IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 9, September 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.524

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 9, September 2024

|DOI: 10.15680/IJIRSET.2024.1309048|

A Machine Learning based Cyber Attack Detection Model for Wireless Sensor Network in Microgrids

Ravikumar S, Narasimha Murthy M R

Post-Graduation Student, Department of Master of Computer Applications, Vidya Vikas Institute of Engineering & Technology, Mysuru, Karnataka, India

Assistant Professor, Department of Master of Computer Applications, Vidya Vikas Institute of Engineering & Technology, Mysuru, Karnataka, India

ABSTRACT: Modern microgrids rely heavily on wireless sensor networks (WSNs) for real-time infrastructure monitoring and control. However, they are open to several types of cyberattacks because of their dispersed structure and the sensitive data they manage. The goal of this study is to improve the security of WSNs in microgrids by presenting a complete machine learning (ML)-based cyber attack detection methodology. We investigate several machine learning approaches, such as supervised, unsupervised, and deep learning techniques, for identifying various cyberthreats. The model's success is measured using the following metrics: accuracy, precision, recall, real-time performance, and scalability. The findings show that deep learning models offer greater accuracy and flexibility, whereas machine learning-based methods provide strong detection skills. In addition, we talk about the difficulties faced and suggest future lines of inquiry for resolving these problems.

KEYWORDS:Machine Learning, Cyber Attack Detection, Wireless Sensor Networks, Microgrids, Anomaly Detection, Deep Learning, Real-Time Monitoring, Security.

I. INTRODUCTION

BACKGROUND

Microgrids employ wireless sensor networks (WSNs) extensively to track and manage several elements of energy delivery and consumption. These networks are necessary for effective microgrid management because they gather and transfer vital data. But since they are dispersed and open, they are vulnerable to a variety of cyberthreats, such as data injection, denial of service (DoS) assaults, and eavesdropping. Maintaining the integrity and dependability of microgrid operations depends on the security of these networks..

OBJECTIVE

Creating a machine learning-based model to identify cyberattacks in WSNs inside microgrids is the aim of this research. Our objectives are to investigate and contrast different machine learning approaches, evaluate their effectiveness in practical situations, and pinpoint issues and future directions.

II. LITERATURE SURVEY SUMMARY

The literature on machine learning (ML)-based cyber attack detection for wireless sensor networks (WSNs) in microgrids highlights significant progress and ongoing challenges in this field. Researchers have explored various ML techniques to enhance cybersecurity in WSNs, crucial for microgrid operations. Supervised learning methods like Support Vector Machines (SVM) and Random Forests are commonly used for classifying known attack patterns, while unsupervised learning approaches, such as K-means clustering and Isolation Forests, detect anomalies without requiring labeled data. Deep learning models, including Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), are also employed for their advanced pattern recognition capabilities.Key challenges include selecting relevant features from sensor data, ensuring real-time detection capabilities, and addressing scalability issues for large-scale networks. The integration of ML models into existing microgrid infrastructure must balance accuracy with

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 9, September 2024

|DOI: 10.15680/IJIRSET.2024.1309048|

computational efficiency to avoid imposing excessive resource demands. Recent advancements focus on hybrid models that combine different ML approaches to improve adaptability and performance. However, issues such as handling imbalanced datasets, reducing false positives, and adapting to evolving attack vectors remain critical areas for future research. Overall, while ML offers promising solutions for cyber attack detection, ongoing development is needed to address practical deployment challenges effectively.

III. RELATED WORK

1. **Cyber Attack Detection in WSNs**: Recent studies have highlighted various approaches to enhancing the security of WSNs using machine learning. Liu et al. (2019) investigated supervised learning models such as Support Vector Machines (SVM) and Decision Trees, achieving high accuracy for known attack patterns. Similarly, Sadiq et al. (2020) evaluated Random Forests and Gradient Boosting, focusing on handling imbalanced datasets.

2. **Unsupervised and Deep Learning Approaches**: Unsupervised learning techniques, including K-means clustering and Isolation Forests, have been explored by Ahmed et al. (2018) and Yadav et al. (2021). These methods are useful for detecting novel attack patterns. Deep learning models, such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), have been studied by Alzahrani et al. (2021) and Zhang et al. (2022), offering improved accuracy and adaptability in complex environments.

3. **Feature Selection and Real-Time Processing**: Feature selection and data preprocessing play a crucial role in the effectiveness of ML models. Bashir et al. (2020) highlighted how crucial it is to identify pertinent features and normalize data. Real-time detection and scalability challenges were addressed by Khan et al. (2021) and Jiang et al. (2023), focusing on optimizing model performance and adapting to varying network conditions.

IV. METHODOLOGY

Data Collection and Preprocessing: We collected data from simulated WSN environments, including normal and attack scenarios. Data preprocessing involved normalization, feature extraction, and handling class imbalances using techniques like SMOTE.

Model Development:Three main types of ML models were developed:
- **Supervised Learning**: Support Vector Machines (SVM), Random Forests, and Gradient Boosting.
- **Unsupervised Learning**: K-means clustering and Isolation Forests.

Evaluation Metrics: The models were evaluated based on accuracy, precision, recall, F1-score, and real-time processing capability. We also assessed scalability by testing model performance across different network sizes.

V. RESULT AND DISCUSSION

1. Model Performance: The supervised learning models, notably Random Forests, achieved a high accuracy of 94% with a precision of 92% and a recall of 93%, proving effective for known attack patterns. Support Vector Machines (SVMs) offered similar performance but required extensive labeled data. Among unsupervised learning models, Isolation Forests detected novel attacks with an 87% detection rate and low false positives, while K-means clustering effectively identified anomalies but struggled with distinguishing attack types. Deep learning models excelled, with Convolutional Neural Networks (CNNs) reaching 96% accuracy and an F1-score of 95%, and Recurrent Neural Networks (RNNs) performing well in capturing temporal attack behaviors.
2. Real-Time Detection:Deep learning models, particularly CNNs, demonstrated the best real-time performance with minimal latency. Supervised models also performed well but required optimization for real-time data processing.
3. Effectiveness of ML Approaches: Machine learning techniques proved effective in detecting cyber attacks in WSNs for microgrids. Supervised models are strong in environments with known attack patterns, while unsupervised models are valuable for detecting unknown attacks. Deep learning models offer superior performance due to their ability to learn complex patterns and adapt to dynamic conditions
4. Challenges and Limitations: Key challenges include the need for large labeled datasets for supervised models, handling false positives in unsupervised models, and managing computational resources for deep learning models. Real-time processing and scalability are also significant concerns, particularly for large-scale networks.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 9, September 2024

|DOI: 10.15680/IJIRSET.2024.1309048|

5. Future Directions: Future research should focus on hybrid models that integrate supervised, unsupervised, and deep learning techniques to leverage their combined strengths. Enhancing model efficiency and scalability, especially for real-time applications, will be crucial. Additionally, exploring advanced data preprocessing methods and feature extraction techniques can further improve model performance.

VI. CONCLUSION

In conclusion, the integration of machine learning into cyber attack detection for wireless sensor networks (WSNs) within microgrids presents a robust solution to address security challenges. Our study highlights that supervised learning models, particularly Random Forests, achieve high accuracy and effectiveness in identifying known attack patterns. Unsupervised learning models, such as Isolation Forests, excel in detecting novel attacks with minimal false positives. Deep learning models, including Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), demonstrate exceptional performance in capturing complex patterns and temporal dynamics, offering superior accuracy and adaptability. Despite their strengths, challenges remain in data requirements, real-time processing, and scalability. Future research should focus on optimizing these models for real-time applications and developing hybrid approaches that combine the strengths of different ML techniques. By addressing these challenges, machine learning can significantly enhance the resilience and security of WSNs in microgrid environments.

REFERENCES

1. Narasimha Murthy MR, "Future Scope of Artificial Intelligence in Software Engineering", International Journal of Science and Research (IJSR), Volume 12 Issue 12, December 2023, pp. 1401-1402, https://www.ijsr.net/getabstract.php?paperid=SR231113100032
2. Ahmed, M., & Hossain, M. S. (2018). "Anomaly Detection in Wireless Sensor Networks using Machine Learning Techniques." Journal of Network and Computer Applications, 110, 1-10.
3. Alzahrani, B., & Hwang, M. (2021). "Deep Learning Approaches for Intrusion Detection in Wireless Sensor Networks." IEEE Transactions on Network and Service Management, 18(3), 210-220.
4. Bashir, M., & Gupta, S. (2020). "Feature Selection and Data Preprocessing for Cyber Attack Detection in WSNs." International Journal of Computer Applications, 177(28), 1-9.
5. Khan, A., & Ali, M. (2021). "Real-Time Cyber Attack Detection in Wireless Sensor Networks using Machine Learning." Computers & Security, 98, 102034.
6. Liu, H., & Zhang, X. (2019). "Supervised Learning Techniques for Cyber Attack Detection in Wireless Sensor Networks." Computational Intelligence and Neuroscience, 2019, 1-11.
7. Sadiq, A., & Lee, D. (2020). "Evaluating Random Forests and Gradient Boosting for Cybersecurity in WSNs." Journal of Information Security and Applications, 52, 102502.
8. Singh, R., & Kumar, S. (2022). "Challenges in Integrating Machine Learning for Cyber Attack Detection in Resource-Constrained WSNs." Future Generation Computer Systems, 125, 232-245.
9. Wang, J., & Chen, H. (2023). "Integrating Machine Learning-Based Detection Systems into Microgrid Infrastructures." IEEE Transactions on Smart Grid, 14(2), 1867-1878.
10. Yadav, S., & Sharma, R. (2021). "Unsupervised Learning for Intrusion Detection in Wireless Sensor Networks." Pattern Recognition Letters, 142, 44-50.
11. Zhang, L., & Wang, Y. (2022). "Recurrent Neural Networks for Temporal Attack Detection in Wireless Sensor Networks." Neurocomputing, 470, 293-304.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details