Enhancing Cyber Supply Chain Security through Prophetic Analytics for Cyber Threats

K. NAVEEN
B TECH CSE
(Dr MGR EDUCATIONAL AND RESEARCH INSTITUTE, CHENNAI)
Chennai, TAMIL NADU
Kommineninaveen0@gmail.com

A. LAL KRISHNA CHOWDARY
B TECH CSE
(DR MGR EDUCATIONAL AND RESEARCH INSTITUTE ,CHENNAI)
Chennai, TAMIL NADU
lalkrishnachowdary@gmail.com

G.RAJESH
B TECH CSE
(Dr MGR EDUCATIONAL AND RESEARCH INSTITUTE ,CHNNAI)
Chennai, TAMIL NADU
venkatarajesh756@gmail.com

Mr S. NARAYANAN
Assisant PROFESSOR
(Dr MGR EDUCATIONAL AND *RESERCH INTITUTE CHENNAI)*
TAM IL NADU
Narayanan.cse@drmgrdu.ac.in

Dr V. SAI SHANMUGA RAJA
PROFESSOR
(Dr MGR EDUCATIONAL AND RESERCH INTITUTE CHENNAL)
Chennai, TAMIL NADU
saishanmugaraja.cse@drmgrdu.ac.in

Dr G. GUNASEKARAN
PROFESSOR
(Dr MGR EDUCATIONAL AND RESERCH INTITUTE CHENNAL) Chennai,
Chennai, TAMIL NADU
gunasekaran.cse@drmgrdu.ac.in

ABSTRACT: The Cyber Provide series system a multifaceted system with a multiple subsystems carrying out distinct functions. The potential weaknesses and risks originating out of a segment and arrangement that will manipulated at some stage in the provide series. make supply chain security difficult As a result, it is critical for organizations to comprehend and assess the risks in order to implement the appropriate supply chain security management measures. Using machine learning (ML) techniques in conjunction with cyber threat intelligence (CTI), we have been able To examine and predict potential risks using the characteristics of CTI. This makes it possible to pinpoint the innate CSC vulnerabilities and implement the proper countermeasures for an overall increase in cyber security. In order to show the practicality of our method, we collect CTI data and use the Microsoft viruses forecast dataset to produce prophetic investigation using several machine learning (ML) algorithms, The test considers the pounce and TTP as capture variable, while the measures of compromise and vulnerabilities are considered as output parameters, incorporating Decision Tree, Random Forest, Support Vector Machine.

KEY WORDS
Cyber Supply Chain; Cyber warning surveillance; Predictive Analytics, Cyber Safety, Tactical Methods Process

I.INTRODUCTION

Security of the Cyber Supply series is essential to make sure entire business continuity of Smart CPS and dependable service delivery. Due to their intrinsic complexity, CSC systems might have vulnerabilities that spread There are multiple target nodes within the large cyber physical system to which data is transmitted from a source node. numerous instances of CSC attacks that are effective. For example, it is commonly known that the cyber espionage outfit Dragonfly targets CSC organizations. We utilize machine learning to predict assaults since malware infections have cascading consequences and Cyberattacks targeting the cyber supply chain (CSC) are unstoppable. The growing reliance of businesses on CSC systems is crucial for their uninterrupted operations. has led to a corresponding rise in threat landscapes and vulnerabilities. Traditionally, antivirus software, such as Various security measures, such as spam filters, firewalls have been employed to detect and prevent virus attacks. These tools work well enough, but as threat actors become more skilled, they may manipulate nodes on systems, which spreads the infection. we train the dataset using machine learning techniques in order The objectives are to forecast the identification of CSC nodes and determine their vulnerability to cyber attacks, as well as anticipate future trends. The data utilized for this analysis was obtained from the Microsoft viruses forecast website. to show how our method is applicable. In addition An ensemble is employed to connect the SVM, Logistic Regression algorithms in large part Voting. The algorithms are executed on the training data, and 10-fold cross verify is utilized to validate the parameter estimation, precise results, and predictions. The results illustrate the application of decision tree techniques in machine learning algorithms for cyber supply series prophetic analytics, enabling the identification and analysis of potential risks. forecast patterns in upcoming cyberattacks.

II. LITERATURE SURVEY:

[1] ABEL YEBOAHOFORI , SHAREEFUL ISLAM2, SINWEELEE2, ZIA USH SHAMSZAMAN, "Cyber Threat Predictive Analytics for Improving Cyber Supply Chain Security",2021

Globally, the amount of renewable energy produced is rising. Predicting power production from renewable energy sources effectively is required to integrate them into electrical smart networks that can adjust to variations in power demand in heterogeneous local zones. These forecasts can be used to schedule the output of non-renewable energy facilities in order to distribute the generated power appropriately and offset any imbalances that may occur. Predicting the imbalance at the local level (zones) The SVM, Decision Tree, algorithms combined implement Majority Voting. These outcome demonstrate the utilization of decision tree techniques in machine learning algorithms for cyber supply series prophetic analytics, facilitating the identification and analysis of potential risks.is very crucial. In this work, we suggest an innovative approach an innovative technique for forecasting the direction and imbalance in middle of the capacity generated by renewable the local capacity intake, taking into account areas with a variety of characteristics and multiple power plants. The approach makes use of a collection of old characteristics that can figure out how historical facts and power imbalance in diverse geographic areas relate to one another. We used data gathered over a seven-month period by a participant in the energy market as a case study to assess the suggested approach. In this pilot study, we assessed many iterations of the suggested approach, yielding outcomes deemed acceptable by an energy market participant

[2] Theresa Sobb, Benjamin Turnbull and Nour Moustafa" Cyber Threat Predictive Analytics for Improving Cyber Supply Chain Security"2020

We utilize machine learning to predict assaults since malware infections have cascading consequences and cyberattacks on the CSC systems are impervious. The growing reliance of enterprises on CSC systems is crucial for maintaining business continuity. has led to a corresponding rise in threat landscapes and vulnerabilities. These techniques are often successful, risks that could be taken advantage of in this research, using machine learning approaches. Predicting. What are the resilient mechanisms against cyberattacks, and what are our future goals? to show how applicable our strategy was. Moreover, the SVM, Decision Tree, and Logistic Regression algorithms are connected through the use of Majority Voting. To ensure reliable results and predictions, these algorithms are trained on data and their parameter estimation is verified using 10-fold cross validation. Thus, this work demonstrates the use of decision tree machine learning algorithms to cyber supply chain predictive analytics for threat detection and forecasting

3.Kaushal Ramesh bhai Patel, "Enhancing Cyber Supply series Security through Predictive Analytics for Cyber Threats" 2023

Although cloud computing is becoming more and more popular, security remains the largest obstacle to widespread use. Users of cloud services are constantly concerned about issues with availability, security lapses, and data loss. With in advancement of machine learning techniques, learning-based approaches for security applications have been more and more prominent in the literature lately. But getting unbiased, real-time datasets is a big problem for these techniques. A lot of internal datasets could not have the necessary statistical properties or cannot be released because of privacy concerns. Because of this, scientists tend to create datasets which might not be entirely comprehensive for use in confined or simulated experimental environments for testing and training reasons. When using models of machine learning are trained in to one dataset, the outcomes and their applications typically have different semantic meanings. Few studies have been conducted that show how well these models perform when applied to various datasets collected in various contexts. We contend that testing the machine learning models' robustness is essential, particularly under the varied operating conditions that are common in cloud situations. In this work, the supervised machine learning is trained using the UNSW dataset. models. Next, we use the ISOT dataset to test these models. We discuss our findings and make the case that further machine learning research is still necessary before it can be applied to cloud.

III. REQUIRMENT ANALYSIS

3.1 Introduction

The crucial stage of the system development process is system analysis. The System is examined and examined in great detail. The system analyst delves deeply into how the current system functions and takes on the crucial role of an interrogator. Analysis entails a thorough examination of these system functions as well as the connections between them both inside and outside the system. One important query addressed here is, "What steps need to be taken to solve the problem?" After analysis is finished, the analyst knows exactly what has to be done.

A collection of CSC attacks that take use of system vulnerabilities is presented in a recent NCSC paper. Businesses delegate some of operations to outside providers who may pose a risk to the company. There are numerous instances of CSC attacks that are effective. A significant cyberattack forced the Saudi Aramco power plant to shut down. Existing research takes into account CSC risks and threats, but it doesn't concentrate enough on threat intelligence characteristics to improve cyber security as a whole.

example, it is commonly known that the cyber espionage outfit Dragonfly targets CSC organizations. A significant cyberattack caused the Saudi Aramco power plant to shut down. 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.

First, we look at Cyber Threat Intelligence (CTI), which uses concepts like threat actor skill, motivation, IoC, TTP , and events to systematically gather and analyze 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. The purpose of CTI's intelligence information is to both stop attacks and reduce the time it takes to find new ones. We employ a number of classification techniques, In the realm of machine learning algorithms, Random Forests, Support Vector Machines, and Logistic Regression (LG) are widely utilized for various tasks. ***3.2 HARDWARE REQUIREMENTS:*** Hardware interfaces define the logical properties of each interface that a software product has with the system's hardware elements. The hardware specifications are as follows.

• Operating systems: Linux and Windows

• Processor: Intel i3 minimum

• Hard disk: minimum 250 GB; minimum RAM of 4 GB

3.3 Software requirements outline the logical properties of each interface and the software that makes up the system. Here are a few specifications for the software.

• Version 3.7 of Python Idel (or)

• Jupiter (or)

• Anaconda 3.7 (or)

• Google Collab

IV DESIGN

4.1 PROJECT ARCHITECTURE

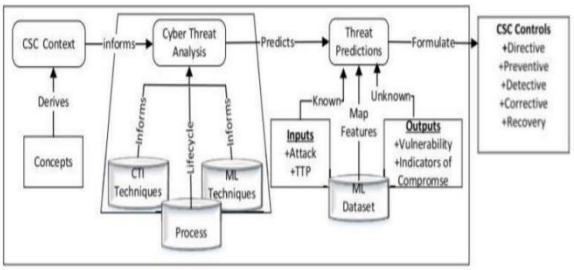


Figure 4.1: Project Architecture

Gathering and consuming data It is necessary to get and consume data from multiple sources. This comprises information gleaned from publicly

accessible sources, vendors, the company's internal network, and outside threat intelligence feeds.

4.2 Preprocessing and cleaning:

raw data is frequently necessary to guarantee consistency and dependability while working with raw data. Data normalization, addressing missing values, and combining data from many sources and formats may all be part of this process.

4.3 Data Administration and Storage:

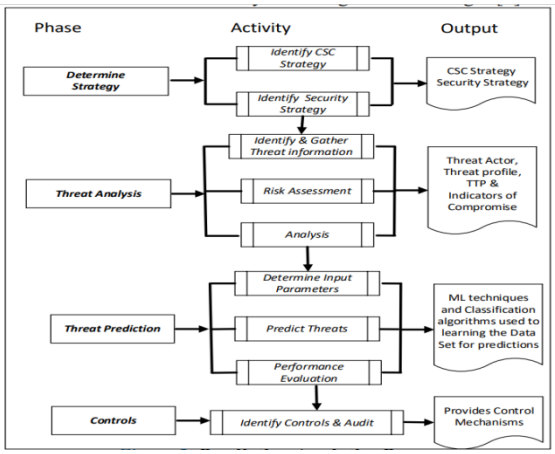
A scalable and secure data repository—a data warehouse, data lake, or big data platform—is where data is kept safe. To preserve data security and integrity, appropriate data governance procedures are necessary.

4.4 Feature Engineering and Extraction:

From the gathered data, characteristics important for predicting cyber threats are taken out or created.

4.5 ANALYSIS:

In order to identify the true source of the attack, its type, its pattern, its TTP, and its attack vectors, this task center on analyzing the warning. This will help identify the necessary controls and the IoC.



4.6 THREAT PREDICATION:

Using three consecutive actions, the phase merge CTI and ML to prevent attack forecast of familiar and hidden assaults, taking into account CSC system nodes that are susceptible to cyberattacks. Establish input parameters, forecast threats, and assess performance

4.7 CONTROL:

Finding record of power to address the warning is target of this last stage. The controls ought to guarantee that the necessary security mechanisms and strategies are implemented in order to lessen the risks. This covers determining the necessary security measures, conducting internal and external audits, and keeping an eye on and reporting on threats. Information exchange comes last in the process, followed by the identification and evaluation of current controls and third-party audit.

V. RESULT

Nonetheless, the CPS's security continues to be a problem because any flaw in the system might put the supply chain at risk. In order to improve CSC security, this article employs CTI and ML to identify and anticipate possible risks before they materialize. To evaluate and forecast the threat, we applied CSC and CTI concepts along with a systematic methodology. We discovered that CTI is helpful in obtaining threat intelligence, which may be utilized in machine learning classifiers to forecast the probability of a specific threat. This makes it possible for the CSC organization to assess the security measures that are in place at the moment and find new ones that may be added to improve overall cyber security. Furthermore, we found that CTI is a useful tool for extracting threat intelligence that can be included into machine learning classifiers to predict threats. This makes it possible for the CSC organization to evaluate the current controls and identify new ones that will enhance overall cyber security. To generalize our results, an industrial case study and complete process automation are required. In addition, based on the outcomes of our predictions, we want to take into account assessing the current controls and the requirement for further controls in the future.

IV.REFERENCE

1.Yeboah-Ofori and. Islam_ cyber security threat modelling for supply chain organizational environment" MDPI.FUTURE INTERNET, .Mar.2019

2.Woods and A.B0chman,_supply chain in the software era, "in Scowcroft enter for strategic and security Washington, DC ,USA: Atlantic council, may 2018

3.Exploring the opportunities and Limitations of current Threat Intelligence Plat from, version 1,ENISA,DEC.2017

4.Research Prediction, (2019), Microsoft Malware Predation, [online]

5.lqbal H. sacker" Intelligent Data Analysis and Automation in Cybersecurity" in 2022