PREDICTIVE ANALYTICS FOR CYBER THREATS TO IMPROVE CYBER SUPPLY CHAIN SECURITY

[1] Mudimela Madhusudhan, [2]Kadari Gohathi ,[3]Kathi Venkata Saketh Reddy, and [4]Kosamba Pradeep
[1] *Assistant Professor of Dept of CSE,CMR Technical Campus,Medchal, Hyderabad*
[1]*madhusudhan.cse@gmail.com*
[2,3,4] *B.Tech Student*,Dept of CSE, *CMR Technical Campus*, Hyderabad
[2] *kadarigohathi@gmail.com,*[3]*sakethkathi147@gmail.com,*[4]*pradeepkosamba@gmail.com*

Abstract: In this project, the aim is to analyse and predicate threats to improve cyber supply chain security. We have applied Cyber Threat Intelligence (CTI) with Machine Learning (ML) techniques to analyse and predict the threats based on the CTI properties. That allows to identify the inherent CSC vulnerabilities so that appropriate control actions can be undertaken for the overall cybersecurity improvement. To demonstrate the applicability of our approach, CTI data is gathered and a number of ML algorithms. The results relating to the prediction reveal that Spyware/Ransomware and spear phishing are the most predictable threats in CSC. We have also recommended relevant controls to tackle these threats. We advocate using CTI data for the ML predicate model for the overall CSC cyber security improvement.

Key Words — Cyber Threat Intelligence, Cyber supply chain, Cyber threat intelligence

I. INTRODUCTION

Cyber Supply Chain (CSC) security is critical for reliable service delivery and ensure overall business continuity of Smart CPS. CSC systems by its inherently is complex and vulnerabilities within CSC system environment can cascade from a source node to a number of target nodes of the overall cyber physical system (CPS). There are several examples forsuccessful CSC attacks. For instance, Dragonfly, a Cyber Espionage group, is well known for targeting CSC organization.

Due to the invincibility nature of cyber attacks on the cyber supply chain (CSC), and the cascading effects of malware infections, we use machine learning to predict attacks. As organizations have become more reliant on CSC systems for business continuity, so are the increase in vulnerabilities and the threat landscapes. Some traditional approach to detecting and defending malware attack has largely been antimalware or antivirus software such as spam filters, firewall, and IDS/IPS. These tools largely succeed, however, as threat actors get more intelligent, they are able to circumvent and affect nodes on systems which then propagates. we use ML techniques to learn the dataset and predict which CSC nodes have detection or no detection. The purpose is to predict which modes are venerable tocyberattacks and for predicting future trends. To demonstrate the applicability of our approach, we used a dataset from the Microsoft Malware Prediction website. Further, an ensemble is usedto link Logistic Regression, and Decision Tree and SVM algorithms in Majority Voting and runon the training data and then use 10-fold cross validation to test the parameter estimation, accurate results and predictions. The results show that ML algorithms in Decision Treesmethods can be used in cyber supply chain predict analytics to detect and predict future cyber attack trends.

II. LITERATURE SURVEY

A recent NCSC report highlights a list of CSC attacks by exploiting vulnerabilities that exist within the systems. Organizations outsource part of their business and data to the third- party service providers that could lead any potential threat. There are several examples for successful CSC attacks. For instance, Dragonfly, a Cyber Espionage group, is well known for targeting CSC organization. The Saudi Aramco power station attack halted its operation due toa massive cyberattack. There are existing works that consider CSC threats and risks but a lack of focus on threat intelligence properties for the overall cyber security improvement.

III. PROPOSED METHODOLOGY

CSC security strategy combines CTI and cybersecurity risk strategy including mechanisms, resources and plans to determine how security goals and controls will be formulated, implemented and achieved in line with organization goal and objectives. It includes identifying, analyzing, reviewing and evaluating organizational assets including infrastructures,resources and implementation procedures. CSC security strategy combines, CTI andcybersecurity risk assessment strategy to gather intelligence and formulate policies. Strategic, tactical and operational management roles and responsibilities are recursive and support each other to ensure security goals are achieved. Strategic management uses intelligence decision to support plans that determine security goals and assign responsibility including executive authorization of blueprints and budget allocation. It includes risk assessment, CSC requirements capturing and business function.

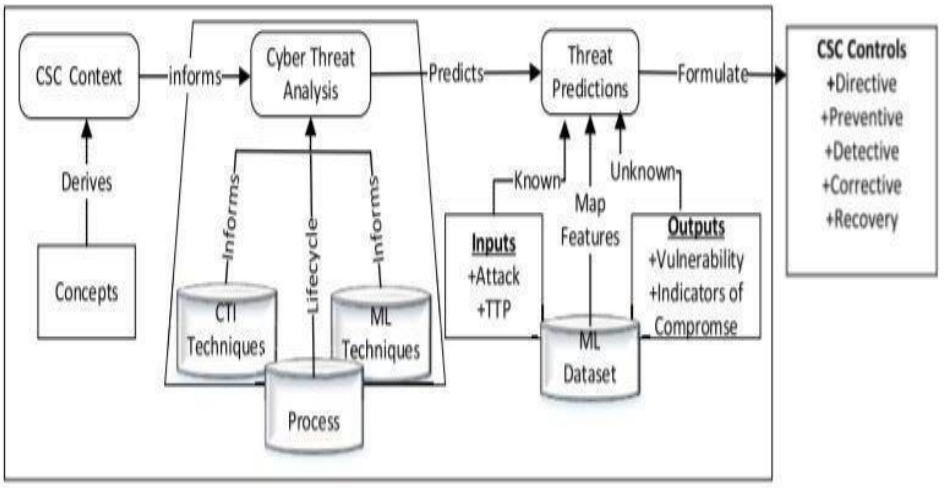

Fig 3.1 Project functionality

IV. ELEMENTS REQUIRED

- **Cyber Threat Intelligence (CTI)**

Cyber Threat Intelligence provides an intelligence analysis to discover unknown to known threats using various properties including threat actor skill and motivation, Tactics, Techniques, and Procedure (TT and P), and Indicator of Compromise (IoC).

- **Cyber Supply Chain (CSC)**

Cyber Supply Chain system is complex which involves different sub-systems performing various tasks. Security in supply chain is challenging due to the inherent vulnerabilities and threats from any part of the system which can be exploited at any point within the supply chain. This can cause a severe disruption on the overall business continuity. Therefore, it is paramount important to understand and predicate the threats so that organization can undertake necessary control measures for the supply chain securit

V. WORKING PROCEDURE OF THE MODEL

- **Identify and Gather Information**:

This step identifies all vulnerable spots on the supply inbound and outbound chains on the meta-model that is used as indicators for an attack. For instance, in case of a malware attack, this activity looks for the relevant information such as the source of the attack, the tools, patterns and the attack vectors from the analysis of the malware attack that used as our indicator.

- **Risk Assessments**

The risk assessment activity includes the process to mitigate CSC risks by determining the probability and impact of CSC attacks and threats as well as the vulnerable spots that could be exploited within the cyber supply inbound and outbound chains and third-party organizations. It identifies all threats that may pose a risk on the system. Risk assesses the CSC security domain and analyse risks access spots that are capture captured. Develop mitigating techniques to control the risks by identifying risks posed by auditing the thirdparty organizations. Classify them based on their service provisions and levels of integration to the various supply chain network system.

- **Analysis**

This activity focuses on analysis of the threats to determine the actual source of the attack, the type of attack, the attack pattern, the TTP and attack vectors. This will assist to assign the IoC required and what controls

VI. RESULTS

Fig 5.1: Login screen

Fig 5.2: Vulnerability Analysis

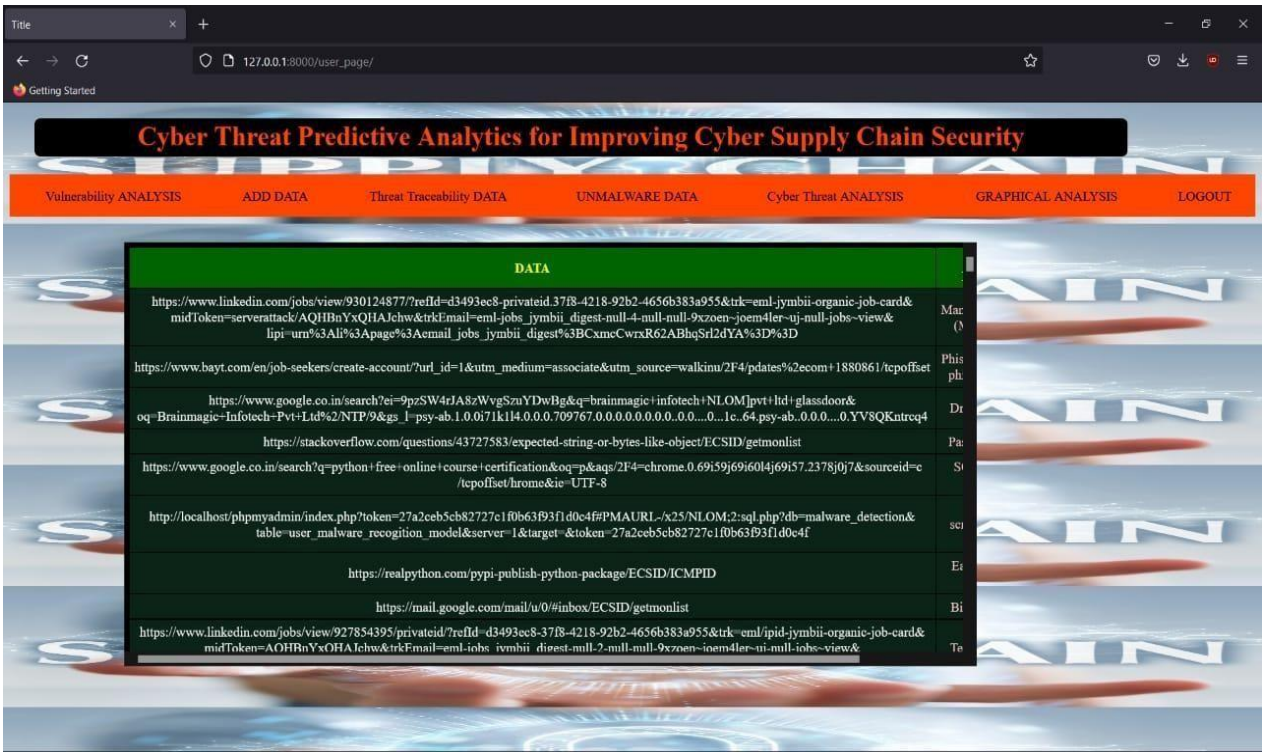

Fig 5.3: Upload Data

Fig 5.4: Threat Traceability Data

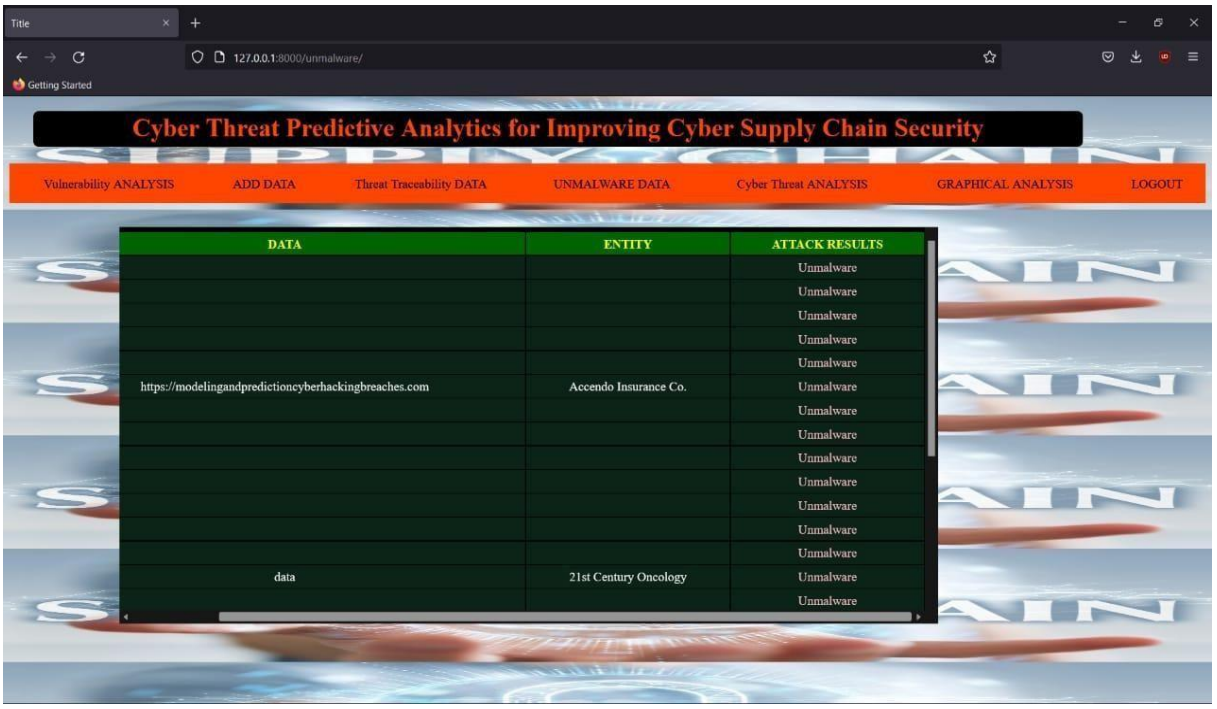

Fig 5.5: Unmalware data

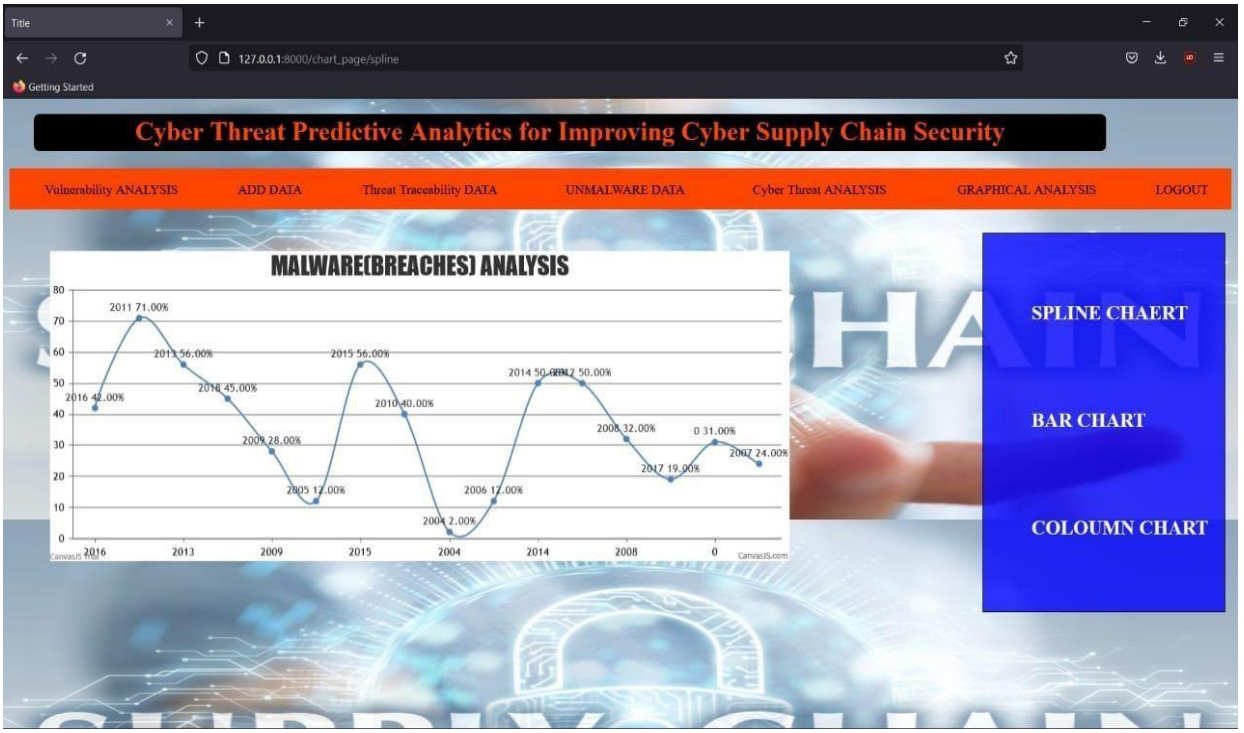

Fig 5.6: Spline Chart

VII. 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 by integrating 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. The experimental 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 of the 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 based on our prediction results

VIII. FUTURE SCOPE

The project can be further developed into the real time application for which can be applied in the organizations on the networks. The, organizational implementation plays an important role in the finding of the infected systems and to show the probable infected systems for which can be vulnerable.

IX. REFERENCES

1. National Cyber Security Centre. (2018). Example of Supply Chain Attacks.
2. A. Yeboah-Ofori and S. Islam, ‘‘Cyber security threat modelling for supply chain organizational environments,’’ MDPI. Future Internet, vol. 11, no. 3, p. 63, Mar. 2019.
3. B. Woods and A. Bochman, ‘‘Supply chain in the software era,’’ in Scowcroft Center for Strategic and Security. Washington, DC, USA: Atlantic Council, May 2018.
4. Exploring the Opportunities and Limitations of Current Threat Intelligence Platforms, Version 1, ENISA, Dec. 2017.
5. C. Doerr, TU Delft CTI Labs. (2018). Cyber Threat Intelligences Standards—A High Level Overview.
6. Research Prediction. (2019). Microsoft Malware Prediction.
7. A.Yeboah-Ofori and F. Katsriku, ‘‘Cybercrime and risks for cyber physical systems,’’ Int. J. Cyber-Secur. Digit. Forensics, vol. 8, no. 1, pp. 43–57, 2019.
8. CAPEC-437, Supply Chain. (Oct. 2018). Common Attack Pattern Enumeration and Classification: Domain of Attack.
9. Open Web Application Security Project (OWASP). (2017). The Ten Most Critical Application Security Risks, Creative Commons Attribution-Share Alike 4.0 International License.
10. US-Cert. (2020). Building Security in Software & Supply Chain Assurance.