Email: editor@ijerst.com or editor.ijerst@gmail.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 17, Issue 2, 2024

Cyber attack and Mitigation for Distributed Systems via Machine Learning

[1]DR.GOHIN, [2]GUTTULA SIVA SANKAR

[1](Associate Professor), MCA, Swarnandhra College

[2]MCA, scholar, Swarnandhra College

ABSTRACT

Distributed systems form the backbone of modern technological infrastructure, serving critical functions in various domains such as finance, healthcare, and communication. However, the distributed nature of these systems makes them susceptible to a wide range of cyberattacks, including DDoS attacks, malware infiltration, and data breaches. Traditional security measures often struggle to keep pace with the evolving sophistication of cyber threats. This paper proposes a novel approach to enhance the security of distributed systems through the integration of machine learning techniques for cyberattack detection and mitigation. By leveraging the vast amount of data generated by distributed systems, machine learning algorithms can effectively identify patterns indicative of malicious activities in real-time. This proactive detection capability enables prompt response to potential threats.

1.INTRODUCTION

The goal of this research is to use machine learning approaches to tackle the problems caused by cyber threats in distributed systems. The use of artificial intelligence allows for,we seek to enhance the resilience of these systems against a wide range of attacks, including but not limited to DDoS (Distributed Denial of Service), malware propagation, and data breaches.

Our goal in this study is to learn more about how machine learning algorithms can monitor distributed systems in real-time and identify suspicious behaviour in the massive amounts of data they produce. By identifying patterns and deviations from normal behaviour, these algorithms can proactively alert administrators to potential threats, enabling timely intervention to mitigate risks and minimize damage.

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 17, Issue 2, 2024

Moreover, this project will investigate the feasibility of employing machine learning for adaptive Défense mechanisms within distributed systems. By continuously learning from past incidents and adjusting their strategies accordingly, these systems can dynamically adapt to emerging threats, thereby strengthening their security posture in an ever-changing threat landscape.

The goal of attack mitigation is to keep the system running smoothly by reducing the impact of harmful assaults. To strengthen the state estimation's security, they substituted their maximum likelihood estimate (MLE) values for the suspicious data, and to counteract data unavailability attacks (DUAs), OPF-based controls suggested a robust SG network built on support vector machines (SVMs) and equipped with decentralised energy resources (DERs).

In sum, this initiative is an important step in making distributed systems more secure and resistant to the growing number of cyberattacks. Through the fusion of machine learning and distributed computing, we aim to develop proactive and adaptive defences mechanisms that can effectively thwart attacks and safeguard critical infrastructure and sensitive data.

Distributed systems are ubiquitous in modern computing environments, facilitating the seamless exchange of data and resources across networks. Malware infections, data breaches, and denial-of-service assaults are only some of the cyber risks that might affect them because of their dispersed nature. Machine learning and other sophisticated approaches are frequently needed since traditional security measures can't keep up with the ever-changing threat environment. By analyzing massive volumes of data, machine learning algorithms can spot trends that could indicate a cyberattack, opening the door to preventative measures. Nonetheless, the efficacy of these models hinges on their accuracy, which can be compromised by factors such as imbalanced datasets, data scarcity, and adversarial manipulation. To mitigate these challenges, This study explores methods to improve machine learning models in distributed systems so that they can identify and mitigate cyberattacks more accurately.

2.LITERATURE SURVEY\

The goal of this research is to use machine learning approaches to tackle the problems caused by cyber threats in distributed

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 17, Issue 2, 2024

systems. The use of artificial intelligence allows for,we seek to enhance the resilience of these systems against a wide range of attacks, including but not limited to DDoS (Distributed Denial of Service), malware propagation, and data breaches.

Our goal in this study is to learn more about how machine learning algorithms can monitor distributed systems in real-time and identify suspicious behaviour in the massive amounts of data they produce. By identifying patterns and deviations from normal behaviour, these algorithms can proactively alert administrators to potential threats, enabling timely intervention to mitigate risks and minimize damage.

Moreover, this project will investigate the feasibility of employing machine learning for adaptive Défense mechanisms within distributed systems. By continuously learning from past incidents and adjusting their strategies accordingly, these systems can dynamically adapt to emerging threats, thereby strengthening their security posture in an ever-changing threat landscape.

The goal of attack mitigation is to keep the system running smoothly by reducing the impact of harmful assaults. To strengthen the state estimation's security, they substituted their maximum likelihood estimate (MLE) values for the suspicious data, and to counteract data unavailability attacks (DUAs), OPF-based controls suggested a robust SG network built on support vector machines (SVMs) and equipped with decentralised energy resources (DERs).

In sum, this initiative is an important step in making distributed systems more secure and resistant to the growing number of cyberattacks. Through the fusion of machine learning and distributed computing, we aim to develop proactive and adaptive defences mechanisms that can effectively thwart attacks and safeguard critical infrastructure and sensitive data.

Distributed systems are ubiquitous in modern computing environments, facilitating the seamless exchange of data and resources across networks. Malware infections, data breaches, and denial-of-service assaults are only some of the cyber risks that might affect them because of their dispersed nature. Machine learning and other sophisticated approaches are frequently needed since traditional security measures can't keep up with the ever-changing threat environment. By analyzing massive volumes of data,

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 17, Issue 2, 2024

machine learning algorithms can spot trends that could indicate a cyberattack, opening the door to preventative measures. Nonetheless, the efficacy of these models hinges on their accuracy, which can be compromised by factors such as imbalanced datasets, data scarcity, and adversarial manipulation. To mitigate these challenges, This study explores methods to improve machine learning models in distributed systems so that they can identify and mitigate cyberattacks more accurately.

3. EXISTING SYSTEM

Anomaly Detection Systems: Many existing systems employ machine learning algorithms for anomaly detection in distributed systems. These systems analyze network traffic, system logs, and other relevant data to identify deviations from normal behavior that could indicate a cyberattack. Techniques such as unsupervised learning, including clustering and autoencoders, are commonly used for anomaly detection.

Intrusion Detection Systems (IDS): IDSs are crucial components in the defense against cyberattacks. They monitor network and system activities for malicious behavior or policy violations. Machine learning algorithms, such as support vector machines (SVM), random forests, and deep learning models, are integrated into IDSs to enhance their detection capabilities and reduce false positives.

Behavioral Analysis Systems: These systems focus on analyzing the behavior of users, applications, and devices within a distributed system to detect potential threats. Machine learning algorithms are trained on historical data to recognize patterns of normal and abnormal behavior, enabling the identification of suspicious activities indicative of cyberattacks.

3.1 PROPOSED SYSTEM

Data Collection and Preprocessing: The proposed system will collect data from various sources within the distributed system, including network traffic, system logs, and application activities. This data will be preprocessed to extract relevant features and prepare it for analysis by machine learning algorithms.

Machine Learning Model Training: Utilizing supervised, unsupervised, and semi-supervised learning techniques, the system will train machine learning models on historical data to recognize patterns

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 17, Issue 2, 2024

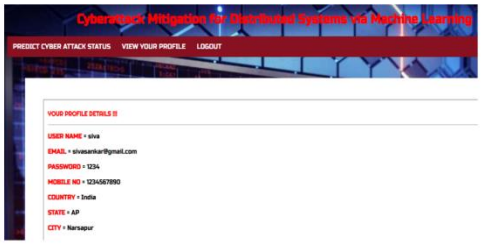
indicative of cyberattacks. Models will be trained to detect anomalies, classify malicious activities, and predict potential threats based on learned patterns.

Real-Time Monitoring and Detection: The trained machine learning models will be deployed for real-time monitoring of the distributed system. Incoming data streams will be continuously analyzed, and anomalies or suspicious activities will be identified promptly. Detection algorithms will adapt to evolving attack patterns and adjust detection thresholds dynamically.

4. OUTPUT SCREENS

Home Page

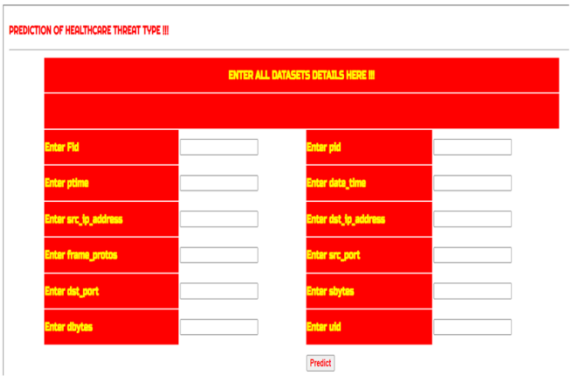
View profile page



View Remote Users

User Login

Output



5. CONCLUSION

This project presents a decentralized attack correlation technique and a hybrid mitigation. Compared to interdiction models in the literature, this work assumes no explicit

ISSN 2319-5991 www.ijerst.com
Vol. 17, Issue 2, 2024

knowledge of the attacker's parameters by the defenders, which in this case, are agents. 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.

In conclusion, this project underscores the importance of augmentation techniques in fortifying the accuracy of machine learning models deployed in distributed systems for cyberattack detection and mitigation. By addressing the inherent challenges associated with data scarcity and adversarial manipulation, augmentation strategies offer a pathway towards more robust and resilient security solutions. The findings of this research contribute to advancing the state-of-the-art in cybersecurity and pave the way for the widespread adoption of machine learning-driven defence mechanisms in distributed computing environments.

6.REFERENCES

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

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

[3] S. Lakshminarayana, J. Ospina, and C. Konstantinou, ''Load-alteringattacks against power grids under COVID-19 low-inertia conditions,''IEEE Open Access J. Power Energy, vol. 9, pp. 226–240, 2022.

[4] I.-S. Choi, J. Hong, and T.-W. Kim, ''Multi-agent based cyber attackdetection

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 17, Issue 2, 2024

and mitigation for distribution automation system,'' IEEE Access,vol. 8, pp. 183495–183504, 2020.

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

[6]C.Moya and J.Wang, ''Developing correlation indices to identifycoordinated cyber-attacks on power grids,'' IET Cyber-Phys. Syst., Theory Appl.,vol. 3, no. 4, pp. 178–186, Dec. 2018.

[7] Y. Lin and Z. Bie, ''Tri-level optimal hardening plan for a resilientdistribution system considering reconfiguration and DG islanding,'' Appl. Energy,vol. 210, pp. 1266–1279, Jan. 2018.

[8] K. Lai, M. Illindala, and K. Subramaniam, ''A tri-level optimization modelto mitigate coordinated attacks on electric power systems in a cyberphysical environment,'' Appl. Energy, vol. 235, pp. 204–218, Feb. 2019.

[9] A. Abedi, M. R. Hesamzadeh, and F. Romerio,''An ACOPF-based bileveloptimization approach for vulnerability assessment of a power system,''Int. J. Electr. Power Energy Syst., vol. 125, Feb. 2021, Art. no. 106455.