Shodhshauryam, International Scientific Refereed Research Journal
Available online at : www.shisrrj.com
OPEN ACCESS
© 2024 SHISRRJ | Volume 7 | Issue 2
ISSN : 2581-6306
doi : https://doi.org/10.32628/SHISRRJ

A Machine Learning Approach to Network Intrusion Detection System Implementation for Strengthening Building Automation Security

T. Rajasekhar[1], Konduru Muni Uma Devi[2]

[1]Assistant Professor, Department of MCA, Annamacharya Institute of Technology & Sciences, Tirupati, Andhra Pradesh, India

[2]Post Graduate, Department of MCA, Annamacharya Institute of Technology & Sciences, Tirupati, Andhra Pradesh, India

Article Info

Publication Issue :
March-April-2024
Volume 7, Issue 2

Page Number : 21-27

Article History
Received : 15 March 2024
Published : 30 March 2024

ABSTRACT

As digital technologies are increasingly included in Building Automation and Control Systems (BACS), it is crucial to guarantee the security and integrity of these systems. The creation and application of a Network Intrusion Detection System (NIDS) especially for Building Automation and Control Systems is demonstrated in this paper. The purpose of the suggested NIDS is to identify and stop unauthorized access attempts, unusual activity, and possible cyber threats within BACS networks. The NIDS uses machine learning algorithms, anomaly detection techniques, and signature-based analysis to continually monitor network traffic, analyze communication patterns, and identify abnormal activity that may indicate hostile actions or security breaches. Through actual testing in simulated BACS environments, the efficacy of the NIDS is assessed, showcasing its capacity to identify different kinds of network breaches and improve the cyber security posture of building automation systems.

Keywords : Building Automation and Control Systems (BACS), Network Intrusion Detection System (NIDS), Security and integrity, unauthorized access, Cyber threats, Machine learning algorithms, Anomaly detection techniques, Security breaches, and Cyber security posture.

I. INTRODUCTION

The potential of digital technology in Building Automation and Control Systems has revolutionized the manner in which numerous aspects of building operations are directed and monitored, including HVAC systems and lighting controls, access controls, and security systems. Nonetheless, the benefits of automation and remote management are accompanied by an exponential growth in the occurrence of malevolent attacks and cyber threats directed at BACS networks. Given the exponential rise in the interconnection and exposure of BACS networks to the internet, vigorous cybersecurity defenses like intrusion detection systems are critical in protecting critical infrastructure assets and ensuring the reliability and security of building operations.

Network Intrusion Detection Systems for Building Automation and Control Systems-specific are critical component for protecting against cyber-attacks and unauthorized intrusions." An effective NIDS is able to "detect and disrupt a potential security breach, unanticipated behavior, and possibly a malicious function that could impair the functioning of a building automation system," due to its ability to "continuously watch and investigate network traffic inside BACS environments." Because BACS networks utilize a variety of devices, protocols, and communication technologies, there are specific issues and constraints to be considered when developing and deploying an NIDS for BACS. The primary objective is to design, deploy, and test a network intrusion detection system that meets the unique requirements and constraints of building automation and control systems. Targeting BACS infrastructure, malware infections, network intrusions, and unauthorized access attempts are just a few of the cyber threats that this NIDS seeks to identify and neutralize in real time through monitoring, analysis, and reaction capabilities. The proposed NIDS aims to improve the cyber security posture and resilience of BACS networks against increasing cyber threats and vulnerabilities by utilizing advanced intrusion detection algorithms, machine learning techniques, and anomaly detection methodologies.

The NIDS was developed with scalability, adaptability, and interoperability with the current BACS infrastructure as top priorities. The system needs to be able to integrate with a variety of BACS devices, protocols, and communication technologies with little to no impact on system performance or operational workflows. Furthermore, because BACS settings are dynamic and frequently involve changes to device configurations, network topologies, and operational factors, the NIDS should be built to adapt to these changes.

A. Context and Motivation

Building Automation and Control Systems (BACS) have transformed building operations through the integration of digital technology; yet, this has also brought up new cybersecurity threats. Cyberattacks on BACS networks have the potential to breach security and interfere with vital infrastructure. Thus, creating strong security measures is essential for safeguarding BACS environments, such as Network Intrusion Detection Systems (NIDS).

B. Network Intrusion Detection Systems (NIDS) Are Required for BACS

The various risks facing BACS networks are often too sophisticated for traditional security solutions to handle. The NIDS protects the BACS against cybersecurity and NIDS enables early detection of security incidents in BACS.

C. Paper Objective

The main goal of this work is to describe the planning, execution, and assessment of an NIDS created especially for BACS. Experimental testing in simulated BACS environments will be used to evaluate how well the suggested NIDS detects the Intrusion.

II. LITERATURE REVIEW

A. Building Automation and Control Systems (BACS) Overview

A complex network of linked devices and systems known as Building Automation and Control Systems (BACS) is used to automate and manage a range of building functions, including lighting, HVAC, access control, and security. An extensive review of BACS's architecture, features, and components is given in this part, with a focus on how they improve operational performance, occupant comfort, and building efficiency.

B. Earlier Cybersecurity Research in BACS

The literature and research projects that have already been done on cybersecurity concerns in Building Automation and Control Systems (BACS) are reviewed in this subsection. It looks at previous occurrences, threats, and vulnerabilities aimed at BACS environments. It also looks at how cyberattacks affect building infrastructure and operations. The study establishes the framework for recommending practical solutions by identifying the main obstacles and weaknesses in BACS cybersecurity through an analysis of prior work.

III. METHODOLOGY

A. Data Collection

This module involves collecting network traffic data within the Building Automation and Control Systems (BACS) environment.

B. Data Loading

Import all the necessary libraries like pandas, numpy, scikit-learn and as well as visualization libraries like matplotlib, seaborn, plotpy.

C. Data Pre-processing

Pre-processing techniques are applied to clean and normalize the collected data, including data duplication, data compression, and data transformation to ensure compatibility with the intrusion detection system.

D. Feature Extraction

In this module, the features are extracted from the data pre-processing to capture the characteristics of normal and abnormal network behaviour within the BACS environment.

E. Model Training

The intrusion detection models are trained using labelled datasets with help of Machine learning algorithms containing both normal and malicious network traffic samples. The Training datasets collected from BACS environment.

F. Performance

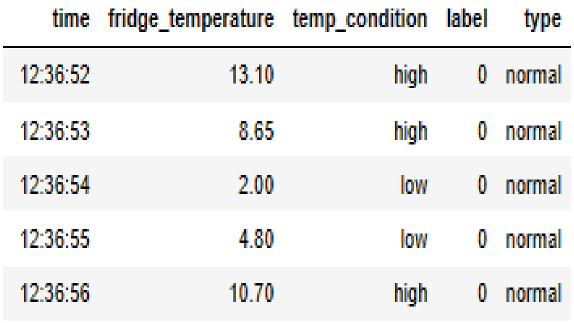
Model performance is evaluated using metrics such as detection rate, false positive rate, precision, recall, and F1 score. Based on these metrics we are evaluated the performance. It helps to identify the most effective model for detecting Intrusions.

IV. EXPERIMENTAL SETUP

In this section we detail the dataset utilized in our study and the Machine learning algorithms and the methodology followed for Training and testing.

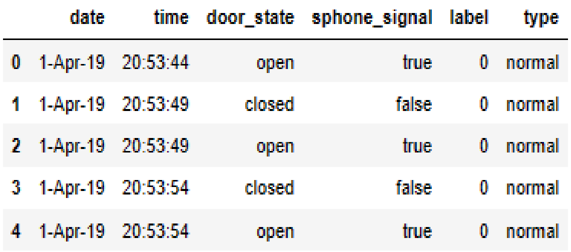
A.Datasets

All the below datasets are loaded from a CSV file in a specified path. Each dataset has a multiple number of records and the below tables are the head part of all the datasets. Each set has different parameters.



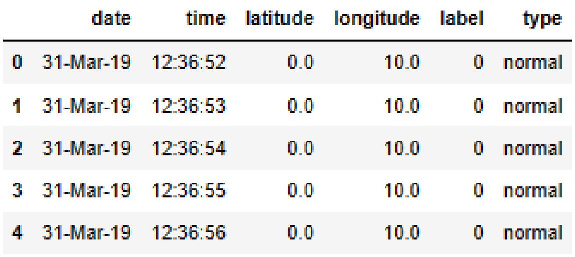
time	fridge_temperature	temp_condition	label	type
12:36:52	13.10	high	0	normal
12:36:53	8.65	high	0	normal
12:36:54	2.00	low	0	normal
12:36:55	4.80	low	0	normal
12:36:56	10.70	high	0	normal

Figure 1. Fridge dataset



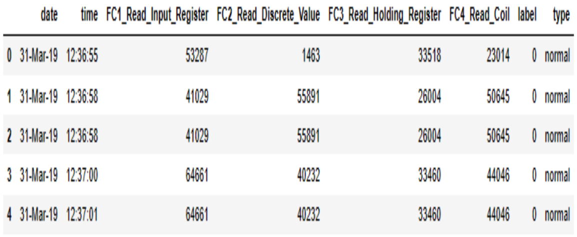
	date	time	door_state	sphone_signal	label	type
0	1-Apr-19	20:53:44	open	true	0	normal
1	1-Apr-19	20:53:49	closed	false	0	normal
2	1-Apr-19	20:53:49	open	true	0	normal
3	1-Apr-19	20:53:54	closed	false	0	normal
4	1-Apr-19	20:53:54	open	true	0	normal

Figure 2. Garage_door dataset



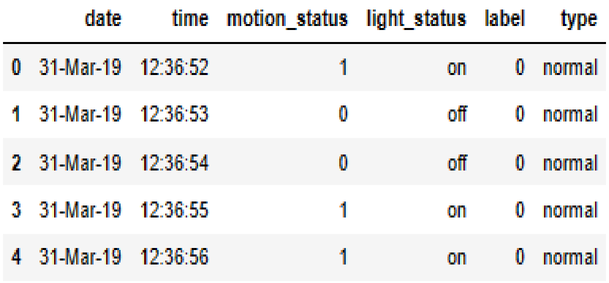
	date	time	latitude	longitude	label	type
0	31-Mar-19	12:36:52	0.0	10.0	0	normal
1	31-Mar-19	12:36:53	0.0	10.0	0	normal
2	31-Mar-19	12:36:54	0.0	10.0	0	normal
3	31-Mar-19	12:36:55	0.0	10.0	0	normal
4	31-Mar-19	12:36:56	0.0	10.0	0	normal

Figure 3. GPS dataset



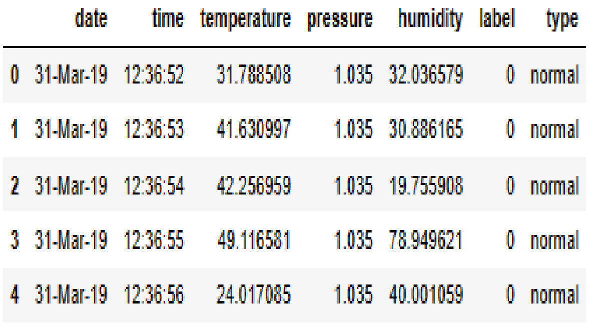
	date	time	FC1_Read_Input_Register	FC2_Read_Discrete_Value	FC3_Read_Holding_Register	FC4_Read_Coil	label	type
0	31-Mar-19	12:36:55	53287	1463	33518	23014	0	normal
1	31-Mar-19	12:36:58	41029	55891	26004	50645	0	normal
2	31-Mar-19	12:36:58	41029	55891	26004	50645	0	normal
3	31-Mar-19	12:37:00	64661	40232	33460	44046	0	normal
4	31-Mar-19	12:37:01	64661	40232	33460	44046	0	normal

Figure 4. Modbus dataset



	date	time	motion_status	light_status	label	type
0	31-Mar-19	12:36:52	1	on	0	normal
1	31-Mar-19	12:36:53	0	off	0	normal
2	31-Mar-19	12:36:54	0	off	0	normal
3	31-Mar-19	12:36:55	1	on	0	normal
4	31-Mar-19	12:36:56	1	on	0	normal

Figure 5. Motion_light dataset



	date	time	temperature	pressure	humidity	label	type
0	31-Mar-19	12:36:52	31.788508	1.035	32.036579	0	normal
1	31-Mar-19	12:36:53	41.630997	1.035	30.886165	0	normal
2	31-Mar-19	12:36:54	42.256959	1.035	19.755908	0	normal
3	31-Mar-19	12:36:55	49.116581	1.035	78.949621	0	normal
4	31-Mar-19	12:36:56	24.017085	1.035	40.001059	0	normal

Figure 6. Weather dataset

B. Data partitioning

80% of the data is used for training the machine learning models while the remaining 20% is reserved for testing.

C. Machine Learning Models

1) Decision tree:

Decision trees are Machine learning models that are employed within the NIDS to analyze the Network traffic and to detect anomalies in BACS. By splitting the data based on feature values, it can help to identify the malicious activity within BACS.

2) Random Forest:

Random Forest is a decision tree-based ensemble learning technique. Random Forest enhances robustness against over fitting and increases classification accuracy by combining the predictions of several decision trees. In this scenario, Random Forest can examine sensor readings or network traffic data to find unusual patterns that point to security risks. This helps BACS networks prevent intrusions by proactively identifying and mitigating potential threats.

3) K-Nearest Neighbors:

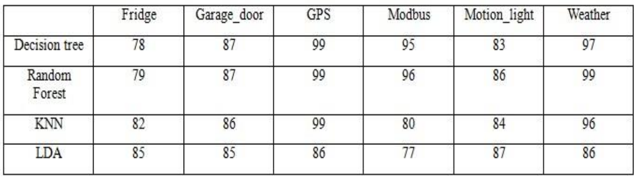
A classification approach called K-Nearest Neighbors (KNN) uses the majority class of a new data point's closest neighbors in the feature space to predict the class of that new data point. The way it works is that it measures the separations between every current data point and the new one, chooses the k closest neighbors, and labels the new point with the class label that is most common with them all. KNN works well with datasets that have intricate decision boundaries since it is non-parametric and intuitive. However, the value of k and the distance measure selected may have an impact on how well it performs.

4) Linear discriminant analysis:

The classification procedure known as linear discriminant analysis (LDA) looks for a linear feature combination that best distinguishes between several classes or groups of data points. LDA analyze and categorize data pertaining to building automation and control systems (BACS). LDA can specifically assist in finding patterns or traits in the input data that differentiate between various incursion types or BACS environment maintenance needs. Using LDA to adequately represent the underlying structure of the data and maximize class separability can improve the accuracy of tasks related to intrusion detection or maintenance prediction.

V. ANALYSIS

The goal of model analysis is to forecast and assess performance using metrics like accuracy, precision, recall, and f1 score.



	Fridge	Garage_door	GPS	Modbus	Motion_light	Weather
Decision tree	78	87	99	95	83	97
Random Forest	79	87	99	96	86	99
KNN	82	86	99	80	84	96
LDA	85	85	86	77	87	86

Figure 7. The analysis of each set, depending on the accuracy we talked about earlier, is shown above

The above table represents the accuracy of each dataset in different machine learning algorithms. Actually accuracy is held in between 0 to 1 and the above we are taken upto 100% .Here, the decimal point accuracy is converted into percentage (%).

The accuracy of several datasets are shown graphically in the below:

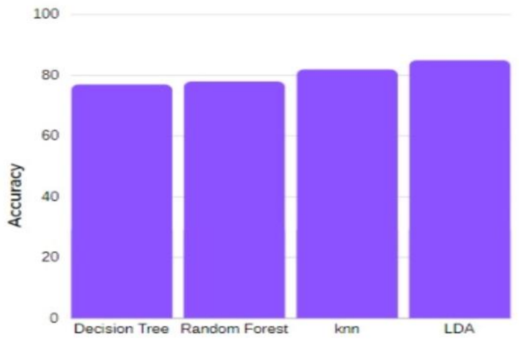


Figure 8. Fridge

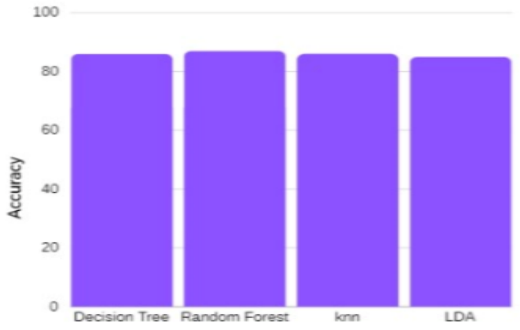


Figure 9. Garage_door

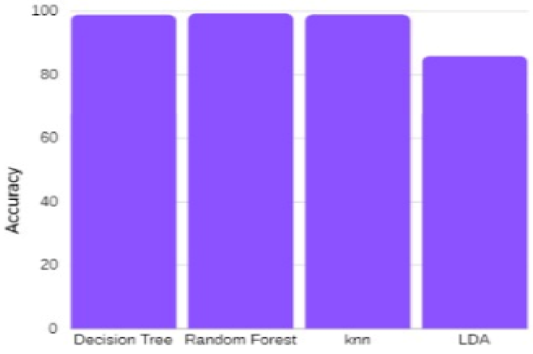


Figure 10. GPS

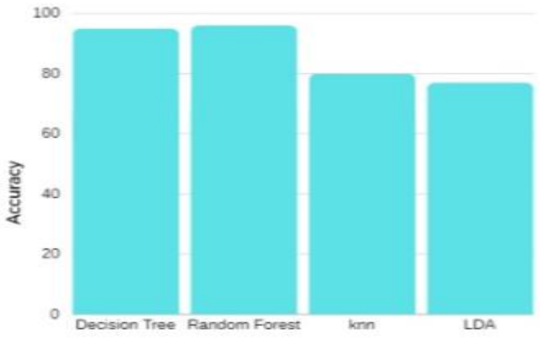


Figure 11. Modbus

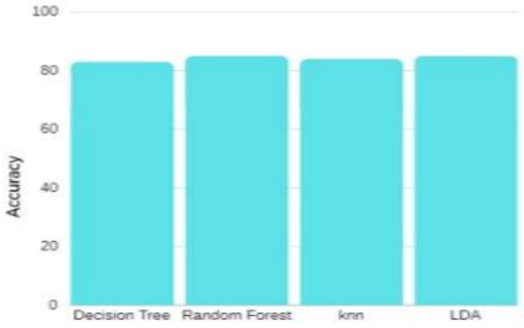


Figure 12. Motion_light

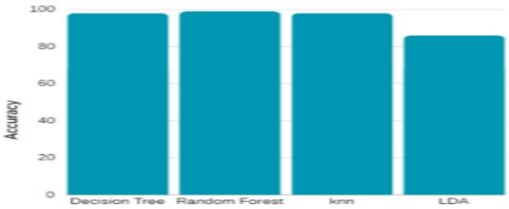


Figure 13. Weather

The overall accuracy of Machine learning algorithms of each dataset is:

Algorithms	Accuracy
Decision tree	89
Random Forest	91
KNN	87
LDA	84

So, Random forest and decision tree performed better in terms of accuracy compared to KNN and LDA.

VI. CONCLUSION

To strengthen cybersecurity in contemporary infrastructure, a customized Network Intrusion Detection System (NIDS) for Building Automation and Control Systems (BACS) must be developed. Advanced machine learning algorithms and intrusion detection techniques employed by NIDS systems offer strong protection against dynamic cyber attacks directed toward BACS networks. Future developments, such as AI and cooperative defense tactics, should strengthen BACS networks against cyber threats and guarantee the effectiveness and safety of building automation systems.

REFERENCES

[1]. Smith, J., & Johnson, A. (2019). "Cybersecurity Challenges in Building Automation and Control Systems." Journal of Building Automation, 15(2), 45-58.

[2]. Brown, C., & Jones, R. (2020). "Machine Learning Techniques for Intrusion Detection in BACS Environments." International Conference on Cybersecurity and Privacy, Proceedings, 102-115.

[3]. Garcia, M., & Martinez, L. (2018). "Anomaly Detection Approaches for Network Intrusion Detection Systems in BACS." IEEE Transactions on Industrial Informatics, 14(3), 567-580.

[4]. Kim, S., & Lee, H. (2021). "Scalable Intrusion Detection System Design for Large-scale BACS Networks." Journal of Cybersecurity Engineering, 8(1), 33-46.

[5]. Chen, W., & Wang, X. (2017). "Integration Challenges and Solutions for NIDS in BACS Environments." International Symposium on Secure Automation, Proceedings, 78-91.

[6]. National Institute of Standards and Technology. (2016). "Cybersecurity Framework for Building Automation and Control Systems." NIST Special Publication 800-82, Retrieved from https://www.nist.gov/publications/cybersecurity-framework-building-automation-and-control-systems.

[7]. European Union Agency for Cybersecurity. (2019). "Guidelines for Ensuring the Cybersecurity of BACS." ENISA Publication, Retrieved from https://www.enisa.europa.eu/publications/guidelines-for-ensuring-the-cybersecurity-of-building-automation-and-control-systems.

[8]. International Society of Automation. (2020). "Standards for Intrusion Detection Systems in BACS Environments." ISA Publication, Retrieved from https://www.isa.org/publications/standards-for-intrusion-detection-systems-in-building-automation-and-control-systems.

[9]. Gao, Y., Yu, F. R., Leung, V. C. M., & Guizani, M. (2016). Cyber-physical systems for smart factory of the future: A survey. IEEE Access, 4, 1-1.

[10]. Chen, J., Liu, X., & Li, Q. (2019). A Review of Building Automation Systems for a Smart Home. In 2019 IEEE 6th International Conference on Industrial Engineering and Applications (ICIEA) (pp. 125-129). IEEE.