



ISSN: 2321-2152

**IJMECE**

*International Journal of modern  
electronics and communication engineering*

E-Mail

[editor.ijmece@gmail.com](mailto:editor.ijmece@gmail.com)

[editor@ijmece.com](mailto:editor@ijmece.com)

[www.ijmece.com](http://www.ijmece.com)

# CYBER THREAT PREDICTIVE ANALYTICS FOR IMPROVING CYBER SUPPLY CHAIN SECURITY

<sup>1</sup> K. LAKSHMAN REDDY, <sup>2</sup> LAKKOJU LAKSHMI SHAILAJAKSHI

<sup>1</sup>(Associate Professor), Dept of MCA, S.V.K.P & Dr K.S. Raju Arts & Science College(A),  
Penugonda

W.G.District, Andhra Pradesh, klreddy@gmail.com

<sup>2</sup> PG, scholar, S.V.K.P & Dr K.S. Raju Arts & Science College(A), Penugonda

W.G.District, Andhra Pradesh, shailajakshi135@gmail.com

## 1.ABSTRACT

Cyber Supply Chain (CSC) 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 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 security. Cyber Threat Intelligence (CTI) provides an intelligence analysis to discover unknown to known threats using

various properties including threat actor skill and motivation, Tactics, Techniques, Procedure (TTP), and Indicator of Compromise (IoC). This paper aims 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, 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. The experiment considers attack and TTP as input parameters and vulnerabilities and Indicators of compromise (IoC) as output parameters. 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.

## 2.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). A recent NCSC report highlights a list of CSC attacks by exploiting vulnerabilities that exist within the systems [1]. Several 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 [2,3]. The Saudi Aram co power station attack halted its operation due to a massive cyber attack [1]. 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. 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 not only provide an understanding of the TTPs, motives and intents of the threat actors but also assist situational awareness of current supply system vulnerabilities.

This paper aims to improve the cyber security of CSC by specifically focusing on integrating Cyber Threat Intelligence (CTI) and Machine Learning (ML) techniques IEEE Access on machine learning, Issue Date: June.2021 to predicate cyber attack patterns on CSC systems and recommend suitable controls to tackle the attacks. The novelty of our work is three • Firstly, we consider Cyber Threat Intelligence -(CTI) for systematic gathering and analysis of information about the threat actor and cyber-attack by using various concepts such as threat actor skill, motivation, IOC, TTP and incidents. The reason for considering CTI is that it provides evidence-based knowledge relating to the known attacks. This information is further used to discover unknown attacks so that threats can be well understood and mitigated. CTI provides intelligence information with the aim of preventing attacks as well as shorten time to discover new attacks.

- Secondly, we applied ML techniques and classification

algorithms and mapped with the CTI properties to predict the attacks. We use several classification algorithms such as Logistic Regression (LG), Support Vector Machine (SVM), Random Forest (RF) and Decision Tree (DT) for this purpose. We follow CTI properties such as Indicator of Compromise (IOC) and Tactics, Techniques and Procedure (TTP) for the attack predication.

- Finally, we consider widely used cyber attack dataset to predict the potential attacks [6]. The predication focuses on determining threats relating to Advance Persistent Threat (APT), command and control and industrial espionage which are relevant for CSC [7] [8] [9]. The result shows the integration of CTI and ML techniques can effectively be used to predict cyber attacks and identification of CSC systems vulnerabilities. Furthermore, our prediction reveals a total accuracy of 85% for the TPR and FPR. The results also indicate that LG and SVM produced the highest accuracy in terms of threat predication.

The rest of the paper is organised as follows: Section 2 presents an overview of related works including CSC security, cyber threat intelligence and Machine Learning for CSC.

Section 3 provides the concepts necessary for the proposed approach and the meta model. Section 4 provides an overview of the proposed approach including the integration of CTI and ML. Section 5 presents the underlying process for the threat analysis and predication. Section 6 implements the process for the threat predication using the widely used Microsoft malware datasets. Section 7 discusses the results and compares the work with the existing works in the literature. Finally, Section 8 provides conclusion and future direction of the work.

### **3.LITERATURE SURVEY**

A comprehensive literature survey on the application of cyber threat predictive analytics for proactive cyber supply chain security involves

a meticulous exploration of a vast array of academic papers, articles, reports, and scholarly resources within the field. The primary objective of such a survey is to systematically gather and analyse existing research findings, methodologies, and insights related to the utilization of predictive analytics techniques for enhancing the detection, prevention, and mitigation of cyber threats within the intricate networks of supply chains. This endeavour requires a clear delineation of the research scope, focusing specifically on proactive security measures aimed at pre-emptively identifying and neutralizing potential cyber threats before they manifest into tangible risks for supply chain operations.

To initiate the literature survey, one must first define the key keywords and search terms relevant to the topic at hand. These may include terms such as "cyber threat predictive analytics," "proactive security," "cyber supply chain," "threat detection," "machine learning," "data mining," and others. Armed

with these keywords, researchers can then delve into renowned academic databases such as Google Scholar, IEEE Xplore, ACM Digital Library, and ScienceDirect to systematically search for scholarly articles, papers, and publications pertaining to the subject matter.

Moreover, it is essential to identify and scrutinize reputable journals and conferences that specialize in cybersecurity, supply chain management, and predictive analytics. By scouring recent issues and proceedings of these publications, researchers can unearth pertinent studies, methodologies, case studies, and experimental results that offer valuable insights into the application of predictive analytics in fortifying cyber supply chain defenses.

In the process of conducting the literature survey, researchers must meticulously evaluate the relevance, credibility, and quality of the identified sources. This involves critically analyzing the methodologies employed, the rigor of the research conducted, the

validity of the findings, and the significance of the contributions made by each study. Furthermore, researchers should pay close attention to the reference lists of relevant papers to identify additional sources and explore papers that cite the key articles already identified.

As the literature survey progresses, researchers should endeavor to organize and summarize the findings of the selected papers based on themes, methodologies, findings, or any other relevant criteria. By synthesizing the insights gleaned from the literature, researchers can gain a comprehensive understanding of the current state of research, emerging trends, and key challenges in the field of cyber threat predictive analytics for proactive cyber supply chain security.

Additionally, the literature survey should facilitate the identification of gaps in the existing research landscape and provide insights into potential avenues for future research and innovation. By critically analysing the strengths and limitations of current approaches



and methodologies, researchers can propose novel strategies, frameworks, and solutions aimed at advancing the state-of-the-art in predictive analytics for proactive cyber supply chain security.

In conclusion, a thorough literature survey on cyber threat predictive analytics for proactive cyber supply chain security serves as a foundational step in advancing knowledge, informing best practices, and guiding future research endeavours in this critical domain. By synthesizing existing research findings, identifying gaps, and proposing innovative solutions, such a survey contributes significantly to the ongoing efforts to safeguard supply chain networks against the ever-evolving landscape of cyber threats

#### **4.EXISTING SYSTEM**

The CSC security provides a secure integrated platform for the inbound and outbound supply chains systems with third party service provider including suppliers, and distributors to achieve the organizational goal [10]. Cybersecurity from supply

chain context involves various secure outsourcing of products and information between third party vendors, and suppliers [11]. This outsourcing includes the integration of operational technologies (OT) and Information technologies (IT) running on Cyber Physical Systems (CPS) infrastructures. However, there are threats, risks and vulnerabilities that are inherent in such systems that could be exploited by threat actors on the operational technologies and information technologies of the supply inbound and outbound chains systems. The outbound chain attacks include data manipulations, information tampering, redirecting product delivery channels, and data theft. The IT risks include those attacks on the cyber physical and cyber digital system components such as distributed denial of service (DDoS) attacks, IP address spoofing, and Software errors [12]. Regarding CSC security, NIST SP800 [13] proposed a 4 tier framework approach for improving critical infrastructure cybersecurity that

incorporates the cyber supply chain risk management framework into it as one of its core components. Tier 1 considers the organizations CSC risk requirement strategy. Tier 2 considers the supply chain associated risk identifications including products and services in the supply inbound and outbound chains. Tier 3 implementation considers the risk assessments, threats analyses, associated impacts and determine the baseline requirements for governance structure. Tier 4 consider real time or near-time information to understand supply chain risk associated with each product and service. However, the approach and tiers considered risks management but did not emphasize on ML and threat prediction for future trends in the CSC attack patterns that structured and codifies supply chain attacks. The goal of the framework was to provide a comprehensive view of supply chain attacks of malicious insertion across the full acquisition lifecycle to determine the associated threat and vulnerability information.

## DISADVANTAGES

- 1) Existing works that consider CSC threats and risks but a lack of focus on threat intelligence properties for the overall cyber security improvement. Further, it I also essential to predict the cyberattack trends so that the organization can take the timely decision for its countermeasure.
- 2). There is no technique called Inbound and Outbound Supply Chain to detect cyber threat.

## 5.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. The novelty of our work is threefold:

- Firstly, we consider Cyber Threat Intelligence(CTI) for systematic gathering and analysis of information about the threat actor and cyber-attack by using various



concepts such as threat actor skill, motivation, IoC, TTP and incidents. The reason for considering CTI is that it provides evidence-based knowledge relating to the known attacks. This information is further used to discover unknown attacks so that threats can be well understood and mitigated. CTI provides intelligence information with the aim of preventing attacks as well as shorten time to discover new attacks.

- Secondly, we applied ML techniques and classification algorithms and mapped with the CTI properties to predict the attacks. We use several classification algorithms such as Logistic Regression (LG), Support Vector Machine (SVM), Random Forest (RF) and Decision Tree (DT) for this purpose. We follow CTI properties such as Indicator of Compromise (IoC) and Tactics, Techniques and Procedure (TTP) for the attack predication.

- Finally, we consider widely used cyberattack dataset to predict the potential attacks [6]. The predication focuses on determining threats relating to Advance Persistent Threat (APT), command and control and industrial espionage which are relevant for CSC [7] [8] [9]. The result shows the integration of CTI and ML techniques can effectively be used to predict cyberattacks and identification of CSC systems vulnerabilities. Furthermore, our prediction reveals a total accuracy of 85% for the TPR and FPR. The results also indicate that LG and SVM produced the highest accuracy in terms of threat predication.

### **ADVANTAGES**

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

### **6.ARCHITECTURE**

System Architecture mainly consist s of 2 modules and database to store all the data .Those are:

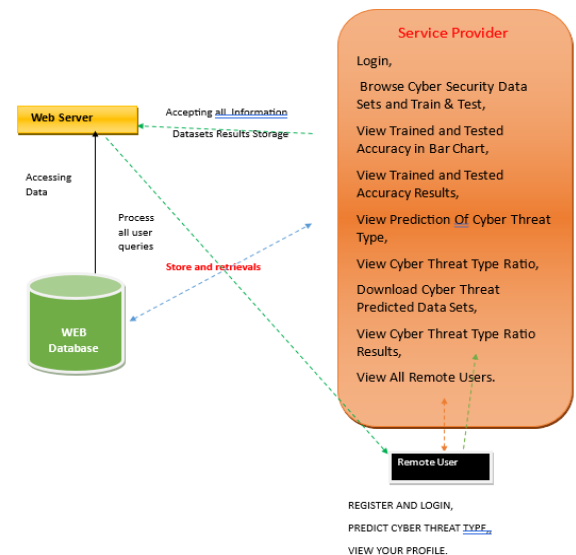
- Remote User
- Service provider

The Remote User module can perform the following operation: Register and login, view your profile, Predict Recommendation Type

The Service provider module can perform the following operations:

Login, Browse and Train &Test data sets, View Trained And tested Accuracy in Bar Charts, view Trained and Tested Accuracy Results, View Predicted Water Quality Type Ratio, Download Trained data sets, view Water Quality ratio results.

### Architecture Diagram



## 7.MODULES

### SERVICE PROVIDER

In this module, the Service Provider has to login by using valid user name and password. After login successful he can do some operations such as 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.

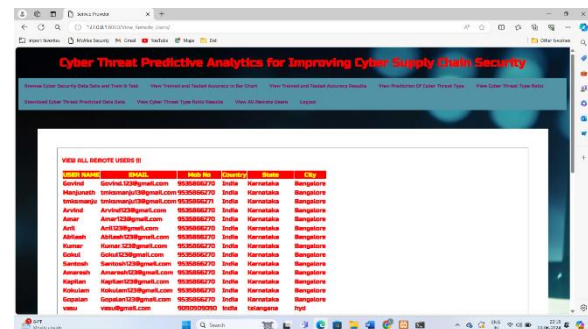
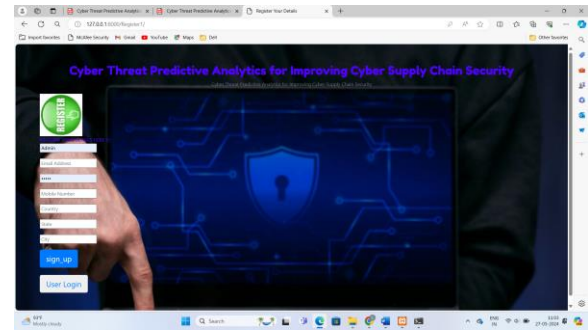
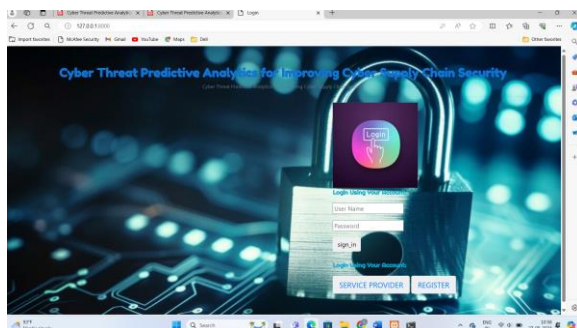
## VIEW AND AUTHORIZE USERS

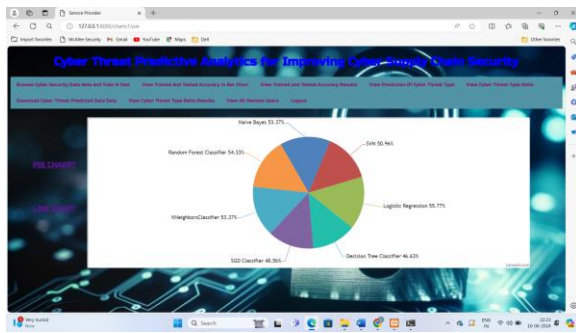
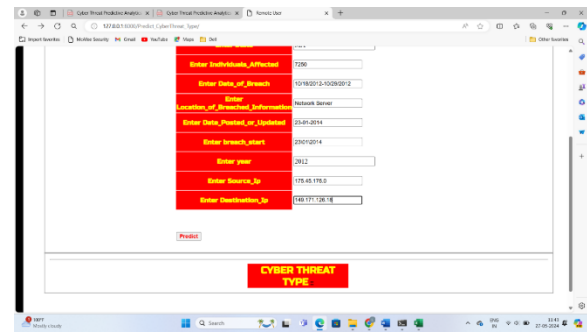
In this module, the admin can view the list of users who all registered. In this, the admin can view the user's details such as, user name, email, address and admin authorizes the users.

## REMOTE USER

In this module, there are n numbers of users are present. User should register before doing any operations. Once user registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password. Once Login is successful user will do some operations like REGISTER AND LOGIN, PREDICT CYBER THREAT TYPE, VIEW YOUR PROFILE

## 8. OUTPUTSCREENS



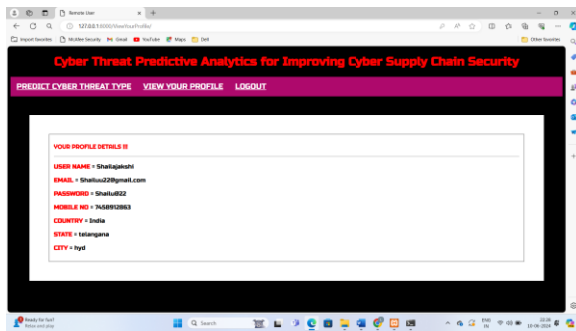



**PREDICT CYBER THREAT TYPE**

Form Fields:

- Enter Individuals\_Affected
- Enter Date\_of\_Breach
- Enter Location\_of\_Breach
- Enter Date\_Predicted\_or\_Updated
- Enter Severity\_Level
- Enter Year
- Enter Source\_IP
- Enter Destination\_IP

**Predict**

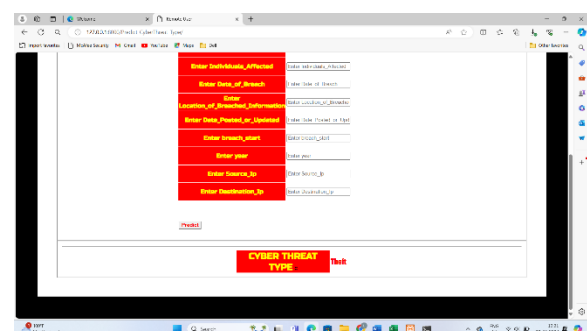


**Cyber Threat Predictive Analytics for Improving Cyber Supply Chain Security**

**PREDICT CYBER THREAT TYPE VIEW YOUR PROFILE LOGOUT**

**YOUR PROFILE DETAILS II**

USER NAME : ShalikaGauti  
 EMAIL : Shalika22@gmail.com  
 PASSWORD : Shalika22  
 MOBILE NO : 9898989898  
 COUNTRY : India  
 STATE : Telangana  
 CITY : Hyderabad



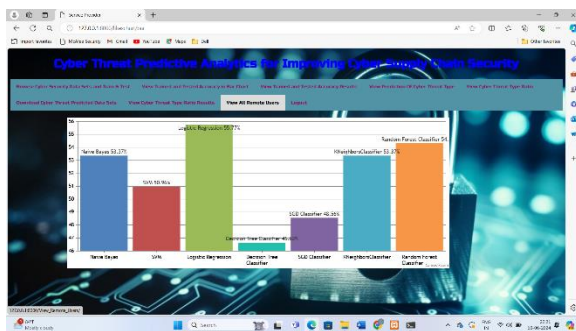
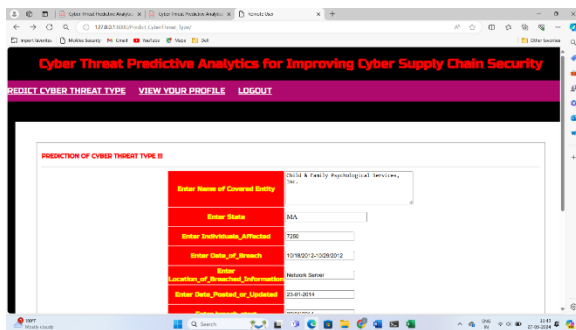
**PREDICT CYBER THREAT TYPE**

Form Fields:

- Enter Individuals\_Affected
- Enter Date\_of\_Breach
- Enter Location\_of\_Breach
- Enter Date\_Predicted\_or\_Updated
- Enter Severity\_Level
- Enter Year
- Enter Source\_IP
- Enter Destination\_IP

**Predict**

**CYBER THREAT TYPE Risk**

**Cyber Threat Predictive Analytics for Improving Cyber Supply Chain Security**

**PREDICT CYBER THREAT TYPE VIEW YOUR PROFILE LOGOUT**

**PREDICTION OF CYBER THREAT TYPE II**

Form Fields:

- Enter Name of Connected Entity
- Enter State
- Enter Individuals\_Affected
- Enter Date\_of\_Breach
- Enter Location\_of\_Breach
- Enter Date\_Predicted\_or\_Updated

**Predict**

**CYBER THREAT TYPE Risk**

## 9. 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.

## 10.REFERENCE

[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](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>. [11] R. D. Labati, A. Genovese, V. Piuri and F. Scotti, "Towards the Prediction of Renewable Energy Unbalance in Smart Grids," 2018 IEEE 4th

International Forum on Research and Technology for Society and Industry (RTSI), Palermo, Italy, 2018, pp. 1-5, doi: 10.1109/RTSI.2018.8548432. [12] J. Boyens, C. Paulsen, R. Moorthy, and N. Bartol, "Supply Chain Risk Management Practices for Federal Information Systems and Organizations". NIST Computer. Sec. 2015, SP800, 1, doi:10.6028/NIST.SP.800. [13] NIST 2018 "Framework for Improving Critical Infrastructure Cybersecurity" National Institute of Standards and Technology. Ver. 1.1. <https://doi.org/10.6028/NIST.CSWP.04162018>. [14] J. F Miller, "Supply Chain Attack Framework and Attack Pattern". MITRE Technical Report. MTR140021. 2013. [Online] Available: <https://www.mitre.org/sites/default/files/publications/supply-chain-attack-framework-14-0228.pdf>. [15] C. Ahlberg, C. Pace, "What Are the Phases of The Threat Intelligence Lifecycle?" The Threat Intelligence Handbook. A Practical Guide for Security Teams to Unlock the Power of Intelligence. CyberEdge Group.

LLC. Annapolis MD. USA. 2018.

[16] J. Freidman, and M Bouchard, "Definition Guode to Cyber Threat Intelligence. Using Knowledge About Adversary to Win The War Against Targeted Attacks." iSightPartners.CyberEdge Group LLC. Annapolis, MD. USA 2018.

[17] EY. Cyber Threat Intelligence: Designing, Building and Operating an Effective Program. 2016. [Online] Available: <https://relayto.com/ey-france/cyber-threat-intelligence-report-js5wmwy7/pdf>.

[18] A. Yeboah-Ofori and C. Boachie, "Malware Attack Predictive Analytics in a Cyber Supply Chain Context Using Machine Learning," 2019 International Conference on Cyber Security and Internet of Things (ICSIoT), 2019, pp. 66-73, doi: 10.1109/ICSIoT47925.2019.00019.

[19] B. Gallagher and T. Eliassi-Rad. "Classification of HTTP Attacks: A Study on the ECML/PKDD 2007 Discovery Challenge". Lawrence Liverpool National Laboratory (LLNL) Livermore, CA. 2009. doi.org/10.2172/1113394. [20] D. Bhamare, T. Salman, M. Samaka, A.

Erba and R. Jain. "Feasibility of Supervised Machine Learning for Cloud Security" 3rd International Conference on Information Science and Security. IEEE Xplore. 2016. DOI: 10.1109/ICISSEC.2016.7885853.

[21] A. L. Buczak, and E. Guven. "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection". IEEE Communications Surveys & Tutorials. Vol. 18. NO. 2, 2nd Quarter. 2016. DOI: 10.1109/COMST.2015.2494502 [22] O. Yavanoglu and M. Aydos. "A Review of Cyber Security Dataset for Machine Learning Algorithms" International Conference on Big Data, IEEE Xplore. Jan 2018. DOI: 10.1109//BigData.2007.8258167.

[23] E. G. V. Villano. "Classification of Logs Using Machine Learning" M. S. Thesis. Norwegian University of Science and Technology. Norway. 2018 [24] R. C. Borges Hink, J. M. Beaver, M. A. Buckner, T. Morris, U. Adhikari and S. Pan, "Machine learning for power system disturbance and cyber-attack



discrimination," 2014 7th International Symposium on Resilient Control Systems (ISRCS), Denver, CO, USA, 2014, pp. 1-8, doi: 10.1109/ISRCS.2014.6900095. [25]

A. Gumaei, M. M. Hassan, S. Huda, Md. R. Hassan, D. Camacho, J. D. Ser, G. Fortino, "A robust cyberattack detection approach using optimal features of SCADA power systems in smart grids." Elsevier Science Direct. Applied Soft Computing, Vol. 96,106658, Nov. 2020, doi.org/10.1016/j.asoc.2020.106658.