A Novel Algorithm for Cyber Security Analysis for Supply Chain Security

Dr. D. V. Divakara Rao (Guide), Computer Science & Engineering Department, Raghu Engineering College, Visakhapatnam, India

Chinni Lakshmi Sruthi, Computer Science & Engineering Department, Raghu Engineering College, Visakhapatnam, India

Perumalla Subba Rao, Computer Science & Engineering Department, Raghu Engineering College, Visakhapatnam, India

Misro Sasi Bhushan, Computer Science & Engineering Department, Raghu Engineering College, Visakhapatnam, India

Hemanth Kristo Doddigarla, Computer Science & Engineering Department, Raghu Engineering College, Visakhapatnam, India

ABSTRACT

The Cyber Supply Chain (CSC) system is a multifaceted system with multiple subsystems carrying out distinct functions. The inherent vulnerabilities and threats from any portion of the system that can be exploited at any point in the supply chain make supply chain security difficult. This can cause a severe disruption on the overall business continuity. Thus, it is critical for organizations to comprehend and assess the risks in order to implement the appropriate supply chain security management measures. In order to analyse and forecast the risks based on the features of Cyber Threat Intelligence (CTI), we have combined CTI with Machine Learning (ML) approaches. To demonstrate the applicability of our approach, CTI data is gathered and a number of ML algorithms, i.e., Logistic Regression (LG), Support Vector Machine (SVM), Random Forest (RF) and Decision Tree (DT), are used to develop predictive analytics using the Microsoft Malware Prediction dataset.

KEYWORDS:

Cyber Supply Chain, Malware, Cyber Threat Intelligence, Machine Learning.

1. INTRODUCTION

Security of the Cyber Supply Chain (CSC) is essential to ensuring the entire business continuity of Smart CPS and dependable service delivery. CSC systems inherently are 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). A collection of CSC attacks that take use of system vulnerabilities is presented in a recent NCSC paper. Several organizations outsource part of their business and data to third-party service providers that could lead to any potential threat. There are several examples of successful CSC attacks. For instance, Dragonfly, a Cyber Espionage group, is well known for targeting CSC organization. The Saudi Aram co power station attack halted its operation due to a massive cyber-attack. While CSC dangers and risks are taken into account in some of the existing works, threat intelligence properties are not given enough attention for the overall enhancement of cyber security.

Further, it is also essential to predict the cyber-attack trends so that the organization can take the timely decision for its countermeasure. Predictive analytics helps with situational awareness of existing supply system vulnerabilities in addition to offering insight into the TTPs, intentions, and objectives of threat actors. This paper aims to improve the cyber security of CSC by specifically focusing on integrating Cyber Threat Intelligence (CTI) and Machine Learning (ML) techniques to predicate cyber-attack patterns on CSC systems and provide appropriate countermeasures to address the assaults.

2. LITERATURE SURVEY

1.A secure Address Resolution Protocol (ARP) is suggested by Gouda and Huang (2003)in their Computer Networks study. By protecting network communications' integrity and secrecy, the protocol seeks to reduce vulnerabilities related to Cyber-attacks. By usingcutting-edge techniques to authenticate ARP messages and stop illegal changes to ARP tables,the secure ARP improves network security. Their method tackles important cyber security issues and provides a strong defence against ARP-based intrusions in computer networks.

2. A secure address resolution protocol called S-ARP is introduced in this article, which was presented in 2003 at the 19th Annual Computer Security Applications Conference. By fixing flaws in conventional ARP, S-ARP seeks to improve network security by providing strong defence against spoofing attempts. S-ARP reduces the possibility of illegal access and data interception by ensuring safe mapping between IP and MAC addresses using creative approaches. The design and deployment of S-ARP are described in depth in the article, with anemphasis on how well it protects network infrastructure against cyber-attacks. This contribution emphasizes how crucial it is to develop protocols in order to protect vital networkfunctions in a constantly changing cyber security environment.

3. RFC 903 introduces the Reverse Address Resolution Protocol (RARP), which was developed by Finlayson et al. (1984). A host can use this protocol to find its IP address by using its MAC address. RARP is an essential tool for network configuration, particularly for hosts (such as diskless workstations) that lack IP address knowledge. RARP makes it easier to manage networks and promotes smooth communication between devices on local networks by enabling devices to dynamically get IP addresses. This ground breaking study is essential to the development of current networking technology and establishes the foundation for further advances in network protocols.

4. RFC 0826, which introduces the Ethernet Address Resolution Protocol (ARP), is presented by Plummer (1982). The process for transforming network protocol addresses into 48-bit Ethernet addresses, which enable their transfer on Ethernet gear, is described in this groundbreaking paper. Because ARP dynamically maps IP addresses to MAC addresses, it isessential for facilitating communication between devices on local networks. Plummer's contribution

lays the foundation for efficient and seamless data transmission across Ethernet networks and offers a vital component of modern networking protocols.

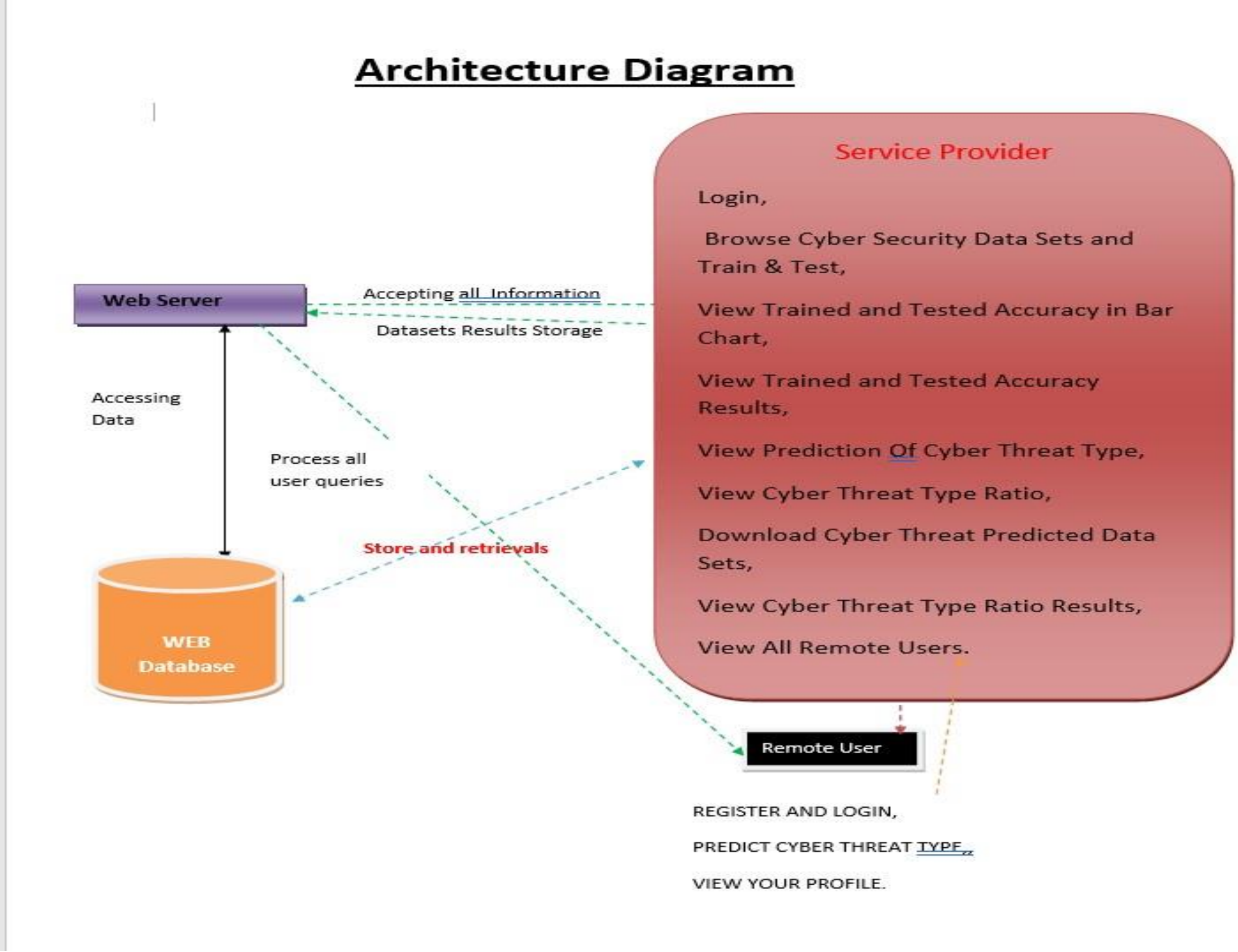
3. IMPLEMENTATION STUDY

3.1 EXISTING SYSTEM

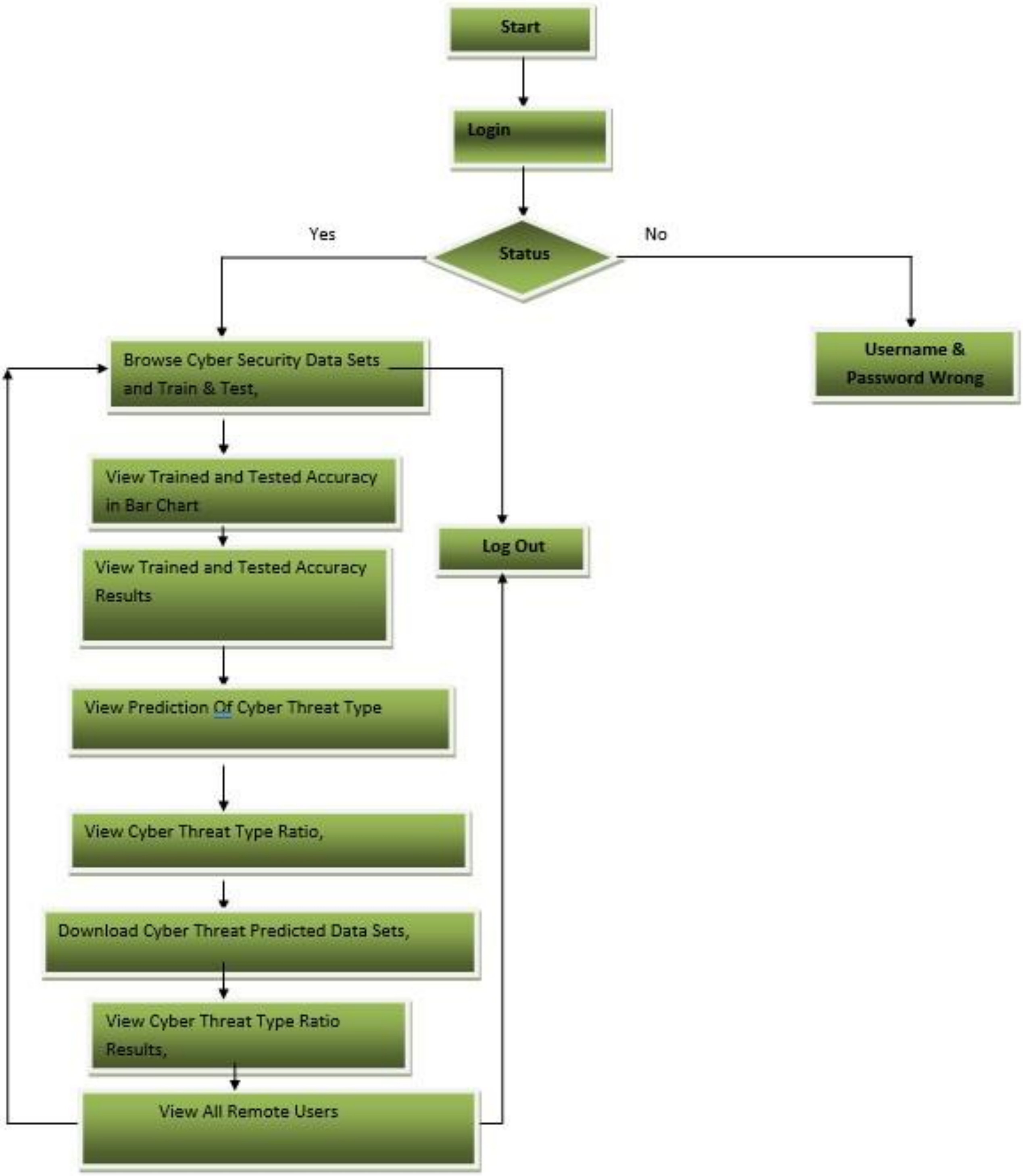
In order to accomplish the organizational objective, the CSC security offers a safe, integrated platform for the inbound and outgoing supply chain systems with third-party service providers, such as suppliers and distributors. In the context of the supply chain, cybersecurity refers to different safe product and information outsourcing between suppliers and third-party providers. Tier 1 considers the organizations CSC risk requirement strategy. Products and services in the supplier's incoming and outbound chains are taken into account when identifying risks related to the supply chain in Tier 2. Tier 3 implementation considers the risk assessments, threats analyses, associated impacts and determine the baseline requirements for governance structure.

3.2 PROPOSED SYSTEM

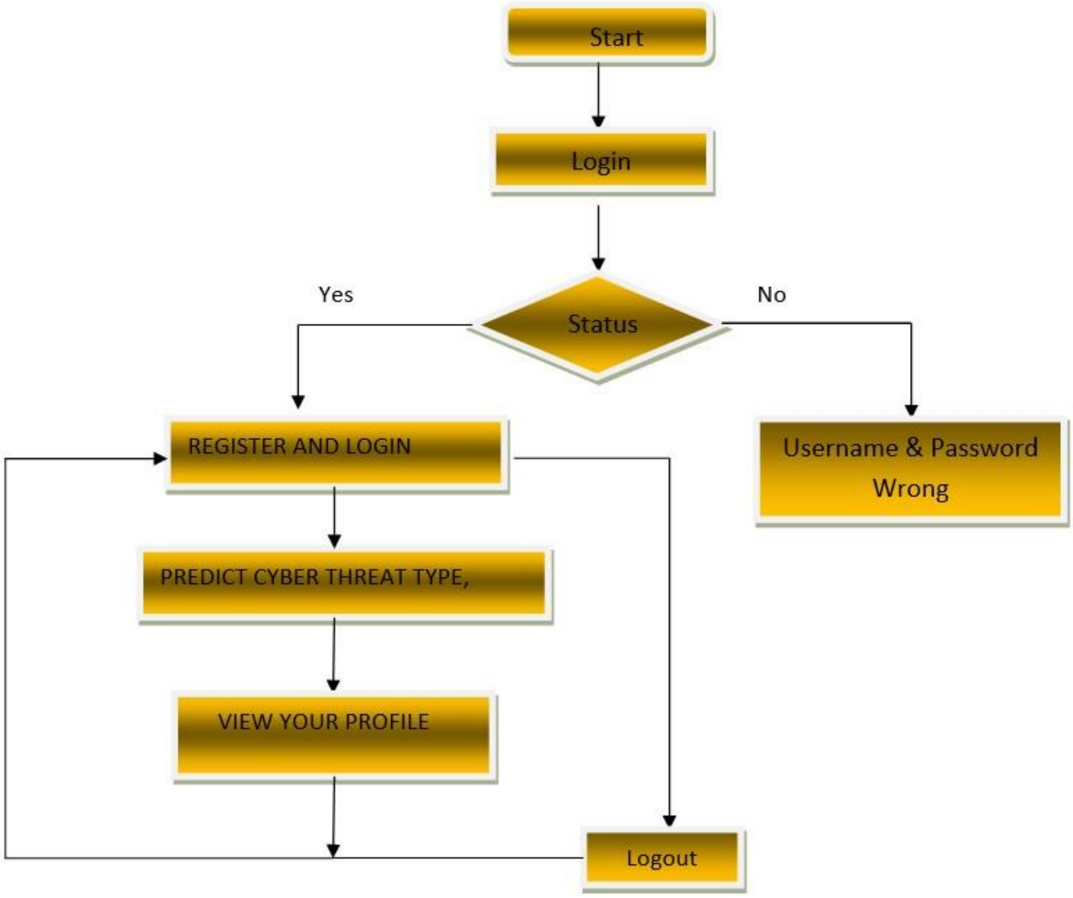
The proposed system aims to improve the cybersecurity of CSC by specifically focusing on integrating Cyber Threat Intelligence (CTI) and Machine Learning (ML) techniques to predicate cyberattack patterns on CSC systems and recommend suitable controls to tackle the attacks. First, we look at Cyber Threat Intelligence (CTI), which uses concepts like threat actor skill, motivation, IoC, TTP, and events to systematically gather and analyse information on the threat actor and cyberattack. The fact that CTI offers knowledge based on evidence regarding known attacks is the rationale for its consideration. In order to fully comprehend and reduce hazards, this information is also utilized to find previously unidentified attacks. The purpose of CTI's intelligence information is to both stop attacks and reduce the time it takes to find new ones. Secondly, we applied ML techniques and classification algorithms and mapped with the CTI properties to predict the attacks. For this, we employ a number of classification techniques, including Decision Tree (DT), Random Forest (RF), Support Vector Machine (SVM), and Logistic Regression (LG). For the purpose of predicting attacks, we adhere to CTI features such the Indicator of Compromise (IoC) and Tactics, Techniques, and Procedure (TTP). Ultimately, we utilize a popular cyberattack dataset to forecast future attacks. The prediction focuses on identifying dangers related to industrial espionage, command and control, and advance persistent threat (APT) that are pertinent to CSC. The outcome demonstrates how well CTI and ML approaches may be combined to identify weaknesses in CSC systems and anticipate intrusions. Additionally, our forecast shows that the TPR and FPR have an overall accuracy of 85%. Additionally, the outcomes show that LG and SVM generated.


Architecture Diagram
Service Provider
Login,
Browse Cyber Security Data Sets and Train & Test,
View Trained and Tested Accuracy in Bar Chart,
View Trained and Tested Accuracy Results,
View Prediction Of Cyber Threat Type,
View Cyber Threat Type Ratio,
Download Cyber Threat Predicted Data Sets,
View Cyber Threat Type Ratio Results,
View All Remote Users.
Web Server
Accepting all Information
Datasets Results Storage
Accessing Data
Process all user queries
Store and retrievals
WEB Database
Remote User
REGISTER AND LOGIN,
PREDICT CYBER THREAT TYPE,,
VIEW YOUR PROFILE.

- **Flow Chart :** Service Provider


Start
Login
Status
Yes
No
Username & Password Wrong
Browse Cyber Security Data Sets and Train & Test,
View Trained and Tested Accuracy in Bar Chart
View Trained and Tested Accuracy Results
View Prediction Of Cyber Threat Type
View Cyber Threat Type Ratio,
Download Cyber Threat Predicted Data Sets,
View Cyber Threat Type Ratio Results,
View All Remote Users
Log Out

➢ **Flow Chart : Remote User**



4. SOFTWARE AND LIBRARIES DESCRIPTION

SCAPY: Scapy is a powerful interactive packet manipulation software and library written in Python. It is a flexible tool for network investigation, testing, and troubleshooting since it enables users to create, decode, send, and record network packets at a detailed level. Users may design personalized packets using scapy for a number of different network protocols, such as TCP/IP, UDP, ICMP, and ARP. Because of its versatility and ease of use, network engineers, security professionals, and researchers appreciate it for tasks like network scanning, sniffing, and protocol exploitation. Scapy is an indispensable tool for anybody working in the subject of network security and analysis because of its vast documentation, lively community support, and ability to perform complicated networking tasks programmatically.

DJANGO: Django is a high-level Python web framework that enables rapid development of secure and maintainable websites. Django takes care of much of the hassle of web development, allowing you to focus on writing your app without needing to reinvent the wheel. It follows the Model-View-Template (MVT) design pattern, emphasizing reusability and clean, pragmatic design. With features like an ORM for database interactions, built-in authentication, and powerful template rendering, Django is widely used for creating robust web application.

Operating Systems:

Linux: Linux distributions like Ubuntu or Kali Linux are commonly used due to their robustnetworking capabilities and availability of security tools.

Windows: Windows operating systems can also be used, but may require additional setup forcertain tools and libraries.

Network Security Tools:

Wireshark: Wireshark is a widely-used network protocol analyzer, helpful for capturing andanalyzing ARP packets to detect anomalies.

Virtualization and Containerization:

VirtualBox / VMware: Virtualization platforms enable the setup of test environments forsimulating network scenarios and testing detection mechanisms.

5. 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. CPS security is still difficult, though, because any weakness in the system might put the entire supply chain at danger. Through the integration of CTI and ML for threat analysis and prediction, this research seeks to enhance CSC security. 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 predicti

6. 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. December 2017. [online]

[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/cyber-threat-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 Application Security 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.