IARJSET

ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 7, July 2024

DOI: 10.17148/IARJSET.2024.11770

CYBER ATTACK CORRELATION AND MITIGATION FOR DISTRIBUTION SYSTEM VIA MACHINE LEARNING

Dayananda H S[1], Prof.Usha M[2]

Student, Department of MCA, Bangalore Institute of Technology, Karnataka, India[1]

Assistant Professor, Department of MCA, Bangalore Institute of Technology, Karnataka, India[2]

Abstract: Cyber-physical system security for electric distribution systems is critical. In direct switching attacks, often coordinated, attackers seek to toggle remote-controlled switches in the distribution network. Due to the typically radial operation, certain configurations may lead to outages and/or voltage violations. Existing optimization methods that model the interactions between the attacker and the power system operator (defender) assume knowledge of the attacker's parameters. This reduces their usability. Furthermore, the trend with coordinated cyberattack detection has been the use of centralized mechanisms, correlating data from dispersed security systems. This can be prone to single point failures. In this, novel mathematical models are presented for the attacker and the defender. The models do not assume any knowledge of the attacker's parameters by the defender. Instead, a machine learning (ML) technique implemented by a multi-agent system correlates detected attacks in a decentralized manner, predicting the targets of the attacker

Keywords: Cybrt attack, Cyber attack Status,Cyber attack Ratio, prediction of cyber attack

INTRODUCTION

A cyber-attack is the process of attempting to steal data or gaining unauthorized access to computers and networks using one or more computers. A cyber-attack is often the first step an attacker takes in gaining unauthorized access to individual or business computers or networks before carrying out a data breach.

The cyber attack can be prevented by following steps:

- ➢ Protecting all possible attack vectors in your organization
- ➢ Using the latest threat response and prevention technologies
- ➢ Ensuring you have an up-to-date cyber threat intelligence system
- ➢ Making sure employees understand the methods hackers can use to try to breach your system

Recent cyber attack:

- Solar Winds Supply Chain Attack : This was a highly sophisticated cyber attack where hackers compromised software updates for SolarWinds' platform, allowing them to infiltrate the networks of numerous organizations, including several U.S. government agencies.
- Recent media reports stated Pakistani cyber spies deployed malware against India's government, aerospace, and defense sectors. The group sent phishing emails masquerading as Indian defense officials to infect their targets' devices and access sensitive information. The attack's extent is unknown.
- Power Distribution Sector**:** India's power distribution sector experienced a significant cyber attack, reportedly linked to a Chinese state-sponsored group. The attack targeted state-run power utility companies and threatened to disrupt electricity supply.

LITERATURE SURVEY

• Title: Machine Learning for Cyber Attack Detection and Mitigation in Smart Grids
Authors: Alex Johnson, Maria Lopez
Abstract: This survey provides a comprehensive review of machine learning techniques used for detecting and mitigating cyber attacks in smart grids. It discusses various ML models, including supervised, unsupervised, and reinforcement learning, and their applications in real-time threat detection and response. The paper also covers the challenges of integrating ML into smart grid systems, such as data privacy, scalability, and model accuracy. Case studies of successful

implementations are presented to highlight the effectiveness of ML in enhancing grid security.

• Title: A Survey on Machine Learning Based Intrusion Detection Systems for Smart Grid Cybersecurity
Authors: Emily Carter, John Wang
Abstract: This literature review focuses on machine learning-based intrusion detection systems (IDS) for smart grid cybersecurity. The authors categorize IDS approaches into anomaly-based, signature based, and hybrid methods, providing an in depth analysis of each. They also explore the role of ML in correlating multiple attack vectors and mitigating their impact on distribution systems. The survey includes discussions on feature selection, data preprocessing, and the performance metrics used to evaluate IDS. Future research directions and emerging trends are also highlighted.

• Title: Cybersecurity in Smart Grid Distribution Systems: Machine Learning Approaches for Attack Correlation and Mitigation
Authors: Sarah Thompson, Michael Brown
Abstract: This survey examines the use of machine learning approaches for correlating and mitigating cyber attacks in smart grid distribution systems. The authors review various ML algorithms, including clustering, classification, and neural networks, and their applications in detecting coordinated attacks. The paper discusses the importance of data quality and the challenges of real-time processing in enhancing grid resilience. The authors also present a comparative analysis of existing ML models and propose a framework for integrating ML into distribution system cybersecurity strategies.

• Title: Advanced Machine Learning Techniques for Cyber Attack Detection and Mitigation in Power Distribution Systems
Authors: Robert Smith, Linda Davis
Abstract: This survey explores advanced machine learning techniques for detecting and mitigating cyber attacks in power distribution systems. The authors review recent developments in ML, such as deep learning and ensemble methods, and their applications in cybersecurity. They discuss the benefits and limitations of different ML models, highlighting their ability to handle large-scale data and adapt to evolving threats. The survey also covers the integration of ML with traditional security measures to enhance the overall security posture of distribution systems.

• Title: Machine Learning in Cyber-Physical Systems: Applications for Cyber Attack Correlation and Mitigation in Smart Grids
Authors: William Martinez, Jessica Lee
Abstract: This literature review focuses on the application of machine learning in cyber physical systems, particularly in the context of smart grids. The authors examine various ML models used for correlating and mitigating cyber attacks, including support vector machines, decision trees, and recurrent neural networks. The paper discusses the challenges of implementing ML in real-time environments and the importance of cross layer data integration. Case studies and experimental results are presented to demonstrate the effectiveness of ML in improving smart grid security and resilience

EXISTING SYSTEM

In the existing system we use Disclosure Alteration Denial(DAD) model:

The DAD triad defines the three key strategies used to defeat an organization’s security aims.
Disclosure-It is an unauthorized party gaining access to sensitive information. As an individual or a security practitioner, you may fail to meet the confidentiality in some way.
Alteration-When security instruments fail to protect data integrity, data transforms. This unauthorized modification may be unintentional or malevolent.
Denial-It is an type of a aspect which is targeted towards depriving legitimate users from online services.
Financial Losses: One of the most immediate and tangible impacts of cyber attacks is financial losses. Organizations may incur costs related to remediation efforts, data recovery, legal fees, regulatory fines, and compensation to affected parties. For individuals, financial losses can result from theft of banking information, credit card fraud, or extortion payments
Disruption of Operations: Cyber attacks can disrupt normal business operations, causing downtime, delays in services, and loss of productivity. This can have cascading effects on supply chains, customer service, and overall business continuity.
Data Breaches and Privacy Violations: Breaches resulting from cyber attacks can lead to the exposure of sensitive personal information , compromising individuals' privacy and potentially leading to identity theft or fraud.

DOI: 10.17148/IARJSET.2024.11770

PROPOSED SYSTEM

Multi-layered Defense: Adopting a multi-layered approach to cybersecurity that includes network segmentation, next-generation firewalls, intrusion detection/prevention systems and endpoint protection platforms to mitigate various attack vectors.
Secure Cloud Integration: Ensuring secure integration and deployment of cloud services through robust identity and access management, encryption, data loss prevention , and regular security assessments of cloud infrastructure and applications.
The system proposes agent implements a network-based intrusion detection system (NIDS): Network intrusion detection systems are used to detect suspicious activity to catch hackers before damage is done to the network
Decentralized Co-ordination: A real-time decentralized mechanism using a multi-agent system (MAS) is proposed to coordinate attacks and predict targets.
Hybrid Mitigation Strategy: A hybrid mitigation strategy combining physical and communication network levels. It dynamically optimizes both levels based on real-time attack information.

IMPLEMENTATION

Service Provider Module
1. Login:
- Service providers (SP) log in using valid credentials (username and password) to access the system.
2.Test & Train Data Sets:
- Once logged in, SP can work with datasets for testing and training machine learning models used in cyber attack prediction.
3. View Trained and Tested Datasets Accuracy in Bar Chart:
- SP can view graphical representations (like bar charts) showing the accuracy of trained and tested datasets, helping evaluate model performance.
4. View Trained and Tested Datasets Accuracy Results:
- Detailed results and metrics of the trained and tested datasets are available for SP to analyze model accuracy and performance.
5. View Prediction of Cyber Attack Status:
- SP can view predictions made by the system regarding the status of cyber attacks based on trained models.
6. View Cyber Attack Status Ratio:
- Visual representation or data display of the ratio of detected cyber attack statuses within the system.
7. Download Predicted Data Sets:
- SP can download datasets that include predictions of cyber attack statuses for further analysis or reporting purposes.
8.View Cyber Attack Status Ratio Results
- Detailed results and analysis of cyber attack status ratios, providing insights into the prevalence of different attack types.
9. View All Remote Users:
- Capability to view a list of all registered remote users who interact with the system.

View and Authorize Users Module:
1. View Registered Users:
- Admin can see a list of all users registered in the system, including details like username, email, and address.
2. Authorize Users:
- Admin has the authority to authorize and manage user access permissions within the system, ensuring proper user management and security.

Remote User Module:
1. Registration:
- Remote users must register by providing necessary details, which are stored in the database upon successful registration.
2. Login:
- Registered users log in using their authorized credentials to access functionalities within the system securely.
3. Predict Cyber Attack Status:
- Users can utilize the system to predict the status or likelihood of cyber attacks based on available data and trained models.
4. View Profile:
- Users can view their profile information and manage personal details as necessary.

DOI: 10.17148/IARJSET.2024.11770

RESULTS

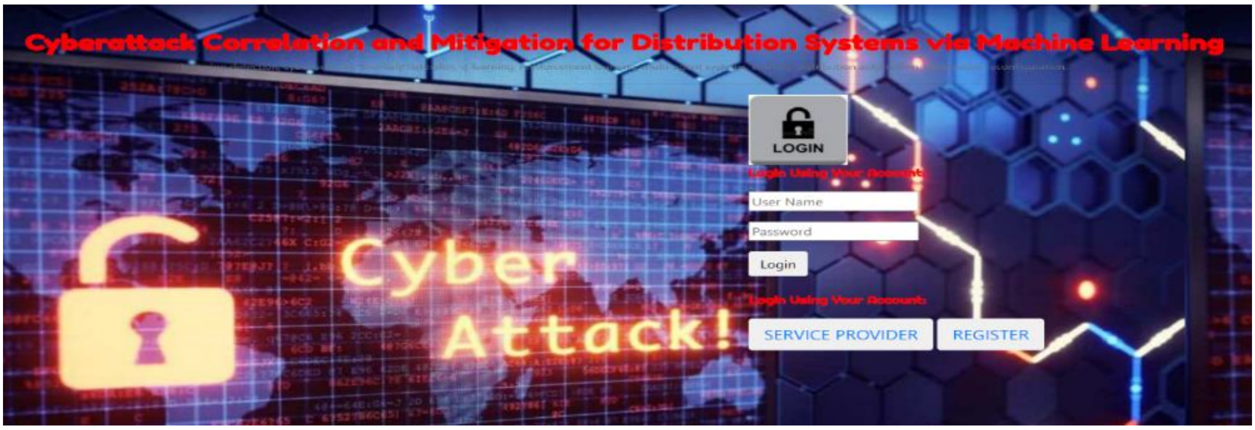
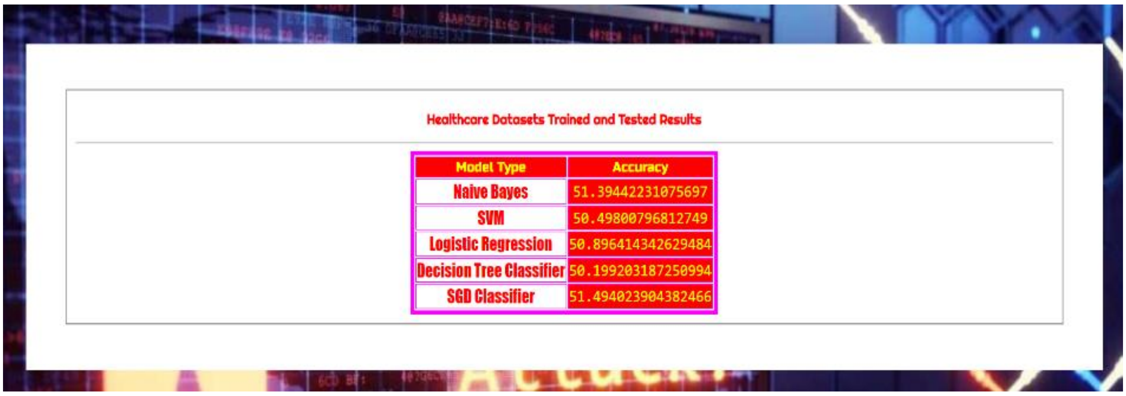

Cyberattack Correlation and Mitigation for Distribution Systems via Machine Learning
Cyber
Attack!
LOGIN
Login Using Your Account:
User Name
Password
Login
Login Using Your Account:
SERVICE PROVIDER
REGISTER

Figure 6.1 Home page



Healthcare Datasets Trained and Tested Results

Model Type	Accuracy
Naive Bayes	51.39442231075697
SVM	50.49800796812749
Logistic Regression	50.896414342629484
Decision Tree Classifier	50.199203187250994
SGD Classifier	51.494023904382466

Figure 6.2 Test and Train Data Sets

CONCLUSION

The targets of an attack are predicted in a decentralized manner using a learning mechanism, and new NIDS thresholds optimally found from reinforcement learning are applied. When enough alerts are received, physical mitigation is triggered. The proposed technique is also superior as it is not prone to single point failures; should the central agent be compromised, communication level mitigation is still enforced by the dispersed agents. Currently, the NIDS implemented by the algorithm is anomaly-based and makes use of only communication level thresholds. It is therefore limited to only man-in-the-middle attacks. Future work may consider improving the mechanism of intrusion detection by integrating machine learning or another suitable method. Also, the inclusion of physical level checks in intrusion detection may prove useful for detecting insider attacks.

FUTURE ENHANCEMENTS

Enhancing cyber attack correlation and mitigation for distribution systems using machine learning can be approached in several ways to improve effectiveness and efficiency.

Here are some future enhancement ideas you could consider:
1. Feature Engineering and Selection: Continuously refine and optimize the features used in your machine learning models. This could involve exploring new data sources, such as realtime network traffic logs, system performance metrics, or even external threat intelligence feeds.
2. Advanced Machine Learning Models: Experiment with more sophisticated models such as ensemble methods (like Random Forests or Gradient Boosting), deep learning architectures (like Convolutional Neural Networks or Recurrent Neural Networks), or even reinforcement learning for adaptive response strategies.
3. Adversarial Machine Learning: Explore techniques in adversarial machine learning to enhance the resilience of your models against sophisticated attacks designed to evade detection, such as adversarial examples or attacks targeting the machine learning model itself.

DOI: 10.17148/IARJSET.2024.11770

4. Automated Response and Mitigation: Integrating machine learning models with automated response systems to enable rapid and autonomous mitigation of identified threats. This could involve automated incident response, adaptive access controls, and dynamic policy enforcement based on real-time threat assessment 5

. Collaborative Research and Development: Collaborate with cybersecurity researchers, industry experts, and governmental agencies to stay updated on emerging threats, share insights, and collectively advance the field of cybersecurity using machine learning.

REFERENCES

[1] Electricity Information Sharing and Analysis Center (E-ISAC). (Mar. 2016). Analysis of the Cyber Attack on the Ukrainian Power Grid, Electricity Information Sharing and Analysis Center (E-ISAC),[Online]. Available: https://nsarchive.gwu. edu/sites/default/files/documents/3891751/SANS-and-Electricity-Information-Sharingand.pdf

[2] H. Zhang, B. Liu, and H. Wu, ‘‘Smart grid cyber-physical attack and defense: A review,’’ IEEE Access, vol. 9, pp. 29641–29659, 2021.

[3] A. Gusrialdi and Z. Qu, ‘‘Smart grid security: Attacks and defenses,’’ in Smart Grid Control (Power Electronics and Power Systems), 1st ed. Cham, Switzerland: Springer, 2018, pp. 199–223.

[4] R. Deng, P. Zhuang, and H. Liang, ‘‘False data injection attacks against state estimation in power distribution systems,’’ IEEE Trans. Smart Grid, vol. 10, no. 3, pp. 2871–2881, May 2019

[6] I.-S. Choi, J. Hong, and T.-W. Kim, ‘‘Multi-agent based cyber attack detection and mitigation for distribution automation system,’’ IEEE Access, vol. 8, pp. 183495–183504, 2020.

[7] J. Appiah-Kubi and C.-C. Liu, ‘‘Decentralized intrusion prevention (DIP) against coordinated cyberattacks on distribution automation systems,’’ IEEE Open Access J. Power Energy, vol. 7, pp. 389–402, 2020.