Cyber resilience in supply chain system security using machine learning for threat predictions

Cyber Resilience in Supply Chain System Security Using Machine Learning for Threat Predictions

[1]Abel Yeboah-Ofori, [2]Cameron Swart, [3]Francisca Opoku-Boateng, [4]Shareeful Islam
[1]School of Computing & Engineering, University of West London, London, W5 5RF, UK,
[2]School of Mathematics, Computer Science and Engineering, City, University of London.
[3]College of Computer & CyberScience, Dakota State University, Dakota, USA
[4]School of Computing & Information Science, Anglia Ruskin University, Cambridge, UK
[1]abel.yeboah-ofori@uwl.ac.uk; [2]cameron.swart@city.ac.uk; [3]francisca.opoku-boateng@dsu.edu;
[4]shareeful.islam@aru.ac.uk

Abstract
Purpose - Cyber resilience in cyber supply chain (CSC) systems security has become inevitable as attacks, risks, and vulnerabilities increase in real-time critical infrastructure systems with little time for system failures. Cyber resilience approaches ensure the ability of a supply chain system to prepare, absorb, recover, and adapt to adverse effects in the complex CPS environment. However, threats within the CSC context can severely disrupt the overall business continuity. The paper aims to use machine learning techniques to predict threats on cyber supply chain systems, improve cyber resilience, focus on critical assets, and reduce the attack surface.
Design/Methodology/Approach - The approach follows two main cyber resilience design principles that focus on common critical assets and reduce the attack surface for this purpose. Machine Learning (ML) techniques are applied to various classification algorithms to learn a dataset for performance accuracies and threats predictions based on the CSC resilience design principles. The critical assets include Cyber Digital, Cyber Physical and physical elements. Second, we consider Logistic Regression, Decision Tree, Naïve Bayes, and Random Forest, Neural Network classification algorithms in a Majority Voting to predicate the results. Finally, we mapped the threats with known attacks for inferences to improve resilience on the critical assets.
Finding - That paper contributes to CSC system resilience based on understanding and predicting the threats. The result shows a 70% performance accuracy for the threat prediction with cyber resilience design principles that focus on critical assets and controls and reduce the threat.
Research Limitations/Implications - There is a need to understand and predicate the threat so that appropriate control mechanisms and actions can be implemented to ensure system resilience. However, there are limited controls and attributions due to the invincibility and dynamic nature of cyberattacks. Thus, posing severe implications to cyber supply chain systems and their cascading impacts.
Implications - There are no social implications; instead, it has severe impacts on organizations and third-party vendors.
Originality/Value - The paper's originality is that cyber resilience design principles that focus on common critical assets are used to determine the attack surface, including Cyber Digital, Cyber Physical and Physical Elements. Machine Learning (ML) techniques are applied to various classification algorithms to learn a dataset for performance accuracies and threats predictions based on the CSC resilience design principles to reduce the attack surface for this purpose.

Keywords: Cyber Resilience, Cyber Supply Chain, Cyber Security, Cyber Threat Prediction. Machine Learning

Paper Type: Research Paper

1. Introduction

Cyber supply chain (CSC) systems are complex by their inherent nature due to the interdependencies among multiple systems and networks nodes from different organizations. Cyber-attack in any part of the network can cascade to the other network nodes and poses any potential risk to the overall business continuity. Additionally, organizations may face unpredicted risks despite security in all phases of a supply chain, for which no mitigation strategies have been planned in advance. Cyber resilience in CSC plays an important role in ensuring system reliability and overall business continuity. It is the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stress, attacks, or compromises on cyber resources [1], [2]. CSC requires a mature level of cyber resilience capability to tackle the disruption and regenerate its performance after a cyberattack. However, understanding the threats and achieving an optimal level of resilience in all parts of CSC is a challenging task. The threats landscape is constantly evolving and highly uncertain. An attack can originate from any part of the supply chain and cascade to the other part, making it prohibitively difficult to conduct a risk assessment. Due to unexpected threats and a lack of incident handling capability in place, that could lead to significant business interruption. Cyber resilience in the CSC domain is still in the early stage. Therefore, it is necessary to develop a knowledge base to understand cyber resilience, features, principles to determine the required controls.

The paper aims to improve cyber resilience on cyber supply chain systems security using machine learning techniques to predict threats, focusing on critical assets, and reducing the attack surface. Our work provides an overview of resilience strategies applicable for the CSC context and determines the controls required to achieve a

mature level of resilience. The novelty of our work is threefold. Firstly, we consider the necessary concepts required to understand the cyber resilience of the CSC context. These concepts, i.e., actor, goal, asset, attack surface, incident, IoC, CSC requirements, are considered from several relevant domains, including CSC, cyber resilience, and threat. The paper's contribution to CSC system resilience, based on understanding the threat landscape and predicting the threats. We follow the two main resilience design principles, i.e., Focus on common critical assets and reduce the attack surface for this purpose. Secondly, we have applied Machine Learning (ML) techniques on a dataset to analyse and predict the threats based on the CSC resilience design principles. A widely used cyberattack data set is used to predict from Microsoft Malware Prediction [3]. We consider the performance accuracies of Logistic Regression (LR), Decision Tree (DT), Random Forest (RM), Naïve Bayes (NB), and Neural Networks (NN) classification algorithms in a Majority Voting (MV) to predicate the results. Finally, we mapped the threats with known attacks for inferences and determined the controls required to improve resilience on the critical assets. The ML predictive analysis determines a 70% performance accuracy for the threat predictions. The result shows that it is necessary to consider the critical cyber resilience design principles that focus on critical assets to improve overall CSC resilience.

2. Related Works

This section discusses the state of the art in cyber resilience and related works in cyber supply chain security systems. MITRE 2015 defines cyber resilience as the ability of cyber systems and cyber dependent missions to anticipate, continue to operate correctly in the face of, recover from and evolve to better adapt to advanced cyber threats [2]. Cyber resilience in cyber supply inbound and outbound chains are in the early stage due to the evolving nature of critical infrastructure systems and their integrations in the cyber physical systems environment. Omera et al. 2015 define supply chain cyber resilience as the capability of a supply chain to maintain its operational performance when faced with cyber risk [4]. Omera et al. 2015 created a plan for future research in supply chain resilience by identifying models and frameworks that can incorporate the dimensions of cyber risk and cyber resilience [4]. Bodeau et al. 2016 present observations about cyber resilience metrics drawn from experience, workshop sessions, and literature that could help those seeking to define cyber resilience [5]. The authors considered cyber resilience from five perspectives: systems of systems, mission of the systems of system, the CERT resilience management, critical infrastructure sectors mission supports with a collaborative system of systems and transnational enterprises supported by a virtual system of system. MITRE proposes a cyber resiliency framework and provides information that systems engineers and architects can help us as guidance when deciding which cyber resiliency techniques to apply [6]. Linkov & Kott 2018 refers to cyber resilience as the systems' ability to prepare, absorb, recover, and adapt to adverse effects, especially those associated with cyberattacks. The cyber resilience components constitute a bridge between hardware, software, and sensing for sustaining system operations while ensuring mission execution [7]. MITRE 2017 presented a representative set of cyber resilience design principles and described factors used in selecting a set appropriate to a given system in different degrees throughout the system lifecycle [8]. These principles include security, resilient engineering, survivability and evolvability [9].

2.1 Machine Learning

Machine learning is a technique used in the cybersecurity domain to predict cyberattack trends impact and the probability of fraudulent activities. It uses a supervised learning approach to accurately predict system performance using the dataset to train and test the classification algorithms. Mohasseb et al., 2019, used ML techniques and Naive Bayes and SVM algorithms on various datasets collected from SMEs for classification accuracies and predictive analytics on cyber security incidents [10]. Bilge et al. 2017, used ML techniques to propose a risk teller system to build a risk prediction model that analysis binary file appearance logs of machines to predict which devices are at risk of getting infected or clean by Malware in advance [11]. Yavanoglu et al. (2017) used machine learning techniques to analyze network traffic and detect abnormalities [12]. Hink et al. (2014) explored the viability of machine learning for power systems disturbance and cyberattack discrimination methods. They focused specifically on detecting cyberattacks where deception is the core tenet of the event [13]. Gallagher et al. (2009) proposed a vector space ML model for predicting attacks by identifying malicious codes embedded in incoming HTTP requests and eradicating bad requests at points before their processing [14]. Morris et al. (2014) explored the suitability of using various ML methods on different classification algorithms to predict discriminating disturbances in power systems [13]. Sharma et al. (2007) used ML techniques and SVM algorithms to detect variants of known worms in real-time systems and used unnormalized bi-gram frequency counts as input [15]. Bhamare et al. (2016) analyzed the performance classifications of major supervised learning algorithms with different datasets in a simulated cloud environment for cloud security [16].

Supervised learning considers using a dataset that includes input and outputs parameters for performance accuracies and prediction during training and dataset for testing. Regression algorithms are used to predict continuous response values by utilizing knowledge of existing data to predict an outcome from new data. ML can predict the cyberattack instances, cost of impact, asset value and cost of alternative and probability of fraudulent actions. We briefly discuss the various algorithms used, including LR, RF, DT, NB, NN classifiers, and MV. Logistic regression is a classification algorithm in ML that predicts the binomial probability of a categorical binary variable [17] and estimates the relationship between one dependent variable and one independent variable. Decision trees are an efficient nonparametric method that can be applied to classification or regression tasks. They are hierarchical data structures for supervised learning whereby the input space is split into local regions to predict the dependent variable [18]. Naive Bayes classification works by calculating the probability of a data point not

belonging to each class after repeating this for every class. The lowest value is selected, smallest value probability is whether an instance does not belong to the class, meaning that the highest probability class relation is selected at the end. Neural Networks algorithms consist of a collection of iterations to transform a set of desired outputs through a set of simple processing units or node and connections between them [31]. Majority Voting (MV) algorithm that is used to verify that a prediction satisfies a majority in a given list of outcomes [19], [20] determine the highest number or percentage representation in a list of algorithms.

All these works are relevant and contribute well to improving ML predictions in cyber supply chain security. However, the works do not predict treats in response to cyber resilience. Further, the works are limited as they do not support cyber resilience techniques and control mechanisms in the event of system failures. Therefore, the proposed approach contributes to addressing these limitations.

3. Approach

The approach considers cyber resilience design principles that focus on common critical assets and reduce the attack surface for this purpose. ML techniques are applied to various classification algorithms to learn a dataset for performance accuracies and threats predictions based on the CSC resilience design principles. The critical assets identified include cyber digital, cyber physical and physical elements. We consider LR, DT, NB, and RF algorithms in an MV to predicate the results. Finally, we mapped the threats with known attacks for inferences to improve resilience on the critical assets.

3.1 Background of Cyber Resilience and Threat Prediction for CSC

Cyber Resilience is essential for any CSC system based on the assumption that cyber security may fail, but the critical functions should continue their operation. A CSC system interconnects various organizations network nodes and some components to align their goal, actors, assets, processes and objectives with third party organizations, suppliers, consumers and partners [21]. Therefore, it is necessary to understand the main cyber resilience components and adopt the relevant ones for the CSC. Mitre published a list of cyber resilience design principles relevant to any system [8].

3.2 Cyber Resilience Design Principles

Cyber resilience design principles are from both strategic and structural aspects. The strategic design aspect focuses on establishing and analyzing all supply chain stakeholder entities throughout the supply inbound and outbound chains lifecycle from strategic, tactical, and operational perspectives. The strategic design aspect is applied throughout the system engineering process, including methodologies and frameworks that guide the engineering analysis directions. The rationale is to determine how well the principle is reflected in the architecture, design, technical, techniques, implementation and synergies required for business processes. The structural aspect considers the CSC system infrastructures, design software, network technology, and topology and how they directly affect the various integrations and interactions among the system components that ensure interoperability. The purpose is to align the various infrastructure designs that support the requirements, business processes, implement constraints and prevent possible conflicts among the entities.

The strategic and structural design principles are relevant in cyber supply chain systems due to the various integrations that make up the architecture and the designs. The strategic design aspects are applied from the requirements capturing phase. They are analyzed at every stage of the systems lifecycle by the strategic committee that oversees the systems development. The structure design aspects are implemented based on each organisation's various architectures and deployment. We discuss the various principles as follows [5], [22].

- **Focus on common critical assets**: An organizational CSC system integrates part of its core assets to other organizations, third-party vendors, suppliers, and distributors in supplier inbound and outbound chains. These are the integration and computation of embedded systems and physical components such as cyber digital (software), cyber physical (infrastructures/hardware) and the physical element (humans). The threat actor may wish to exploit the vulnerabilities on stakeholder systems to access the main organization using RAT, cross site scripting and island-hopping attacks. Therefore, the focus is to identify common critical assets and access, analyze, and evaluate all vulnerable spots for strategic management imperative and decision-making.
- **Support agility and architectural adaptability:** Due to evolving organizational goal, global competition, market expansion, mobile banking, and 24/7 online sales and services in real-time, CSC systems supports information dissemination and transaction platforms and are required to be able to adapt to these changing trends else the system becomes obsolete. The CSC architectural design must be interoperable, evolvable, integrable, and available to ensure adaptability and resilience and to support the agility of the cyber digital, cyber physical and physical elements.
- **Reduce attack surface:** A key principle in cyber resilience is to ensure the CSC survival instinct during system errors, failure, compromises, and zero-day attacks. That requires utilizing inventory tools throughout the CSC system to automate all software documentation on the various business application systems. Further, mechanisms are required to utilize active discovery tools to identify devices connected to the network and update the inventories of all stakeholder hardware assets. Furthermore, an audit trail is required from all stakeholders to ensure CSC system auditing and situational awareness. Finally, risk identification and assessment capabilities are required to provide preventive controls and mitigations measures to reduce the attack surface.

- **Assume compromised resources:** Due to the invincibility of cyberattacks, the uncertainty, and the cascading impact on the CSC, the organization must carry out cyber threat intelligence gathering to understand attack patterns and attack vectors. These include penetration testing, vulnerability assessment and attack modelling on the supply chain systems to implement control mechanisms, constraints, and configurations in line with international standards. In addition, understanding Advanced persistent threats (APT) and command & control (C&C) and the various attack vectors provide the organization trustworthiness and information assurance.
- **Expect adversaries to evolve**: As the CSC system evolves, so are the threat landscape, threat actor motive, intents, and methods. For example, threat actors deploy the following five evolving attack methods to affect the systems: Penetrate CSC, deploy APT methods, deploy stealthy attacks, take C&C and obfuscate. Therefore, the organization must carry out cyber security threat analysis using attack modelling benchmarks and concepts such as organization goal, security goal, TTP, CSC requirements and threat analysis to understand adversaries' motives, intents and methods. That will be used to evaluate the probability of attacks, attack patterns and their cascading impact to determine the indicators of compromise (IoC) and threat information sharing.

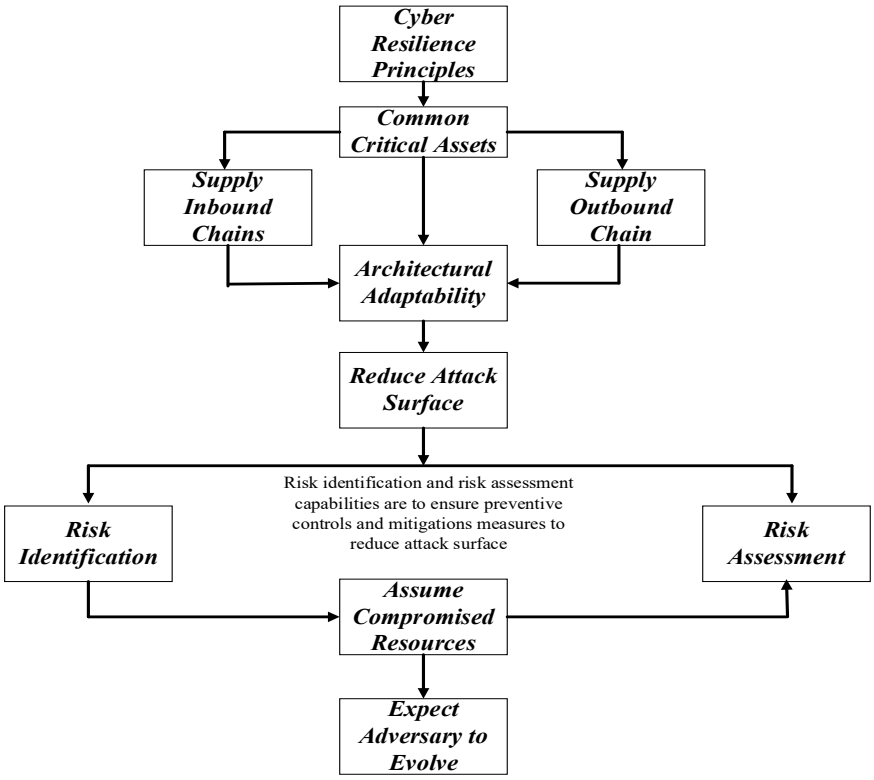


Figure 1. Principles of Cyber Resilience Approach

3.3 Threat Analysis and Prediction

Threat predictions consider input and output parameters as features to determine the attacks surface. Therefore, one of the significant challenges of Microsoft Edge antimalware includes the volume of data that needs to be analyzed to detect potential threats. The antimalware product generates millions of data to be analyzed in real-time and executes over 600 million computers worldwide.

Our work aims to use ML to predict known and unknown attacks to improve cyber resilience. First, the known attacks are derived from the dataset [3]. The Microsoft Malware Prediction dataset consists of known malware attacks representing various categories of attacks from different machine identifies. Furthermore, malware developers introduced polymorphism to the malicious components to evade detection [23]. Therefore, the known attacks are first identified from the large dataset and are categorized according to the machine identifier and a country identifier. Further, the classification criteria of the known attacks will be mapped to the ML and the classified CSC assets for predictive analytics of the unknown attacks.

Furthermore, we use ML techniques on various classification algorithms to learn datasets to determine performance evaluation and predictive analytics. The threat prediction for analytic monitoring and defence response relating to cyber resilience techniques provides an understanding of existing controls required for cyber resilience. That is relevant for cyber resilience and provide a comprehensive CSC security strategy and control mechanisms. The approach uses a causal process to identify the concepts for the organizational goal, analysis, threat prediction, controls, and information sharing. The threat prediction objective is to support predictive analytics using machine learning techniques on various classifications algorithms to learn datasets for future cyberattack trends and resilience.

3.4 Machine Learning Algorithms

This section discusses the ML classification algorithms used for our work, including LR, DT, RF, NB, NN and MV and their implementation processes.

- **Logistic Regression (LR)** classification algorithms are used to predict the binomial probability of binary variables such as "Yes or No", "True or False and "1or 0" [17]. It is used to describe the estimations of a relationship between a dependent and independent variable. LR performs best on large sample sizes of a dataset. LR provides a regression method solving binary classification problems in instances where multiple classes are presented in a target variable. For example, in cyberattack predictions, LR can predicate whether a dataset with antivirus, botnet or spam variables can predict a probability that it has detection or no detection during training and learning [31] [32].
- **Decision Tree (DT)** classifier provides an efficient nonparametric method for applying supervised learning for classification and regression [18] [32] methods to discover patterns in large and complex data for threat predictions. Hierarchical data structures are used to determine the dependent variable for the input space and split into local sections for supervised learning to predict the trends. The DT model is built as a tree-like structure from the top and down. It uses splitting, pruning, and turning the branch nodes into leaf nodes for the tree selection [19] to classify attack instances by plotting each attribute to its root. The branches of the tree are split down into subsets representing possible values for the attributes of output, and each leaf represents a decision. The DT inference process starts at its root and proceeds to the left [33] [34].
- **The Random Forest (RF)** algorithm is used to build predictive models using an ensemble with a set of decision trees classifiers that grows randomly in a selected sub-sample of a dataset [19]. It uses averaging to reduce the learning model's variances through biases-variance and tradeoffs to prevent overfitting in the data classifications. RF classifiers depend more on robust features and not wholly on how many noise variables are present [35]. Each tree in the ensemble is built from a sample drawn from the split with each replacement node from the training sets during construction. The sample size is usually controlled using the maximum sample parameter if the bootstrap default is set as true. Else, the whole dataset is used to build each data tree during training and testing sets [36].
- **Naive Bayes (NB)** algorithm uses a group of probabilistic classifiers and pairs of features based on the Bayes Theorem [38]. NB models are built based on prior assumption that the features of the input dataset of each classifier are considered independent. The models are built on the probabilistic classifiers of an object and effective on large and complex datasets. Change in a value of a feature does not affect the other. NB algorithms can multiply the likelihood of all variables during the training dataset to learn and indicate the conditional probability of the evidence [37] [39].
- **Neural Networks (NN)** algorithms are used in ML to learn datasets and recognize the pattern of behaviours during training and testing. NN concepts are adapted to identify and classify network activities based on limited, incomplete and non-linear data sources related to network security [30] [31]. NN consist of subsets of inputs and outputs using connected nodes to recognize patterns and identify attack instances where rules are not set. Furthermore, NN can automatically learn the coefficients in data inputs and outputs for more accuracy. In the cybersecurity domain, NN algorithms are recognized as an alternative to statistical components of anormally detection systems [30] [31]. Thus, NN performs better in detecting anormally, probable misuse and is reliable compared to other classifiers.
- **Majority Voting (MV)** algorithm is used to verify that a prediction satisfies a majority in any given list of outcomes [34]. MV algorithm determines values that are more than half in a dataset and have the highest number or percentage representation in a list of algorithms. The purpose of the ensemble method is to combine several algorithms in a pipeline to train and test the classifiers for the predictions within a given learning algorithm to improve the performance accuracies.

We have used these ML techniques on classification algorithms to learn a dataset for performance accuracies and predictions. The results show different performances based on the model classifier.

4. Cyber Resilience Modelling for the CSC Systems

This Section presents the proposed approach for CSC resilience. The proposed approach consists of a modelling view to understanding the domain and a systematic threat prediction and resilience assurance process.

4.1 Framing concepts CSC Resilience

This Section considers the conceptual model of the cyber supply chain security resilience system. These concepts and their properties provided us with an in-depth understanding of the CSC cyber resilience systems [20].

- Goal: Goals are high level statements of intended outcomes, which helps an organization scope the resilience domain [2]. The goal of an organization determines the nature of assets required for the business process and describes the objectives. Goals are realized by different factors based on the organizational objectives and business processes [21], [24]. Yu (2011) posits that a goal represents a condition in the world that an actor would like to achieve [21], [24].

- Assets: assets are those infrastructures that are key to business continuity and information assurance and ensure resilience operations to support business operations. These critical infrastructures and resources are both cyber digital and physical and span across all sectors of the economy [21]. Critical assets in the cyber resilience context consider the cyber digital, cyber physical, and physical (human) elements of CPS.
- Actor: An actor's concept includes identifying the various systems users in the CSC environment to ensure the goal is attained or aborted [21]. The actor's properties are the type, internal user, external user, system user, threat actor.
- CSC Requirements: The CSC requirements consider the various functional and non-functional requirements gathered to determine how the business functions and the constraints required to support the stakeholders and business goal. The requirements concepts include properties such as organizational, business, systems, user, and operational requirements.
- Incident: Incidents are the various instances of cyberattacks, including penetrations and manipulation deployed on the CSC. The threat actors use TTPs, various attack patterns and attack vectors to deploy attacks and cause exploits in cyberattack campaigns. The properties of the incident include type, date, source, and severity.
- Attack surface: The Attack surface considers the various routes the threat actor could exploit on the supply chain environments. Understanding the attack surface and how the attacks can be deployed provides cyber threat intelligence and situational awareness on minimizing the attack surface to ensure resilience.
- Indicators of compromise (IoC): are artefacts used to indicate that an incident or event has occurred or is in progress in the supply chain system and needs an urgent response. The traditional approach to identifying IoCs are through IDS/IPS, firewalls and Antivirus.
- Threat Information Sharing: The threat information sharing platform provides the information necessary to assist an organization in identifying, assessing, monitor, and responding to cyber threats [25]. The platform provides a medium for all the CSC stakeholders to independently provide threat information of system artefacts, observable patterns and vectors for correlation, threat intelligence gathering, analysis and sharing [25].
- Risks (with subclass residual risks): Risk is the probability of some error, failure or an attack occurring on the supply chain. CSC risk is high as every stakeholder represent a single point of failure. The potential for the threat actor to maliciously introduce unwanted functions, subvert the system's design, product, or Integrity and sabotage the system are high [26], [27].
- Cyber Course of Actions: Cyber courses of action (CCoA) consider a set or sequence of cyber incident response plans (CIRP) and security controls employed by automation and actors in response to cyber incidents. CCoA could be used to gather CTI that provides an understanding of a set of actual cyber incidents and courses of action that anticipates and address potential threats.

Resilience Feature Considers the critical assets integrated on the supply inbound and outbound chains, including critical functions and threshold. The focus is on identifying common critical assets and assessing, analyzing, and evaluating all vulnerable spots for strategic management imperative and decision-making. The properties include critical asset, adaptability, attack surface, and evolving threat landscape.

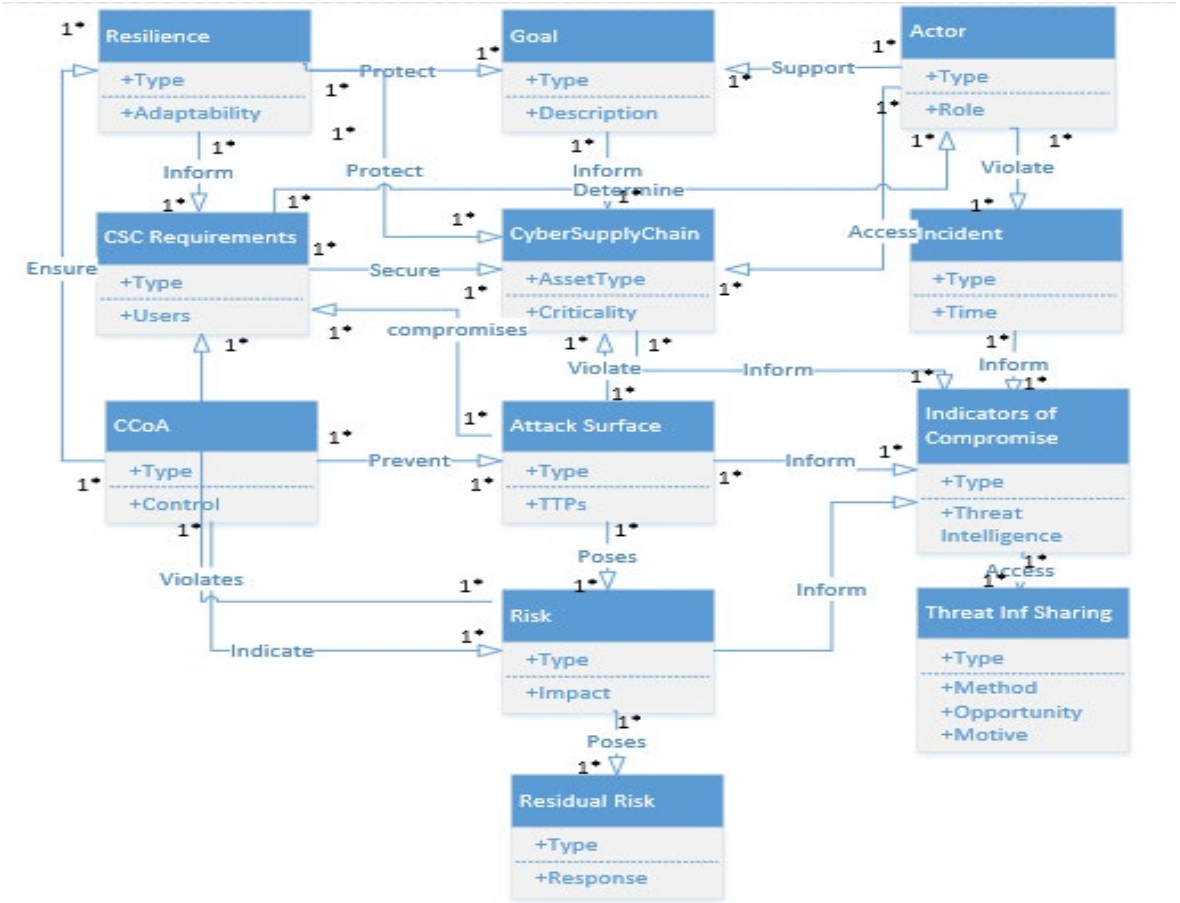


Figure 2. Cyber Resilience Conceptual Model

4.2 Machine Learning Process

This Section presents the overall process for CSC resilience. The method includes sequential phases, and each stage includes necessary steps to support the phase, as shown in Figure 3.

Phase 1: Identification and Analysis of Critical Assets

Critical assets are those infrastructures that are key to business continuity and information assurance that ensure resilience operations to support business operations. Critical assets in the cyber resilience context consider the cyber digital, cyber physical, and physical (human) elements of the CSC system vital to the economy and business growth. Critical assets include infrastructures that generate a complete system by integrating many devices, sensors, and actuators for information dissemination in real-time [21]. The CSC components integrate the Cyber digital, physical, and physical elements in a supply chain environment.

- The cyber digital integrates the embedded systems' software, computational and industrial control systems process that makes a complete system.
- The cyber physical components include the hardware, network architecture, wireless, topologies and communication protocols with Intelligence Electronic Devices (IED), router, and switches that support the distributed control systems.
- The physical elements include linking physical and human elements such as devices, monitors, sensors, and actuators for information sharing [28].
- The cyber digital and the cyber physical integrates to provide intelligence devices to provide services. Cyber attackers with political motives may target these critical infrastructures and attack the core levels where communication occurs or the supporting infrastructure where intelligent components, including controlling and monitoring, occur [21], [29].

Phase 2: Threat analysis and predication

The threat analysis and prediction consider Machine learning techniques on various classification algorithms to learn a dataset for predictive analytics. We consider dataset presentation and description, the feature selection process, performance evaluation and prediction. We follow the steps below out the process.

4.3 Microsoft Malware Prediction Dataset

The data set was collected from a publicly available data source from a Microsoft Malware Prediction website [3]. The dataset is about malware attacks in the Microsoft endpoint system, and such a system can be a critical part of

the CSC security and overall business continuity. The dataset was designed to meet certain business constraints regarding the privacy and period used by a machine. The data set containing these properties and the machine infections were generated by combining threat reports collected by Microsoft Endpoint Protection Solution, Windows Defender. The data was collected by Microsoft Windows Defender with over 40,95488 entries, with 62 columns, and each row represents different telemetry data entries. The data represent malware attacks identified on various endpoint nodes from different countries, with different machine identities, timestamps, organizational identifiers, and default browser identifiers designed to meet various business requirements. Each row in the dataset corresponds to a machine uniquely identified by a machine Identifier. The dataset integrates other systems using other operating systems that only represent Microsoft customer's machines. It has been sampled to include a much larger proportion of malware machine infections.

The objective of using the data set was that cyber supply chain systems interconnect other organizations, third parties' vendor's networks for business process and data flows and adaptability in the supply chain domain. Furthermore, CSC integrates various organizational systems for information dissemination in the CPS environment. Hence, the dataset is relevant for our work as it was gathered from global machines that used Microsoft Windows Defender.

The rationale for using the dataset for our work is that it does not represent Microsoft customer's machines only as it has been sampled to include a much larger proportion of malware infection machines. Therefore, we used this dataset for our predictive analytics as CSC systems integrate various network infrastructures for interoperability and business processes. The attack categories were determined from the dataset of different threat descriptions from the telemetry data that contains the properties of the various families of Malware generated by the Windows defenders.

Activity 1: Data Preparation

The activity involves uploading the dataset from the Microsoft Malware Prediction website [3]. The data was converted based on the average of the dataset columns. Furthermore, we loaded the data from a pre-prepared dataset by calling the categories of the machine learning identifier: Handling NaN (Not a Number) in the training set by using a command that removes all the NaN in the training set into the dictionary and prints the output. Furthermore, we create a NaN dictionary to handle all the unwanted duplicate data. The output generated 4095488 training datasets with 78 variables.

Activity 2: Feature Selection Process

Feature selection activity involves using different techniques to select the available features in the data for applying the ML algorithms. These feature selection techniques include dimensionality reductions in large datasets for practical and reliable training, testing and prediction. Figure 3 identifies all the features and their relative importance to the dataset and feature selection. It shows that of all the features listed, AvSigVersion_2 determines the antivirus version installed on each system with a feature importance score of 69. The antivirus products identified for the specific configuration of the user's antivirus software is the highest and is protected as it is a calculated field derived from the Spynet Report's AV Products field. The last indicates how secure the organization system is when the operating system boot is enabled. Random forest feature selection has been used to determine the most relevant features for prediction, using the Sklearn library, which provides random forest classifiers and selects from model functions. That allows us to transform the training and testing using the selected features provided by the random forest algorithm. In our case, the optimum number of features is 32.

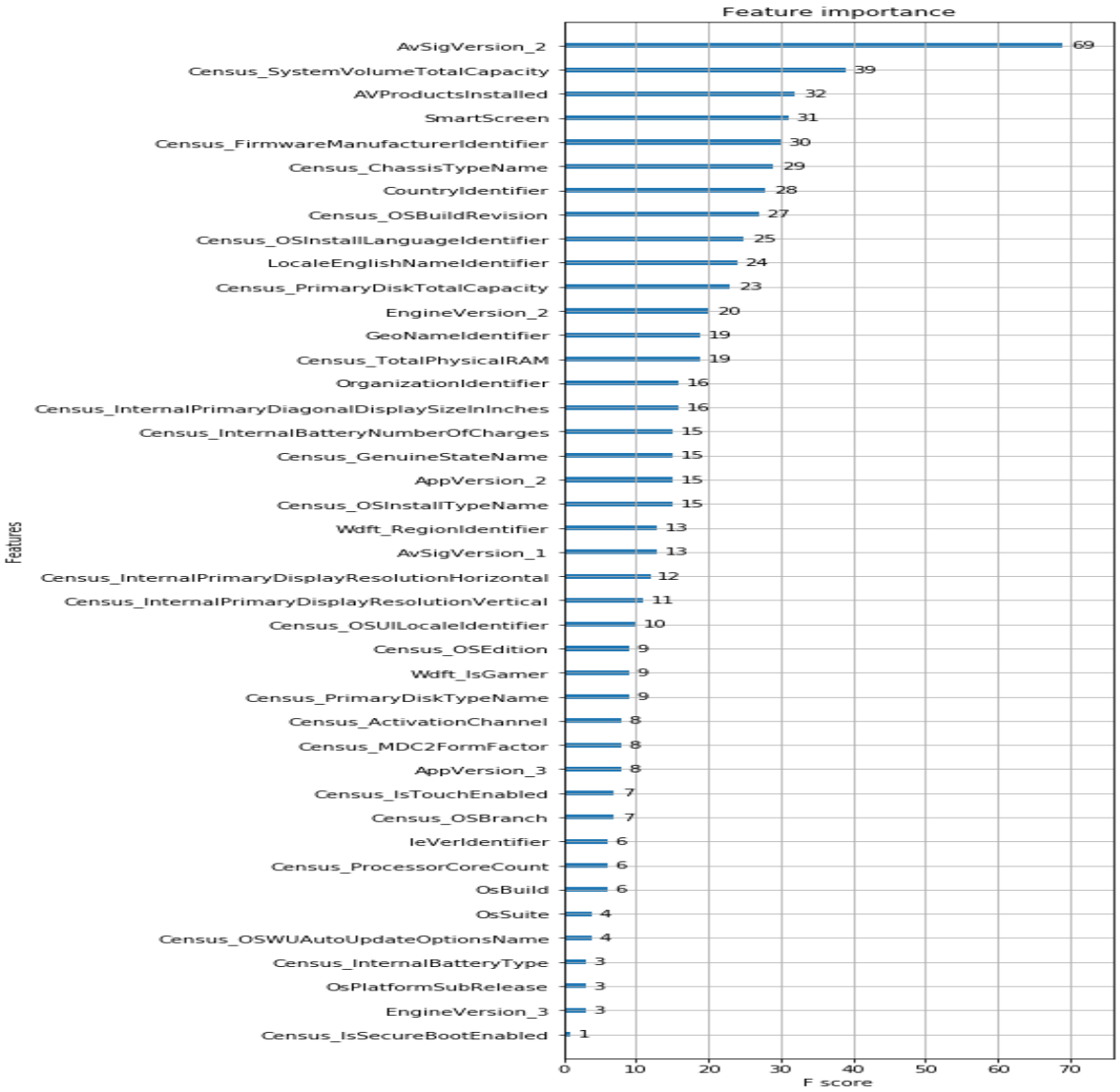


Figure 3. Feature Importance for the Dataset

4.4 Feature Importance

Feature importance determines the relevance of the features used for the ML. Feature importance provides a score for each dataset feature using inbuilt classifications. The highest score indicates how important or relevant the feature is towards the output variable. For example, the features in Figures 3 and 23 represent descriptions of the different telemetry data entries of Microsoft Windows Defender protection information and threat reports gathered from various endpoint nodes [3]. Determining the relevance of the features impacts the feature selection process and contribute to achieving better performance accuracy for the model. In addition, it assists in removing irrelevant features and improves the performance of the models when learning and training the dataset.

The Microsoft Windows Defender protection report includes properties of the types of Antiviruses installed, the disk organizational identifier, antivirus version, the operating system, country identifies, machine identities, timestamps, and default browser identifier designed to meet various business requirements [3].

Activity 3: Performance evaluation

The performance accuracies determine the performances of the different classifications' algorithms. First, we determine the various algorithms used for our prediction. For our study, we use binary classification as it supports the AUC-ROC in distinguishing between the probabilities of the given classes. Further, its precisions can predict correct instances, provide a harmonic mean of precision and recall for the F-score.

AUC-ROC (Area Under Curve – Receiver Operating Characteristics) is a binary classifications metrics used to determine the True Positives Rates (TPR) and True Negatives Rates (TNR) and the trade-off between sensitivity and specificity instances. ROC curve depicts a graphical way to express how the performance of the classifier changed over all the possible classification thresholds [19]. It determines the best possible outcomes of the model by distinguishing the given classifiers in terms of their predictive probabilities. The TPR and TNR should be close to 100% for better predictive analytics and best accuracy. The activities include Import AUC-ROC function, Import Mean Absolute Error, Import Mean Square Error, and Set Entropy Criterion. The equation used

for the accuracy is determined by the percentage scores of the accurately classified instances. The instances use for the accuracies are true positives (TP), false positives (FP), false positive (FP) and false negatives (FN) and are calculated as (TP+TN) / (TP + FN + FP + TN). We consider the following method to understand the confusion matrix. The accuracy of the confusion metric is the proportion of the total number of predictions considered accurate. We use the following equation below to determine the TPR, TNR, FPR, and FNR [19]. The precision determines the total predictive outcomes of positive instances predicted correctly. The instances of the accuracies are based on the following classifications for the model predictions [19] [20].

Accuracy

$$Accuracy\ AC = \frac{\#\ of\ correct\ prediction\ (TP+TN)}{\#\ of\ predictions\ (TP+FP+TN+FN)} \quad (1)$$

True Positive Rate (TPR)

$$TPR\ = \frac{TP}{FN+TP} \quad (2)$$

Precision (P) determines as correct the proportion.

$$P\ = \frac{TP}{TP+FP} \quad (3)$$

Recall (R) determines the correctly predicted positives

$$P\ = \frac{TP}{TP+FN} \quad (4)$$

F-Score determines the harmonic mean of P and R.

$$F = 2\ \frac{Precision\ x\ Recall}{Precision+Recall} \quad (5)$$

Activity 4: Choosing Optimization Algorithm

The optimization algorithm identifies each object's major features or class levels. That depends on the class it corresponds to when it was defined at the start. The algorithms used in work include Naïve Bayes, Support Vector Machine (SVM), Random Forest Classification and Majority Voting (MV). We used the ensemble to combine the algorithms and test the dataset on each to determine the accurate prediction and best results. We used the K-Fold classifier for supervised learning. The activities include:

4.5 Cyberattack Prediction Patterns

Predicting cyberattack patterns in a CSC environment is challenging due to the lack of visibility, uncertainties and ambiguities of cyber threats and the phenomenon surrounding its cascading impacts and effects on other network nodes. We predict cyberattacks using attack properties, penetrations tools, vectors, and the capability of the attack. Furthermore, we use the outputs to understand the attack patterns, vulnerable spots, TTPs and the cascading effects for the ML to predict known and unknown attacks for future predicting. The attack pattern requires carrying out reconnaissance on the supply chain system to determine vulnerable spots that are exploitable. For instance, the adversary could gain access when there are poor constraints and server misconfigurations on the system.

To predict an attack, we need to determine the known and unknown attacks. Known attacks include Malware, Spyware, Ransomware and RAT attacks. These are the known attacks that could be identified. However, unknown attacks are cybercrimes committed after the attacks. Here, after they gain access using the known attacks, the attacker, using APT and C&C to commit cybercrimes such as manipulation during development and altering and changing delivery channels. The extent of these cybercrimes manipulations and the cascading impact are unknown and unquantifiable. Therefore, the ground truth in the CSC environment is determined using a supervised learning approach objectively on known attack datasets and features to train the dataset.

5. Implementation

This section follows the experiment process to implement the ML predictions of malware infections on CSC systems. The known attacks are derived from the ML dataset and features.

5.1 Dataset Description

data preparation concepts to identify known and unknown attacks by Microsoft Defender endpoint protection [3] with over 4095488 entries. The data set containing these properties and the machine infections were generated by combining threat reports collected by Microsoft Endpoint Protection Solution, Windows Defender [3] in section 5.9.3 for the data description. The features were 78 columns, and each row represents different telemetry data entries. The data represent malware attacks identified on various endpoint nodes from different countries, with different machine identities, timestamps, organizational identifiers, and default browser identifiers designed to meet various business requirements. Each row in the dataset corresponds to a machine uniquely identified by a machine Identifier. The dataset integrates other systems using other operating systems that only represent Microsoft customer's machines. It has been sampled to include a much larger proportion of malware machine infections.

5.2 Feature Selection Process

This section identifies features from the primary dataset that are relevant to our work. There were 78 features in the primary data, and the NANs were removed. Secondary data was generated from the primary data by identifying the features we classify as probable threats for our ML profiles. First, we consider concepts of attacks and threat actors from our previous work. We were able to describe threat actor actions, types of attack tools, capabilities, motives, intent, and historically noted behaviour through this. The reason for this was to ascertain recent threats that could be deployed. Further, we identified eight vulnerable spots and their probability that the cyber attacker could exploit those spots. The purpose is to predict the probability that windows machines would get infected by various families of malware attacks based on the properties of the machine.

5.3 Building Attacks Profiles for the ML Prediction

The primary objective of this study is the construction of attack profiles for the ML to predict which network node is vulnerable and likely to be attacked on the cyber digital, cyber physical, and physical/human elements. In addition, the CSC requirements are to build resilience that will ensure privacy, prevent malicious attacks, and detect intrusions.

Table 1. Critical Assets in Cyber Supply Chain Systems

Cyber Digital	Cyber Physical	Physical/Human Elements
Software	Hardware	Sensors
Data	Infrastructures	Monitors
Cloud	Network Topologies	Humans
Internet	SCADA	Monitors
Computational systems	Intelligent Electronic Devices (IED)	Actuates
Embedded Systems	Communication Protocols	Routes/Switchers

The cyber digital and the cyber physical integrates to provide intelligence devices to provide services. Cyber attackers with political motives may target these critical infrastructures and attack the core levels where communication occurs or the supporting infrastructure where intelligent components, including controlling and monitoring, occur [21], [29].

- The cyber digital components include software, data, cloud, internet, computational and industrial control systems process of the embedded systems that make a complete system.
- The cyber physical components include the hardware, architecture, wireless, topologies and communication protocols with Intelligence Electronic Devices (IED), router, and switches supporting distributed control systems.
- The physical elements include linking physical and human elements such as devices, monitors, sensors, and actuators for information sharing [28], [30].

5.4 Machine Learning Prediction

The ML predictions focus on reducing the attack surface by detecting the CSC system's critical assets that integrate part of its core assets to other organizations, third-party vendors, suppliers, and distributors in supplier inbound and outbound chains. These are the integrations of the cyber digital (software), cyber physical (infrastructures/hardware) and the physical element (humans). Finally, we discuss how the ML predictions identify vulnerabilities spots that can be exploited.

Figure 4 determines the number of features that explain the Microsoft malware feature distributions out of 78 features after the feature preparations and removing the NANs. The category of the features of critical assets derived from the dataset was cyber digital (software), cyber physical (infrastructures/hardware) and the physical element (humans). The Microsoft Malware feature distributions for the critical assets predicted that of the total of 78 features, the Cyber digital feature distribution has 36 features, Cyber physical has 19 features and the Physical /Human elements indicated 9 features. The results from the feature distribution show that the cyber digital systems are prone to ransomware and malware attacks if there are no antivirus updates on the system.

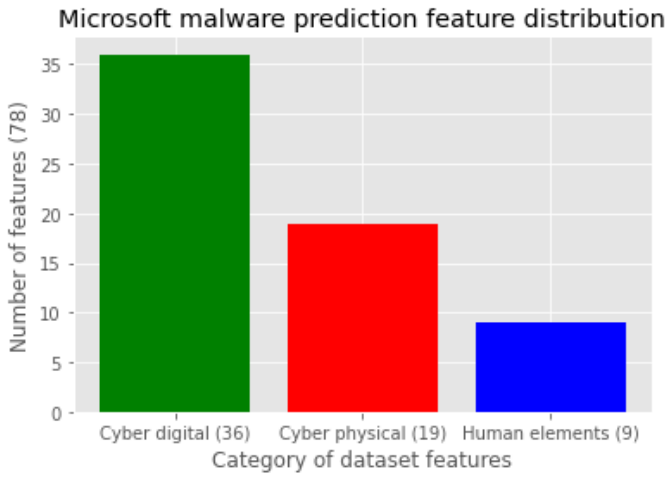


Figure 4. Microsoft Malware Prediction Feature Distribution

5.5 Hyper Parameter Search Space

Figure 5 shows how we used the GridSearchCV through the sklearn library to improve the RF algorithm for the hyperparameter search space. We set the sample size for each classifier and changed the training and test to learn the right features for the models. We optimised the models hyperparameters for the part of the model we can manipulate to improve the predictive performance of the evaluation metrics. Random forest grid search uses cross validation to test the model on different iterations of the dataset with different settings. In our example, we have two sets of different hyperparameters, n_estimators (number of trees in the forest) and min_samples_split (minimum number of samples required to split an internal node), since we have a CV of 10 this is 70 training loops.

```
GridSearchCV(cv=3, estimator=RandomForestClassifier(),
             param_grid={'min_samples_split': [8, 10, 12],
                         'n_estimators': [10, 20, 40, 80]},
             verbose=2)
```

Figure 5. Hyperparameter for Search Space

5.6 Choosing the Classification Algorithms for Optimization Using 10-Fold Cross Validation

Figure 6 discusses the ML classifications algorithms chosen to train and test the dataset: LR, DT and RF, and NB in the MV classifier. Binary classification is used to support AUC-ROC to distinguish between the probabilities of the given classes. The optimization algorithm identifies each data object's major features or class level during training and testing. Furthermore, a 10-Fold cross validation was used to run each algorithm ten times for best results [19], [20]. Moreover, its precisions can predict correct instances, provide a harmonic mean for precision, recall and F-score. Finally, we used an ensemble to combine the classifiers to test the classifiers on each model to determine the accurate performance and best results. To improve the performance of the FR, we have run a grid search on the random forest to check the hyper parameters to improve the prediction results, which gave us a different result compared to the previous. The Figures 5 and 6 explain the classifiers' performances after the training and testing on each model.

5.7 Choosing LR, NN, RF NB Classification Algorithms for Optimization Using 10-Fold Cross Validation

Figure 7 discusses the ML classifications algorithms choosing to train and test the dataset on LR, NN, RF and NB classifiers. Comparing Figures 5 and 6, we could not implement the MV to include NN since the majority voting function was not working with the TensorFlow neural network for the optimization. We used the Sklearn packages for our implementation, so the NN models are not working when we combine the algorithms in an ensemble to perform the cross-validation with the other algorithms. AUC-ROC was used to train and test the dataset on LR, NN, RF and NB classifiers to distinguish between the probabilities of the given classes using 10-Fold cross validation for best results. Table 2 represents the results of the optimization using 10-Fold Cross Validation. Figure 15 depicts the Confusion Matrix and Classification Report for the Neural Network Classifier. Note that we could not run the MV with the NN as we were not able to call the NN package to run with the MV code.

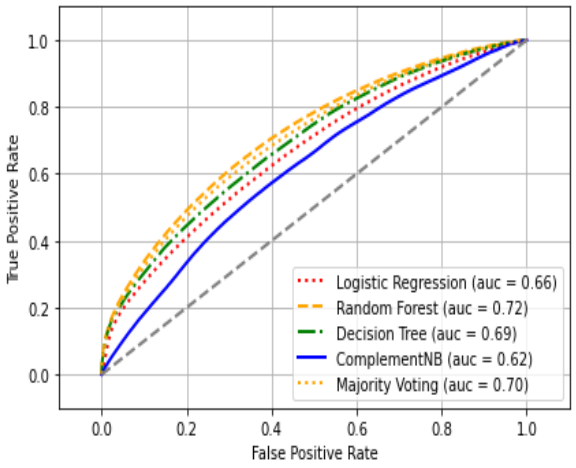


Figure 6. Optimization LR, RF, DT, NB, and MV

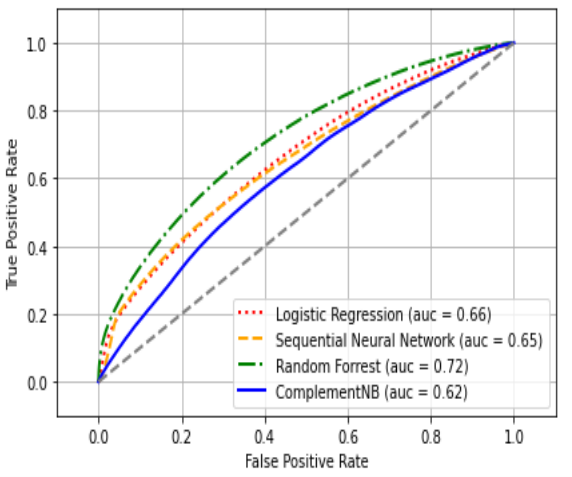


Figure 7. Optimization LR, NN, RF and NB

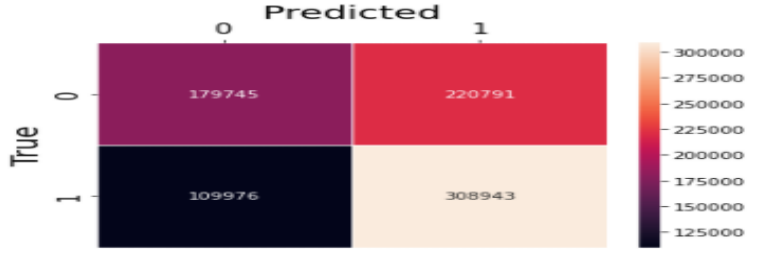
Table 2. Results of the Optimization using 10-Fold Cross Validation

```
Scores with 10 fold cross validation

ROC AUC: 0.65 (+/- 0.00) [Logistic Regression]

ROC AUC: 0.71 (+/- 0.00) [Random Forrest]

ROC AUC: 0.69 (+/- 0.00) [Decision tree]

ROC AUC: 0.62 (+/- 0.00) [ComplementNB]

ROC AUC: 0.60 (+/- 0.00) [Neural network]

ROC AUC: 0.70 (+/- 0.00) [Majority voting]
```

5.8 Performance Accuracies after Evaluation of the Algorithms

Figures 8 evaluate the model's performance by plotting the accuracy of the algorithms in a ROC-AUC and determining the model's performance. First, we plot the algorithms in the ROC curve. AUC_ROC (Area Under Curve – Receiver Operating Characteristics) uses a model selection metric for a bi-multiclass classification problem to distinguish between the probabilities of the given classes. Figure 8 determines the True Positives Rates and False Negatives Rates as discussed in Section 4.4. We label it to determine the x-axis as True Positive Rate (TPR) and the y-axis as False Positive Rate (FPR). The output indicates that the LR, DT SVM, NB in MV predicts an AUC curve average of 0.69, which is not a good prediction for the TPR and FPR as it has less detection rate comparatively. The precision, recall and F1-Score are explained as plotted in the graph below:

The prediction for the TPR and FPR indicates a No Detection of '0' and Has Detection of '1'. The confusion matrix and the classification report for the logistic regression shows a precision 0.62, recall 0.45 and F1-Score 0.52 for the models. Further, the precision with Has Detection of '1' indicates a precision 0.58, recall 0.74 and F1-Score 0.65 for the models. Furthermore, Figure 9 shows the precision and recall curves for the confusion matrix.



	precision	recall	f1-score	support
0	0.62	0.45	0.52	400536
1	0.58	0.74	0.65	418919
accuracy			0.60	819455
macro avg	0.60	0.59	0.59	819455
weighted avg	0.60	0.60	0.59	819455

```
ROC AUC: 0.65 (+/- 0.00) [Logistic Regression]
```

Figure 8. Confusion Matrix and Classification Report for Logistic Regression

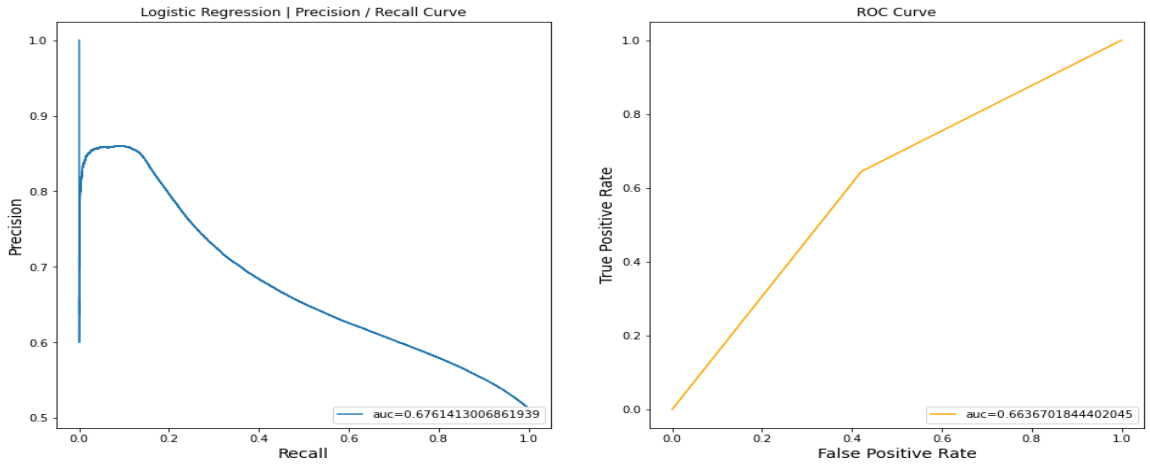
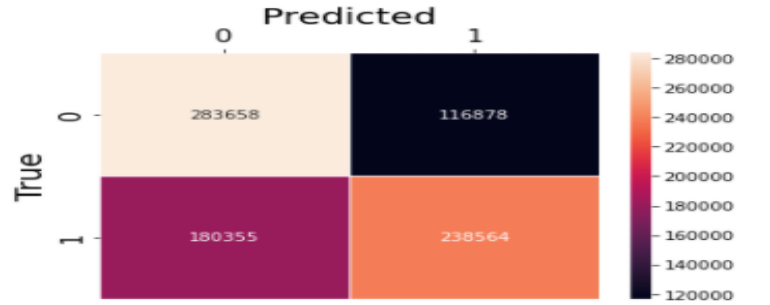


Figure 9. Logistic Regression Precision and Recall Curves

Figure 10 depicts the prediction for the TPR, and FPR indicates a No Detection of '0' and Has Detection of '1'. The confusion matrix and the classification report for the random forest shows a precision 0.61, recall 0.71 and F1-Score 0.66 for the models. Further, the precision with Has Detection of '1' indicates precision 0.67, recall 0.57 and F1-Score 0.62 for the models. Furthermore, Figure 11 shows the precision and recall curves for the confusion matrix.



	precision	recall	f1-score	support
0	0.61	0.71	0.66	400536
1	0.67	0.57	0.62	418919
accuracy			0.64	819455
macro avg	0.64	0.64	0.64	819455
weighted avg	0.64	0.64	0.64	819455

ROC AUC: 0.71 (+/- 0.00) [Random Forrest]

Figure 10. Confusion Matrix and Classification Report for the Random Forest Classifier

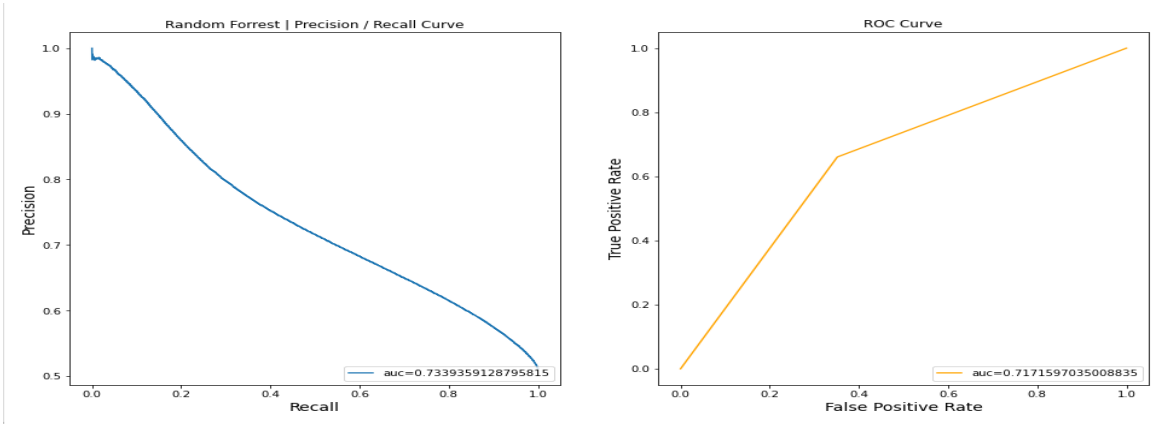
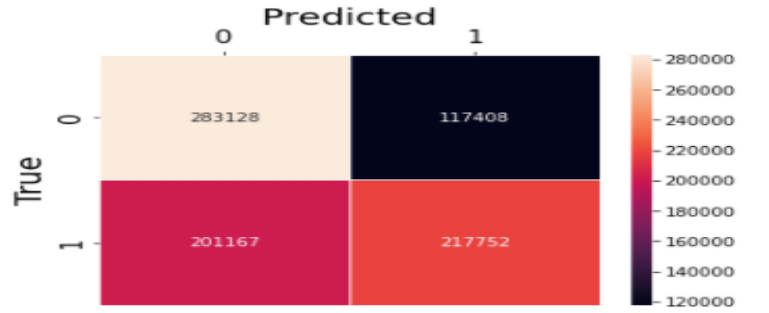


Figure 11. Random Forest Precision and Recall Curves

Figure 12 predicts for the TPR and FPR indicates a No Detection of '0' and Has Detection of '1'. The confusion matrix and the classification report for the DT shows a precision 0.58, recall 0.71 and F1-Score 0.64 for the models.

Further, the precision with Has Detection of '1' indicates precision 0.65, recall 0.52 and F1-Score 0.58 for the models. Furthermore, Figure 13 shows the precision and recall curves for the confusion matrix.



	precision	recall	f1-score	support
0	0.58	0.71	0.64	400536
1	0.65	0.52	0.58	418919
accuracy			0.61	819455
macro avg	0.62	0.61	0.61	819455
weighted avg	0.62	0.61	0.61	819455

ROC AUC: 0.69 (+/- 0.00) [Decision tree]

Figure 12. Confusion Matrix and Classification Report for the Decision Tree Classifier

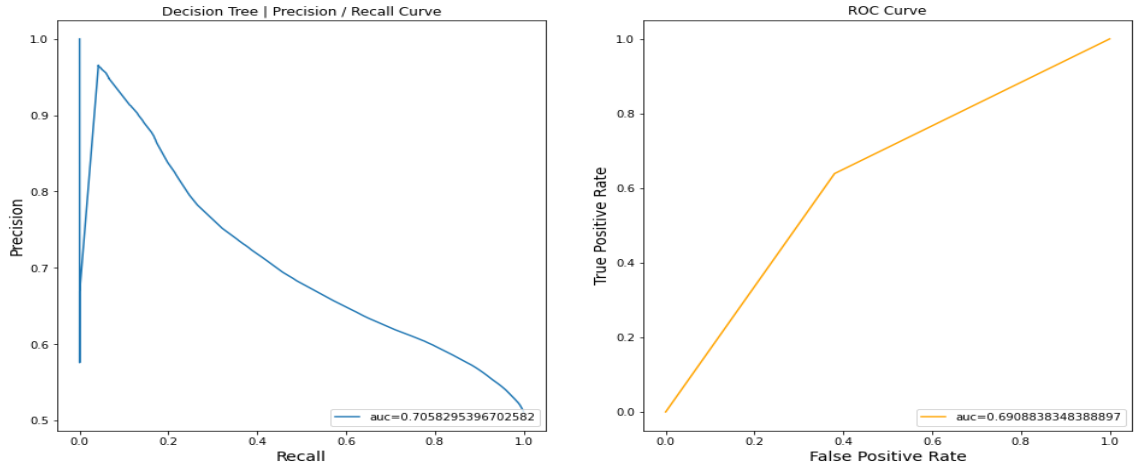
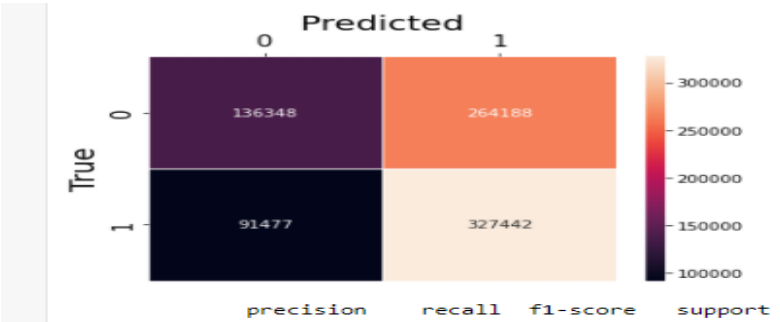


Figure 13. Decision Tree Precision and Recall Curves

Figure 14 depicts the prediction for the TPR, and FPR indicates a No Detection of '0' and Has Detection of '1'. The confusion matrix and the classification report for the NB shows a precision 0.60, recall 0.34 and F1-Score 0.43 for the models. Further, the precision with Has Detection of '1' indicates precision 0.55, recall 0.78 and F1-Score 0.65 for the models. Furthermore, Figure 15 shows the precision and recall curves for the confusion matrix.



	precision	recall	f1-score	support
0	0.60	0.34	0.43	400536
1	0.55	0.78	0.65	418919
accuracy			0.57	819455
macro avg	0.58	0.56	0.54	819455
weighted avg	0.58	0.57	0.54	819455

ROC AUC: 0.62 (+/- 0.00) [ComplementNB]

Figure 14. Confusion Matrix and Classification Report for the Complement NB Classifier

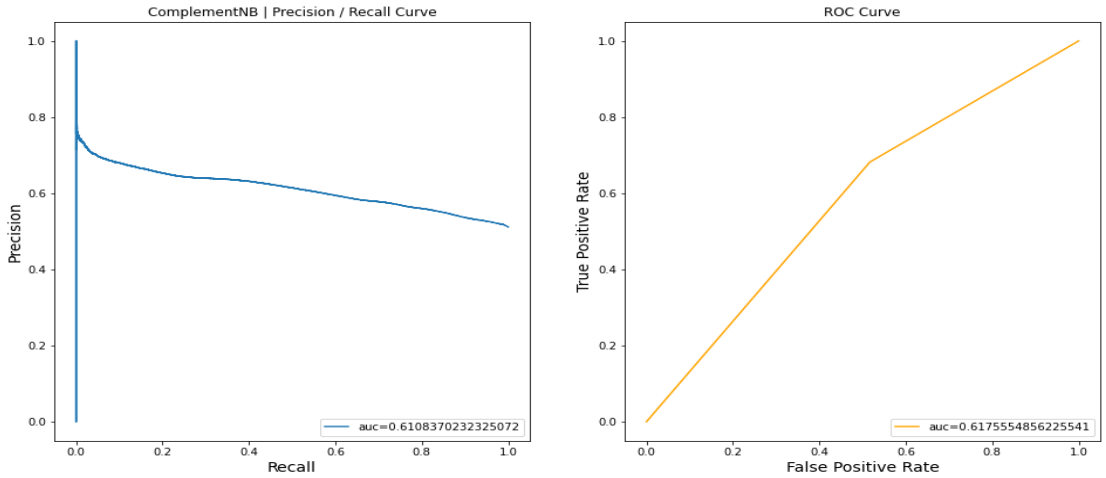
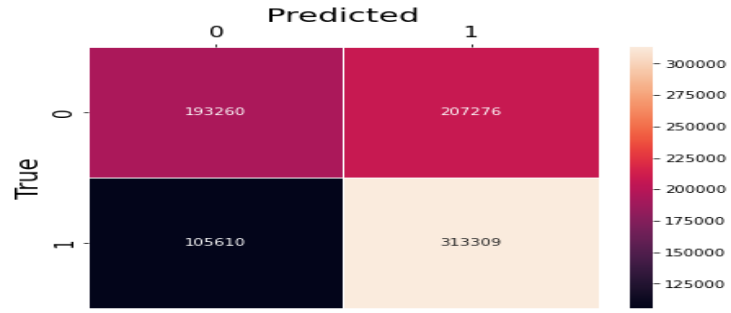


Figure 15. Complement Naïve Bayes Precision and Recall Curves

Figure 16 depicts the prediction for the TPR, and FPR indicates a No Detection of '0' and Has Detection of '1'. The confusion matrix and the classification report for the NN shows a precision 0.65, recall 0.48 and F1-Score 0.55 for the models. Further, the precision with Has Detection of '1' indicates precision 0.60, recall 0.75 and F1-Score 0.67 for the models. Furthermore, Figure 17 shows the precision and recall curves for the confusion matrix.




```
Classification report for Feed forward neural network
              precision    recall  f1-score   support

           0       0.65      0.48      0.55    400536
           1       0.60      0.75      0.67    418919

    accuracy                           0.62    819455
   macro avg       0.62      0.62      0.61    819455
weighted avg       0.62      0.62      0.61    819455

ROC AUC: 0.60 (+/- 0.00) [Neural network]
```

Figure 16. Confusion Matrix and Classification Report for the Neural Network Classifier

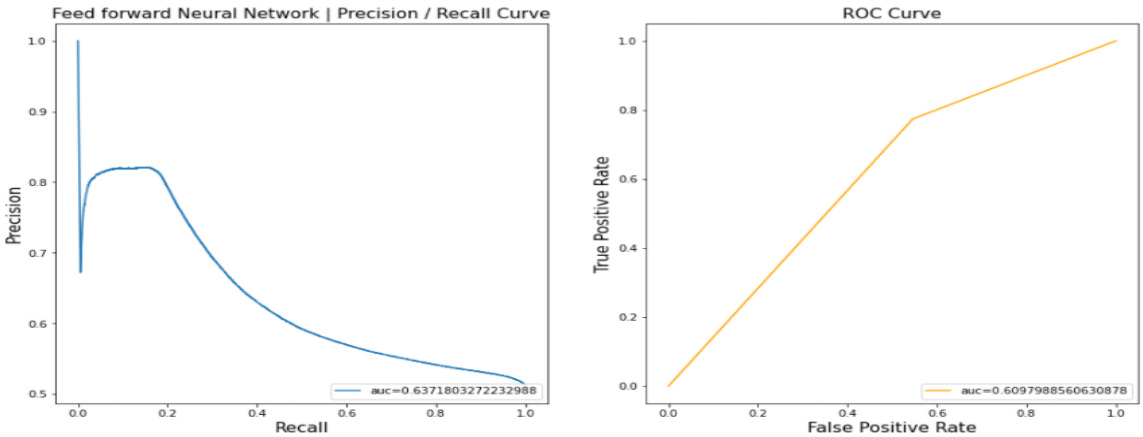


Figure17. Neural Networks Precision and Recall Curves

6. Results

This section discusses the results of the predictions. Figure 18 explains different types of systems that may be most vulnerable in an event where antivirus detection has not been updated to detect any malware. The 'Census_MDC2FormFactor' provides a grouping based on a combination of Device Census level hardware

characteristics. The logic used to define Form Factor is rooted in business and industry standards and aligns with how people think about their devices. (Examples: Smartphone, Small Tablet, All in One, Convertible). Although the amount of Detection is based on the type of computing device form factor, this chart indicates that notebooks are far more likely to be vulnerable to malware intrusion on the system. Additionally, the prediction suggests HasNo detection rates for all the devices. For instance, All in One device experienced about 10%, Convertible 15%, Desktop 40%, Detached 5%, Notebook has 80%, and others have 5% or less No antivirus detection rates.

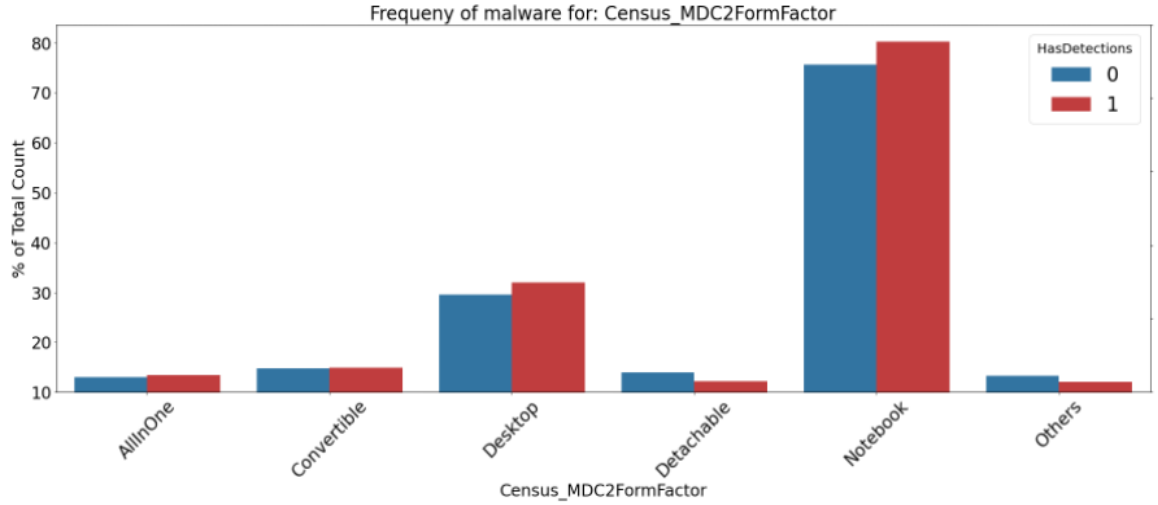


Figure 18. Frequency of Malware Prediction on Devices with Not Updated Antivirus

Figure 19 predicts the frequency of malware attacks to the CSC depending on the State of the Antivirus identified 'AVProductStateIdentifier'. The ML predicts that ID for the specific configuration of a user's antivirus software shows that all but one configuration proved good at preventing attacks with a has a detection rate of 90%. For instance, the State of ID 53447 indicates that this configuration is not performing as expected with no detection of 75% and is performing quite severely compared to the other configurations. Intruders could use this type of knowledge to target a specific system using that product state configuration because it is clearly a weak defence system.

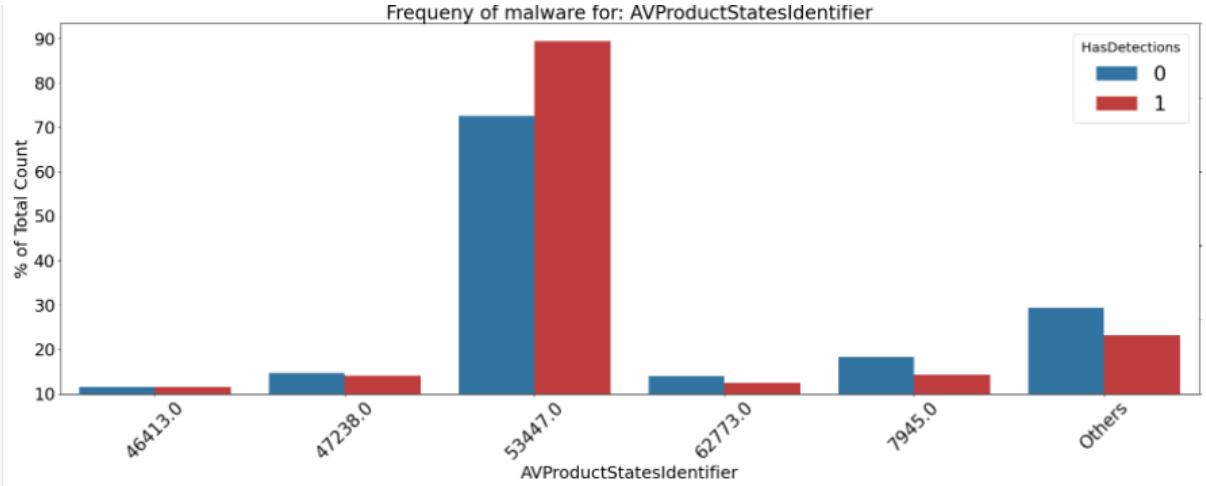


Figure 19. Predicts Frequency of Malware Attacks to CSC Depending on AV Product State Identifier

Figure 20 determines the type of smart screen running on the device, and this is the SmartScreen enabled string value from the registry. This is obtained by checking in order, HKLM\SOFTWARE\Policies\Microsoft\Windows\System\SmartScreenEnabled and HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SmartScreenEnabled. If the value exists but is blank, the value "ExistsNotSet" is sent in the telemetry. The feature "Existsnotset' likely indicates that there is no smart screen active on this machine. The no detection rate is 65%, whereas the has detection is 55%. That correlates strongly with detections since there is a significant disparity between no detections and detections. A malware or ransomware attack will infect all the smart screens that have been enabled but have no antivirus detection leading to cascading impacts on other smart screen devices.

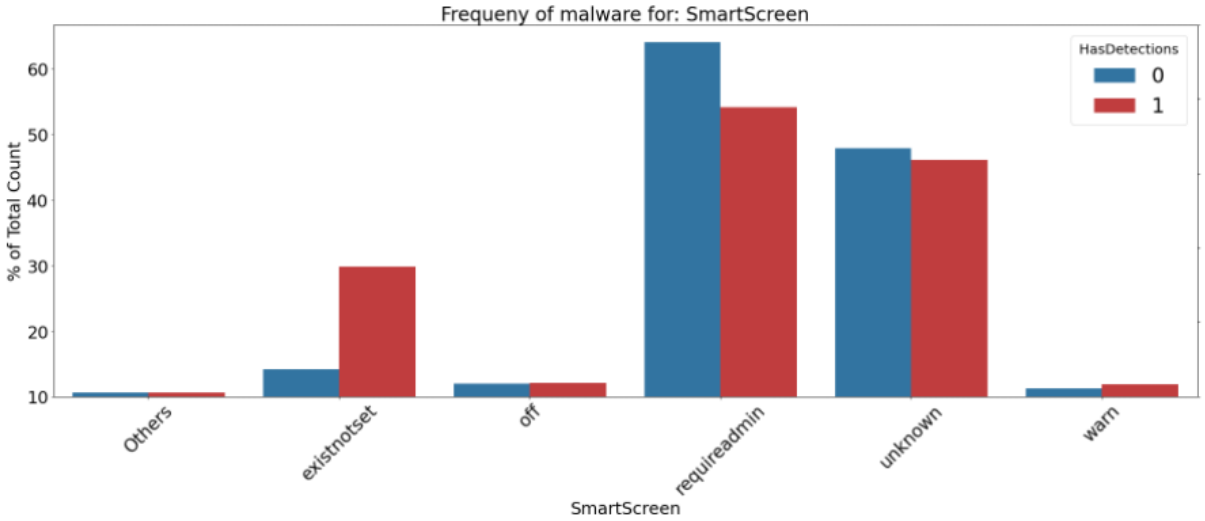


Figure 20. Frequency of Malware Prediction on Smart Screen

Figure 21 indicates the frequency of malware attacks for smart screens used for the workstations. The graph indicates that a 15inch display size was the most frequently occurring class with a detection rate of 90%. It further indicates that the most intrusions indicating that this may be the most common display size for users and thus a good indication to narrow down the user based on physical characteristics of the device.

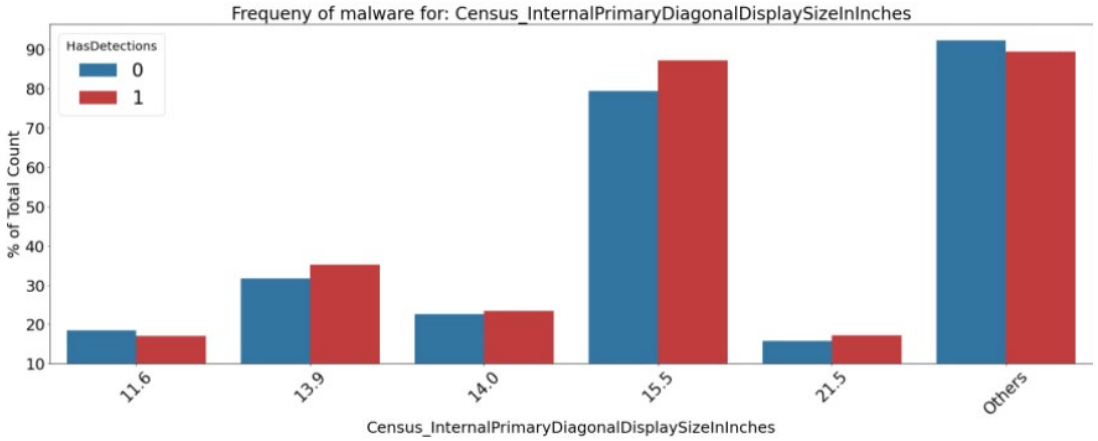


Figure 21. Frequency of Malware Prediction on Smart Screen Size

Figure 22 predicts the frequency of malware attack predictions on primary HDD and SSDs. The attacks impact the Cyber Physical components Systems and indicate that while SSD's are becoming affordable, HDD remains the most common storage medium. The graph shows that the HDD users may experience more disparity between no detections indicating that although 80% has a detection, about 75% has no detections. The users that had an SSD storage medium can link this to SSD's being seen as a specialist item usually requiring self-installation, indicating the user has some knowledge of computer hardware and infrastructure.

Secondly, organizations on the supply chain system with a higher volume of HDD storage mediums can be exposed to during reconnaissance attacks to indicate to the intruder that the internal cyber physical infrastructures are outdated. There may be other weak points in the CSC system network that could be targeted.

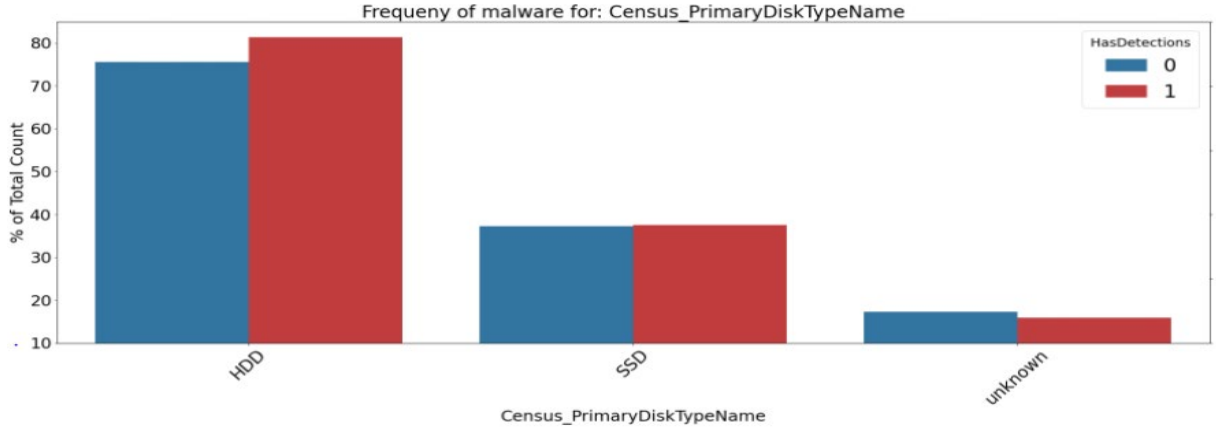


Figure 22. Frequency of Malware Attack Predictions on Primary HDD and SSD

Figure 23 considers the type of windows install performed on the machine, i.e., clean, update, and upgrade. Looking at the graph, the worst performing class is the UUPUpgrade method of OS install type. That stands for Unified Update Platform (UUP), a system by Microsoft to enable users to download updates in smaller file sizes by around 35% through differential downloads. The Has detection rate is 68%, and the No detection rate is 65%. That means that rather than downloading an entirely new image of the OS, users will only download the recent changes to the OS, indicating that while there may be new security patches downloads through this new method, the issue still stands that any malware embedded in the system will stay there through any upgrade procedures if the file system it is imbedded into does not come under upgrade. From the graph, we can assume that this is a leading cause for having a more significant disparity in the detection rate for this class.

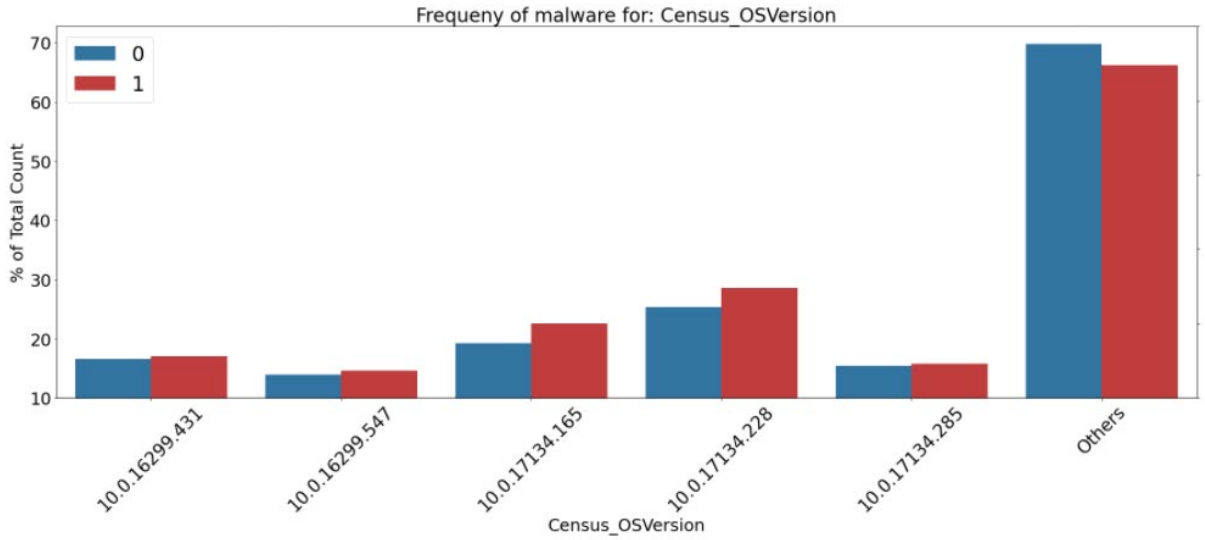


Figure 23. Frequency of Malware Prediction on OS Installed

6.1 Predicting the Attack Profile

Figure 24 explains the threat predictions of the attack profiles from the features on the critical assets based on the dataset. The attack profile predicts that the cyber digital systems components will likely experience 57.8% malware or ransomware attacks. The cyber physical components and infrastructures have a probability of experiencing 29.7% attacks, whiles the physical elements have a probability of experiencing 12.50% of the same attacks.

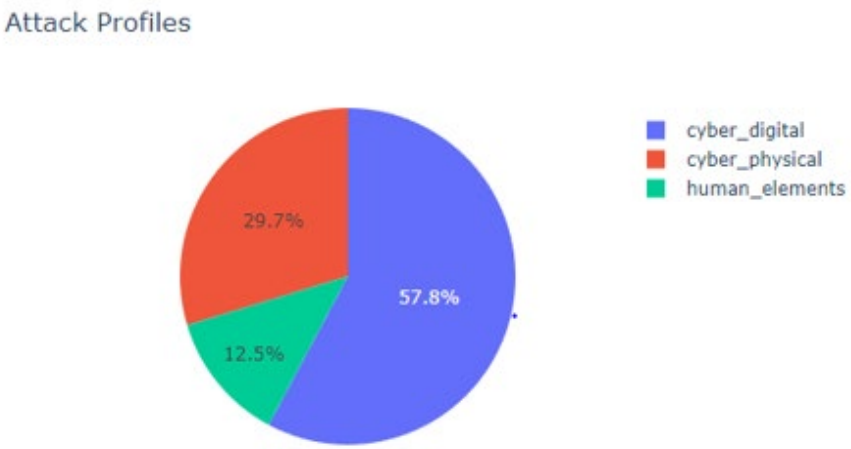


Figure 24. Attack Profiles for Cyber Digital, Cyber Physical and Human Elements

6.3 Decision Tree for Predicting Antivirus Has Detection or No Detection

Figure 25 considered a decision tree for predicting if an antivirus Has Detection or No Detection based on the Product name and OS Edition used. First, we split the dataset into three smaller blocks to graphically represent the decision tree's function. The root node indicates the feature Census_OSEdition with the whole dataset and is shown as samples (4097272). From the root node, we move down to two decision nodes. The first split shown is based upon the gini measurement where a score of more than or equal to 0.5 (true) or less than or equal to 0.499 (false). That split gives us another set of decision nodes, where Census_OSEdition and ProductName are compared. If the

gini rating is less than 0.49, then the tree lands on a terminal node with "No Detection", if more than or equal to 0.5, another decision node is created indicating that the 'Has Detection'.

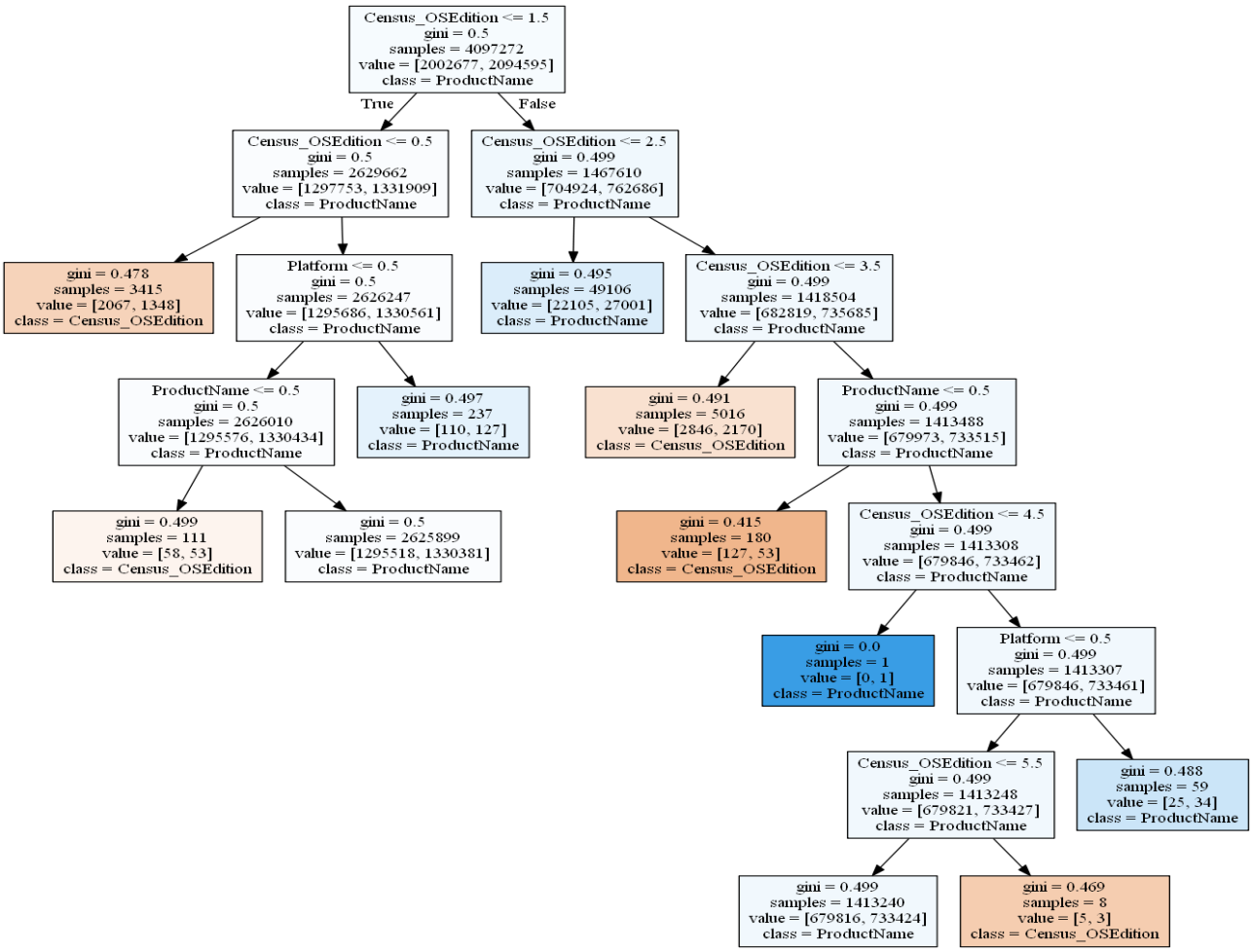


Figure 25. Decision Tree for Predicting Antivirus Has Detection or No Detection

7. Discussion

The need to use ML predictions to ensure cyber resilience in CSC systems security has become predictable in preventing cyberattacks, supply chain risks and vulnerabilities in real-time critical infrastructure systems. Critical assets for CSC systems require a cyber-dependent mission that can anticipate and continue operating correctly in the face of attacks. Cyber resilience provides robust and comprehensive controls to recover from incidents and evolve to better adapt to advanced cyber threats. These critical assets include cyber digital components such as software, data, cloud, internet, computational and industrial control systems process of the embedded systems that make a complete system. The cyber physical components include hardware, architecture, wireless, topologies and communication protocols with Intelligence Electronic Devices (IED), routers, and switches supporting distributed control systems. The physical elements include linking together physical and human elements such as devices, monitors, sensors, and actuators for information sharing.

Further, the ML predictive approach in cyber resilience ensures the ability of supply chain systems to prepare, absorb, recover, and adapt to adverse effects in the complex CPS environment with no or little time for system failures. Malware or Ransomware attacks within the CSC system can severely disrupt the overall business continuity. Therefore, there is a need to understand and predicate these cyber threats so that appropriate control mechanisms and policy formulations can be put in place to enhance system resilience.

7.1 Summary Data Statistics for Accuracy, P, R, F1 and PR-AUC

Table 3 present a summary of the data statistics for the accuracy, precision, recall, F1 Score and PR-AUC of the various models. The collective performance accuracies from the macro-results are derived from Figures 8, 10, 12, 14 and 16. The five different training algorithm evaluation methods, namely LR, RF, DT, NB and NN, are derived for the table. The evaluation metrics are Accuracy, Precision, Recall, F1 and Precision recall curve are measured with AUC. The Precision, Recall and AUC (PR-AUC) represents the evaluation metrics for the classification

models. Figures 9, 11, 13, 15, and 17 represents the results of the PR-AUC classification evaluation reports for the classifiers.

Tabel 3. Summary Data Statistics for Accuracy, P, R, F1 and PR-AUC

Algorithms	Accuracy	Precision	Recall	F1	PR-AUC
Logistic Regression	0.60	0.60	0.59	0.59	0.68
Random Forest	0.66	0.64	0.64	0.64	0.73
Decision Tree	0.61	0.61	0.61	0.61	0.70
Complement NB	0.57	0.58	0.56	0.54	0.61
Neural Network	0.62	0.65	0.48	0.55	0.63

7.2 Mapping the Syber Digital, Cyber Physical and Physical Elements to reduce Attack Surface

This section discusses the probable threat predictions, analysis of the threats and ways to reduce the attack surface in a CSC environment. Figure 24 predicted the attack profiles for cyber digital, cyber physical and human/physical elements. We derive our inferences from the attack profiles in Table 1. to determine which threat is likely to be deployed on the cyber digital, cyber physical, and physical/human elements vulnerable spots. Tables 4, 5 and 6 will assist in building resilience in the CSC systems security requirements to reduce the attack surface.

Table 4. Mapping Cyber Digital Components to Threats to Reduce Attack Surface

Cyber Digital	Threat Predictions	Analysis	Reduce Attack Surface
Software	Malware, Ransomware, rootkit attacks on Antivirus, COTS, Smart Screen.	Test COTS for the Organization and vendors to detect logic bomb, malware, virus, bugs, vulnerability	Utilize inventory tools to identify and secure attack surfaces, vectors, and OS. Antivirus updates, patches
Data	SQL injections, Industrial espionage, IP theft. ID theft, Botnet	Privacy, information leakage, IoT and sensors	Utilize data mining techniques for inferences and sanitizations to secure data.
Cloud	Misconfigurations, API Attacks, poor authentication mechanisms	Analyse threats and vulnerabilities on IaaS, AaaS and SaaS	Utilize cryptography methods such as SSL, TLS and Egress. Backup data. Third party audit.
Internet	RAT, IP Address, Rootkit, Botnet. Island hopping.	Carryout Pentest, Vulnerability assessments to identify threats	Utilize firewall technologies, IDS/IPS. DMZ.
Computational systems	Operating Systems attacks, DDoS, Malware, Virus	Access controls and authorization policies	Change password regularly, User ID, Security groups, roles and responsibilities, a cryptography key

Table 5. Mapping Cyber Physical Components to Threats to Reduce Attack Surface

Cyber Physical	Threat Predictions	Analysis	Reduce Attack Surface
Hardware	Malware, Ransomware, rootkit attacks on Antivirus, COTS, Smart Screen	Test COTS for the Organization and vendors.	Utilize inventory tools to identify and secure attack surfaces, vectors, and OS. Antivirus updates, patches
Infrastructure	SQL injections, Industrial espionage, IP theft. ID theft, Botnet	Privacy, information leakage, IoT and sensors	Utilize data mining techniques for inferences and sanitizations to secure data.
Network Topologies	Misconfigurations, API Attacks, poor authentication mechanisms	Analyse threats and vulnerabilities on IaaS, AaaS and SaaS	Utilize cryptography methods such as SSL, TLS and Egress. Backup data. Third party audit.
SCADA	RAT, IP Address, Rootkit, Botnet. Island hopping.	Carryout Pentest, Vulnerability assessments to identify threats	Utilize firewall technologies, IDS/IPS. DMZ.
Intelligent Electronic Devices (IED)	Operating Systems attacks, DDoS, malware, virus	Access controls and authorization policies	Change password regularly, User ID, Security groups, roles and responsibilities, a cryptography key
Communication Protocols	SSL/TLS, PGP, SSL, attacks digital certificate	Protocols can be exploited via Factoring the public key and faulty encryptions	Utilize standard RSA cryptosystems, Prevent Misconfigurations. Audit third parties systems.

Table 6. Mapping Physical Components to Threats to Reduce Attack Surface

Physical/Human	Threat Predictions	Analysis	Reduce Attack Surface
Sensors	Energy Draining, Homing and Exhaustive attacks on sensor nodes	Test multiple access points of the same nodes with different identities one may be malicious	Reduce time to travel on the access points to prevent abrupt system shutdown. DoS, and Prevent collision
Actuators	Resonance attacks, Intercepting and interruption, modifying orders to oscillate	Analyse intelligence devices that convert energy signals to physical elements for error detections	Deploy configurations mechanisms to track and report on faulty equipment to prevent failures and oscillation attacks
Humans	Physical security, Offended or Disgruntled employees, and cyberattackers	Identify vulnerable spots and on CSC systems. Analyse activity logs	Educate staff, Authentication and authorization. Deploy role-based access control policies. MonitorCCTV
Monitors	Ransomware attacks on smart screens and how they cascaded to other screens.	Identify monitors with high-resolution rates that are prone to malware attacks. Analyse CSC attacks and their cascading impact.	Implement regular and Adhoc antivirus updates and software patches.
Firewalls/IDS/IPS	Detect misconfigurations and block unauthorized access, network traffic and intrusions to the CSC network. Including DDoS, XSS and CSRF attacks.	Analyse and inspect, filter firewall traffic, IDS/IPS devices, review logs, reports and attack trends to the CSC system.	Define network traffic policies and review firewall and IDS/IPS configurations rules. Deploy deep packet inspection and 5G firewalls. Review configuration mechanisms, apply patches to reflect current attack trends.
Routers/Switches	IP Spoofing, DoS, deploy crafted packets sent to DHCP server to block traffic. ARP Poisoning	Analyse routing, switching, IP, Address Resolution Protocol and Subnet configurations.	Configure ports based on policy. Deploy packet analyzer. Monitor network traffic regularly.

7.3 Recommended CSC Security Controls

CSC controls are security strategies and measures formulated and implemented to ensure that the organizational goals and objectives are achieved. Controls are prioritized actions that collectively form a defence-in-depth set of best practices required to mitigate attacks. CSC security controls are managerial, operational, and technical safeguards or countermeasures employed to protect data confidentiality, integrity, and availability. The paper recommends the following approach for implementing CSC security control mechanisms:

- Establish a collaborative mechanism with all stakeholders to protect and secure the supply chain systems. Determine standards required to implement controls to mitigate CSC attacks. E.g., standards, audit, supply chain risk management, policies, and best practices.
- Determine audit control requirements to mitigate the third-party vendors
- Determine realistic and adaptable standards by third party vendors to ensure best practices and business continuity.
- Determine the desired or required level of assurance that ensures that the selected security controls implemented are effective in their application.
- Evaluate the vendors regularly in line with their different roles and responsibilities within the organizational goals and objectives.

8. Conclusion

Our work considered the necessary concepts required to understand cyber resilience in the CSC context. These concepts, i.e., actor, goal, asset, attack surface, incident, IoC, CSC requirements, are considered from several relevant domains, including CSC, cyber resilience, and threat. CSC system resilience is based on understanding the threat landscape, situational awareness and predicting the threats. We considered two main resilience design principles by focusing on common critical assets such as cyber digital, physical, and physical elements. First, the ML prediction is used to detect possible CSC attacks. Then control mechanisms are implemented to reduce the attack surface. Next, the ML techniques were used on a Microsoft Malware Prediction website dataset to analyze and predicate the threats based on the CSC resilience design principles. A total of 78 features we identified for the critical assets and were split into cyber digital feature distribution has 36 features, cyber physical with 19 features and the physical elements with 9 features. The cyber digital systems components were predicted to experience several ransomware and malware attacks in an attack where the antivirus has not updated the system.

Furthermore, we consider the performance accuracies of LR, DT, RM and NB classification algorithms in a Majority Voting to predicate the results. Additionally, we performed training and testing on LR, RM, NB and NN classification algorithms in an ensemble to learn the dataset for accuracies to predicate the results. A ROC-ARC was used in an ensemble and a 10-Fold cross validation on each algorithm for the performance optimization during learning and testing the dataset. The classifiers were run using a confusion matrix to predict the TPR and

FPR for each classification model and detections. Finally, we have mapped the threats with known attacks for inferences and determined the controls required to improve resilience on the critical assets.

References

[1] S. Barnum, "Standardizing cyber threat intelligence information with the structured threat information expression (stix)," Mitre Corporation, 2012. Accessed: Oct. 01, 2021. [Online]. Available: http://www.standardscoordination.org/sites/default/files/docs/STIX_Whitepaper_v1.1.pdf

[2] D. Bodeau, R. Graubart, W. Heinbockel, and E. Laderman, "Cyber Resiliency Engineering Aid – The Updated Cyber Resiliency Engineering Framework and Guidance on Applying Cyber Resiliency Techniques," 2015. https://www.mitre.org/sites/default/files/publications/pr-15-1334-cyber-resiliency-engineering-aid-framework-update.pdf (accessed Oct. 10, 2021).

[3] Kaggle, "Microsoft Malware Prediction," 2019. https://kaggle.com/c/microsoft-malware-prediction (accessed Oct. 01, 2021).

[4] O. Khan and D. Estay, "Supply Chain Cyber-Resilience: Creating an Agenda for Future Research," *Technol. Innov. Manag. Rev.*, vol. 5, no. 4, pp. 6–12, 2015.

[5] D. Bodeau and R. Graubart, "Cyber Resilience Metrics: Key Observations," 2016. https://apps.dtic.mil/sti/pdfs/AD1107819.pdf (accessed Oct. 10, 2021).

[6] J. Miller, "Supply Chain Attack Framework and Attack Patterns," Mitre Corporation, MITRE TECHNICAL REPORT MTR140021, 2013. Accessed: Oct. 01, 2021. [Online]. Available: https://www.mitre.org/sites/default/files/publications/supply-chain-attack-framework-14-0228.pdf

[7] I. Linkov and A. Kott, "Fundamental Concepts of Cyber Resilience: Introduction and Overview," in *Cyber Resilience of Systems and Networks*, A. Kott and I. Linkov, Eds. Cham: Springer International Publishing, 2019, pp. 1–25. doi: 10.1007/978-3-319-77492-3_1.

[8] D. Bodeau and R. Graubart, "Cyber Resiliency Design Principles Selective Use Throughout the Lifecycle and in Conjunction with Related Disciplines," MITRE CORP BEDFORD MA BEDFORD United States, Jan. 2017. Accessed: Oct. 10, 2021. [Online]. Available: https://apps.dtic.mil/sti/citations/AD1107919

[9] R. Ross, V. Pillitteri, R. Graubart, D. Bodeau, and R. McQuaid, "Developing cyber resilient systems:: a systems security engineering approach," National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-160v2, Nov. 2019. doi: 10.6028/NIST.SP.800-160v2.

[10] A. Mohasseb, B. Aziz, J. Jung, and J. Lee, "Predicting CyberSecurity Incidents using Machine Learning Algorithms: A Case Study of Korean SMEs:," in *Proceedings of the 5th International Conference on Information Systems Security and Privacy*, Prague, Czech Republic, 2019, pp. 230–237. doi: 10.5220/0007309302300237.

[11] L. Bilge, Y. Han, and M. Dell'Amico, "RiskTeller: Predicting the Risk of Cyber Incidents," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, Dallas Texas USA, Oct. 2017, pp. 1299–1311. doi: 10.1145/3133956.3134022.

[12] O. Yavanoglu and M. Aydos, "A review on cyber security datasets for machine learning algorithms," in *2017 IEEE International Conference on Big Data (Big Data)*, Dec. 2017, pp. 2186–2193. doi: 10.1109/BigData.2017.8258167.

[13] 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," in *2014 7th International Symposium on Resilient Control Systems (ISRCS)*, Denver, CO, USA, Aug. 2014, pp. 1–8. doi: 10.1109/ISRCS.2014.6900095.

[14] B. Gallagher and T. Eliassi-Rad, "Classification of HTTP Attacks: A Study on the ECML/PKDD 2007 Discovery Challenge," LLNL-TR--414570, 1113394, Jul. 2009. doi: 10.2172/1113394.

[15] O. Sharma, M. Girolami, and J. Sventek, "Detecting worm variants using machine learning," in *Proceedings of the 2007 ACM CoNEXT conference on - CoNEXT '07*, New York, New York, 2007, p. 1. doi: 10.1145/1364654.1364657.

[16] D. Bhamare, T. Salman, M. Samaka, A. Erbad, and R. Jain, "Feasibility of Supervised Machine Learning for Cloud Security," in *2016 International Conference on Information Science and Security (ICISS)*, Pattaya, Thailand, Dec. 2016, pp. 1–5. doi: 10.1109/ICISSEC.2016.7885853.

[17] J. M. Hilbe, "LOGISTIC REGRESSION," 2011. https://encyclopediaofmath.org/images/6/69/Logistic_regression.pdf (accessed Oct. 10, 2021).

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

[19] A. Boschetti and L. Massaron, *Python data science essentials: become an efficient data science practitioner by understanding Python's key concepts*, Second Edition. Birmingham Mumbai: Packt Publishing Ltd, 2016.

[20] A. Yeboah-Ofori *et al.*, "Cyber Threat Predictive Analytics for Improving Cyber Supply Chain Security," *IEEE Access*, vol. 9, pp. 94318–94337, 2021, doi: 10.1109/ACCESS.2021.3087109.

[21] A. Yeboah-Ofori and S. Islam, "Cyber Security Threat Modeling for Supply Chain Organizational Environments," *Future Internet*, vol. 11, no. 3, Art. no. 3, Mar. 2019, doi: 10.3390/fi11030063.

[22] D. J. Bodeau and R. D. Graubart, "Structured Cyber Resiliency Analysis Methodology," May 2016, Accessed: Oct. 10, 2021. [Online]. Available: https://www.mitre.org/publications/technical-papers/structured-cyber-resiliency-analysis-methodology

[23] J. Drew, M. Hahsler, and T. Moore, "Polymorphic malware detection using sequence classification methods and ensembles: BioSTAR 2016 Recommended Submission - EURASIP Journal on Information Security," *EURASIP J. Inf. Secur.*, vol. 2017, no. 1, p. 2, Dec. 2017, doi: 10.1186/s13635-017-0055-6.
[24] E. S. K. Yu, P. Giorgini, N. Maiden, and J. Mylopoulos, *Social Modeling for Requirements Engineering*. MIT Press, 2011.
[25] C. S. Johnson, M. L. Badger, D. A. Waltermire, J. Snyder, and C. Skorupka, "Guide to Cyber Threat Information Sharing," National Institute of Standards and Technology, NIST SP 800-150, Oct. 2016. doi: 10.6028/NIST.SP.800-150.
[26] A. Yeboah-Ofori and D. Opoku-Akyea, "Mitigating Cyber Supply Chain Risks in Cyber Physical Systems Organizational Landscape," in *2019 International Conference on Cyber Security and Internet of Things (ICSIoT)*, Accra, Ghana, May 2019, pp. 74–81. doi: 10.1109/ICSIoT47925.2019.00020.
[27] A. Yeboah-Ofori, J. Abdulai, and F. Katsriku, "Cybercrime and Risks for Cyber Physical Systems," *Int. J. Cyber-Secur. Digit. Forensics IJCSDF*, vol. 8, no. 1, Art. no. 1, Mar. 2019, doi: 10.17781/P002556.
[28] A. Humayed, J. Lin, F. Li, and B. Luo, "Cyber-Physical Systems Security—A Survey," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1802–1831, Dec. 2017, doi: 10.1109/JIOT.2017.2703172.
[29] A. A. Cárdenas, S. Amin, Z.-S. Lin, Y.-L. Huang, C.-Y. Huang, and S. Sastry, "Attacks against process control systems: risk assessment, detection, and response," in *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*, New York, NY, USA, Mar. 2011, pp. 355–366. doi: 10.1145/1966913.1966959.
[30] M. Chen, U. Challita, W. Saad, C. Yin and M. Debbah, "Artificial Neural Networks-Based Machine Learning for Wireless Networks: A Tutorial," in *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3039-3071, Fourthquarter 2019, doi: 10.1109/COMST.2019.2926625.
[31] J. R. Parveen, "Neural Networks in Cyber Security" International Research Journal of Computer Science. Issue 09, Vol. 4 2017.
[32] Barros, R. C. De Carvalho A. C. P. L. F., Freitas, A. A.: Automatic Design of Decision-Tree Induction Algorithms", Springer. Briefs in Computer Science, DOI 10.1007/978-3-319-14231-9_2. (2015).
[33] R. C. Barros, A. C. P. L. F. De Carvalho. and A. A. Freitas, "Automatic Design of Decision-Tree Induction Algorithms", Springer. Briefs in Computer Science, DOI 10.1007/978-3-319-14231-9_2. (2015).
[34] T. Hastie, R. Tibshirani and J. Friedman. "The Elements of Statistical Learning". Data Mining, Inference, and Prediction. Springer Series in Statistics. 2nd Edition. 2017.
[35] L. Breiman, "Random Forests", Machine Learning, Springer. 45(1), 5-32, 2001
[36] SKLearn. Random Forest Classifier https://scikit-learn.org/stable/modules/generated/sklearn.ensemble.RandomForestClassifier.html
[37] G. Shobha and S, Rangaswamy, "Computational Analysis and Understanding of Natural Languages: Principles, Methods and Applications" Elsevier, Chapter - Machine Learning. Volume 38. 2018. pages 197-228 https://doi.org/10.1016/bs.host.2018.07.004
[38] S. Prabhakaran, "How Naïve Bayes Algorithm Works (With Example and Code)" 2018. https://www.machinelearningplus.com/predictive-modeling/how-naive-bayes-algorithm-works-with-example-and-full-code/
[39] G. Appruzzese, L. Ferretti, M. Marchetti, M. Colajanni, A. and Guido, "On the Effectiveness of Machine Learning for Cyber Security. International Conference on Cyber Conflict." 2018. IEEE. DOI: 10.23919/CYCON.2018.8405026