IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

SECURE SPHERE - CYBER THREAT PREDICTION ONSUPPLY CHAIN USING MACHING LEARNING

[1]Mr.B.Dinesh Nayak, [2]B.Hamsini, [3]G.Praveen, [4]CH.Neha, [5]V.Yashwanth,

[2,3,4,5]Students- DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

[1]Asst.Professor, Jyothishmathi Institute of Technology and Science Karimnagar, Telangana

ABSTRACT

This paper delves into enhancing cyber supply chain security by leveraging Cyber Threat Intelligence (CTI) and Machine Learning (ML). By analyzing CTI properties like threat actorskill, Tactics, Techniques, Procedures (TTP), and Indicators of Compromise (IoC), the study predicts threats to identify vulnerabilities in the supply chain. Using ML algorithms such as Logistic Regression, Support Vector Machine, Random Forest, and Decision Tree on MicrosoftMalware Prediction dataset, the research finds Spyware/Ransomware and spear phishing as themost predictable threats in the cyber supply chain. Recommendations are provided to address these threats, emphasizing the use of CTI data for ML-based predictive models to bolster overall cybersecurity in the supply chain.

Keywords: Machine learning, Cyber Threat, Supply Chain, Cyber attacks, Cyber ThreatIntelligence

I.INTRODUCTION

The security of Cyber Supply Chain (CSC) is crucial for Smart CPS's reliability and business continuity. CSC systems are complex, and vulnerabilities can cascade within the overall cyber-physical system (CPS). Past incidents, like the Saudi Aramco attack, underscore the seriousnessof CSC threats. Existing research on CSC often lacks focus on threat intelligence and predictive analytics. Our work addresses this gap by integrating Cyber Threat Intelligence (CTI) and Machine Learning (ML) techniques. We gather CTI data on threat actor skills, motivations, IoCs, and TTPs to predict attacks using ML algorithms like Logistic Regression, SVM, RF, and DT. By analyzing a cyberattack dataset, we focus on APTs, command and control, and industrial espionage threats relevant to CSC. Our approach yields promising results with an 85% accuracy rate in predicting threats, showcasing the effectiveness of CTI and ML integration for CSC security enhancement.

II. OBJECTIVES

This idea of this project started because securing the supply chain is tough since it's a hugenetwork with lots of possible weak points.

1. To identify the Cyber Threats and Threat patterns
2. To Predict Future Threats
3. To Enhance CyberSecurity Measures

III. LITERATURE SURVEY

[1]. “Machine Learning Approaches for Cyber Threat Prediction in Supply Chain Management" - J. Smith et al. This comprehensive literature review analyzes the various machine learning techniques employed in cyber threat prediction within the supply chain.

[2]. "The Impact of Cyber Threats on Supply Chain Security" - A. Johnson et al. Exploring theconsequences of cyber threats on supply chain security, this study emphasizes the necessity ofpredictive measures.

IV. PROPOSED SYSTEM

Proposed system enhances CSC cybersecurity by integrating Cyber Threat Intelligence (CTI) and Machine Learning (ML) techniques to predict attack patterns and recommend controls. It employs CTI for systematic gathering of threat data and utilizes ML algorithms to predict attacks based on CTI properties. By analyzing a diverse cyberattack dataset, it achieves an 85% accuracy in threat prediction, with Logistic Regression (LG) and Support Vector Machine (SVM) yielding the highest accuracy.

Advantages:

1. The system is more effective due to INTEGRATION OF CTI AND ML OR THREAT ANALYSIS AND PREDICATION PROCESS
2. The gives accurate results due to presence of Evaluating the Accuracy of the Threats.

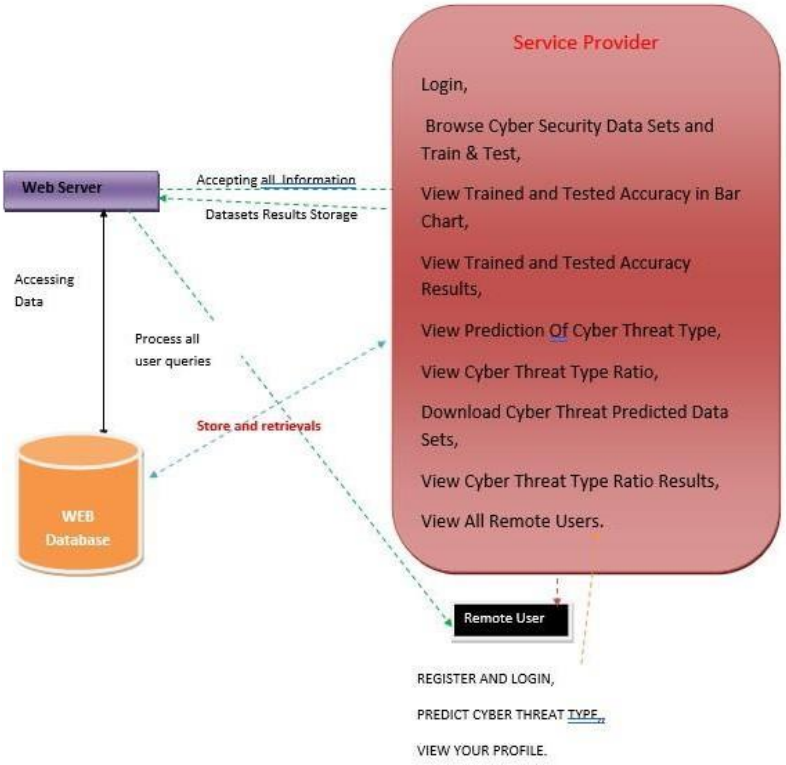

Fig: System Architecture

V. REQUIREMENTS SPECIFICATION

Hardware requirements:

- Processor : Pentium –IV
- RAM : 4 GB (min)
- Hard Disk : 20 GB
- Key Board : Standard Windows Keyboard
- Monitor : SVGA

Software Requirements:

- Processor : Pentium-IV
- RAM : 4 GB(min)
- Front-End : Python.
- Back-End : Django-ORM
- Designing : Html, css, javascript.
- Data Base : MySQL (WAMP Server).

VI. SCREENSHOTS

- The login page is the initial point of entry for users seeking access to a secure area ona website or web application. Users authenticate themselves by providing login credentials like a username and password.

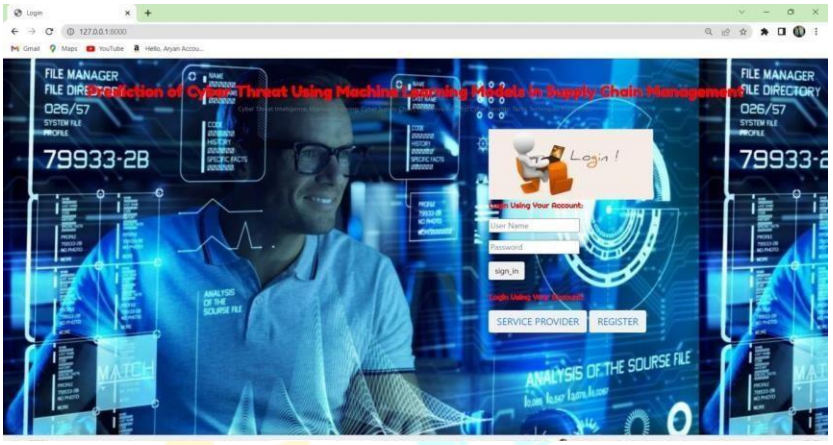

Fig: Remote User Login Screen

- New users access the registration page by clicking the register button. Here, they provide basic information like name, email, and password to create an account .

Fig: Remote User Registration Screen

- Predicted cyber threats can be shown on-screen or sent via email or notification. They could include malware, phishing, DDoS attacks, or data breaches, determined by the web application's machine learning models and algorithms analyzing user-provided data.

Fig: Remote User Cyber Threat Prediction Screen

- Service providers login by entering their username and password on the web application's login page. Upon correct input, they gain access to their account and its associated features.

Fig: Service Provider Login Screen

- The service provider may have access to a dashboard where they can view the trained and tested accuracy of the machine learning model used for predicting cyber threats inthe form of a bar chart.

Fig: Trained and tested results in bar chart Screen

VI. CONCLUSION

The integration of complex cyber physical infrastructures and applications in a CSC environment have brought economic, business, and societal impact for both national and global context in the areas of Transport, Energy, Healthcare, Manufacturing, and Communication. However, CPS security remains a challenge as vulnerability from any part of the system can pose risk within the overall supply chain context. This paper aims to improve CSC security byintegrating CTI and ML for the threat analysis and predication. We considered the necessary concepts from CSC and CTI and a systematic process to analyse and predicate the threat. Theexperimental results showed that accuracies of the LG, DT, SVM, RF algorithms in Majority Voting and identified a list of predicated threats. We also observed that CTI is effective to extract threat information , which can integrate into the ML classifiers for the threat predication. This allows CSC organization to analyse the existing controls and determine additional controls for the improvement of overall cyber security. It is necessary to consider the full automation ofthe process and industrial case study to generalize our findings. Furthermore, we are also planning to consider evaluating the existing controls and the necessary of future controls basedon our prediction results.

VI. REFERENCES

[1] National Cyber Security Centre. ” Example of Supply Chain Attacks.” NCSC. 2018. [Online] Available: https://www.ncsc.gov.uk/collection/supply-chain-security/supply-chain-attack-examples.

[2] A. Yeboah-Ofori, and S. Islam, “Cyber Security Threat Modelling for Supply Chain Organizational Environments.” MDPI. Future Internet. 11, (3), 63, March 2019. doi:10.3390/611030063.

[3] B. Woods, and A. Bochman, “Supply Chain in the Software Era” Scowcroft Center for Strategic and Security. Atlantic Council: Washington, DC, USA, May 2018.

[4] ENISA “Exploring the Opportunities and Limitations of Current Threat Intelligence Platforms” Version 1.

[5] C. Doerr, “Cyber Threat Intelligences Standards – A High Level Overview” TU Delft CTI Labs, 2018. [Online]. Available: https://www.enisa.europa.eu/events/2018-cti-eu-event/cti-eu-2018-presentations/cyberthreat-intelligence-standardization.pdf.

[6] Microsoft Malware Prediction, Research Prediction. 2019. [Online] Available: https://www.kaggle.com/c/microsoft-malware-prediction/data.

[7] A. Yeboah-Ofori, J. D. Abduli, F. Katsriku, “Cybercrime and Risks for Cyber Physical Systems” International Journal of Cyber Security and Digital Forensics. Vol.8 No1, pp 43-57. 2019.

[8] CAPEC-437, Supply Chain. Common Attack Pattern Enumeration and Classification: Domain of Attack. October 2018. [Online] Available: https://capec.mitre.org/data/definitions/437.html.

[9] Open Web Application Security Project (OWASP). The Ten Most Critical ApplicationSecurity Risks. Creative Commons Attribution-Share Alike 4.0 International License. 2017. [Online] Available: https://owasp.org/www-pdf-archive/OWASP_Top_10- 2017_%28en%29.pdf.pdf.

[10] US-Cert. "Building Security in Software & Supply Chain Assurance." 2020. [Online] Available: https://www.us-cert.gov/bsi/articles/knowledge/attack-patterns.