 1–10, 2025. doi: 10.1007/s10207-024-00926-9

[24] M. Almatari *et al.*, "cardiovascular disease risk factors prediction using deep learning convolutional neural networks," *Int. J. Electr. Comput. Eng*., vol. 14, no. 4, pp. 4471–4487, 2024.

[25] B. Sharma, L. Sharma, C. Lal, and S. Roy, "Explainable artificial intelligence for intrusion detection in IoT networks: A deep learning-based approach," *Expert Syst. Appl.*, vol. 238, no. 1, 2024. doi: 10.1016/j.eswa.2023.121751

[26] F. R. Mughal, J. He, B. Das *et al*., "Adaptive federated learning for resource-constrained IoT devices through edge intelligence and multi-edge clustering," *Sci. Rep*., vol. 14, p. 28746, 2024. doi: 10.1038/s41598-024-78239-z

[27] A. Rahman, G. Mustafa, A. Q. Khan, M. Abid, and M. H. Durad, "Launch of denial-of-service attacks on the modbus/TCP protocol and development of its protection mechanisms," *Int. J. Crit. Infrastruct. Prot*., vol. 39, p. 100568, 2022. doi: 10.1016/j.ijcip.2022.100568

[28] A. E. Alrashdi, B. A. S. A. Rimy, and S. E. Sappagh, "Strengthening ICS defense: Modbus-NFA behavior model for enhanced anomaly detection," *J. Inf. Secur. Appl*., vol. 89, 103990, 2025.

[29] F. Katulic, D. Sumina, I. Erceg and S. Gros, "Enhancing modbus/TCP-based industrial automation and control systems cybersecurity using a misuse-based intrusion detection system," in *Proc. 022 International Symposium on Power Electronics, Electrical Drives, Automation and Motion (SPEEDAM)*, Sorrento, Italy, 2022, pp. 964−969. doi: 10.1109/SPEEDAM53979.2022.9842239