IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received April 19, 2021, accepted May 10, 2021, date of publication June 7, 2021, date of current version July 9, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3087109

Cyber Threat Predictive Analytics for Improving Cyber Supply Chain Security

ABEL YEBOAH-OFORI[1], SHAREEFUL ISLAM[2], SIN WEE LEE[2], ZIA USH SHAMSZAMAN[3], (Senior Member, IEEE), KHAN MUHAMMAD[4], (Member, IEEE), METEB ALTAF[5], AND MABROOK S. AL-RAKHAMI[6], (Member, IEEE)

[1]Department of Computer Science and Engineering, University of West London, Ealing London W5 5RF, U.K.
[2]School of Architecture Computing and Engineering (ACE), University of East London, London E16 2RD, U.K.
[3]Department of Computing and Games, Teesside University, Middlesbrough TS1 3BX, U.K.
[4]Visual Analytics for Knowledge Laboratory (VIS2KNOW Lab), School of Convergence, College of Computing and Informatics, Sungkyunkwan University, Seoul 03063, South Korea
[5]Advanced Manufacturing and Industry 4.0 Center, King Abdulaziz City for Science and Technology, Riyadh 11442, Saudi Arabia
[6]Research Chair of Pervasive and Mobile Computing, Information Systems Department, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia

Corresponding author: Mabrook S. Al-Rakhami (malrakhami@ksu.edu.sa)

This work was supported by the Deanship of Scientific Research at King Saud University through the Vice Deanship of Scientific Research Chairs: Chair of Pervasive and Mobile Computing.

ABSTRACT Cyber Supply Chain (CSC) system is complex which involves different sub-systems performing various tasks. Security in supply chain is challenging due to the inherent vulnerabilities and threats from any part of the system which can be exploited at any point within the supply chain. This can cause a severe disruption on the overall business continuity. Therefore, it is paramount important to understand and predicate the threats so that organization can undertake necessary control measures for the supply chain security. Cyber Threat Intelligence (CTI) provides an intelligence analysis to discover unknown to known threats using various properties including threat actor skill and motivation, Tactics, Techniques, and Procedure (TT and P), and Indicator of Compromise (IoC). This paper aims to analyse and predicate threats to improve cyber supply chain security. We have applied Cyber Threat Intelligence (CTI) with Machine Learning (ML) techniques to analyse and predict the threats based on the CTI properties. That allows to identify the inherent CSC vulnerabilities so that appropriate control actions can be undertaken for the overall cybersecurity improvement. To demonstrate the applicability of our approach, CTI data is gathered and a number of ML algorithms, i.e., Logistic Regression (LG), Support Vector Machine (SVM), Random Forest (RF), and Decision Tree (DT), are used to develop predictive analytics using the Microsoft Malware Prediction dataset. The experiment considers attack and TTP as input parameters and vulnerabilities and Indicators of compromise (IoC) as output parameters. The results relating to the prediction reveal that Spyware/Ransomware and spear phishing are the most predictable threats in CSC. We have also recommended relevant controls to tackle these threats. We advocate using CTI data for the ML predicate model for the overall CSC cyber security improvement.

INDEX TERMS Cyber threat intelligence, machine learning, cyber supply chain, predictive analytic, cyber security, tactic techniques procedures.

I. INTRODUCTION

Cyber Supply Chain (CSC) security is critical for reliable service delivery and ensure overall business continuity of Smart CPS. CSC systems by its inherently is complex and vulnerabilities within CSC system environment can cascade from a source node to a number of target nodes of the overall cyber physical system (CPS). A recent NCSC report highlights a list of CSC attacks by exploiting vulnerabilities that exist within the systems [1]. Organizations outsource part of their business and data to the third-party service providers that could lead any potential threat. There are several examples for successful CSC attacks. For instance, Dragonfly, a Cyber Espionage group, is well known for targeting CSC organization [2], [3]. The Saudi Aramco power station attack halted its operation due to a massive cyberattack [1]. There are

The associate editor coordinating the review of this manuscript and approving it for publication was Po Yang.

existing works that consider CSC threats and risks but a lack of focus on threat intelligence properties for the overall cyber security improvement. Further, it is also essential to predict the cyberattack trends so that the organization can take the timely decision for its countermeasure. Predictive analytics not only provide an understanding of the TTPs, motives and intents of the threat actors but also assist situational awareness of current supply system vulnerabilities.

This paper aims to improve the cybersecurity of CSC by specifically focusing on integrating Cyber Threat Intelligence (CTI) and Machine Learning (ML) techniques to predicate cyberattack patterns on CSC systems and recommend suitable controls to tackle the attacks. The novelty of our work is threefold:

- Firstly, we consider Cyber Threat Intelligence(CTI) for systematic gathering and analysis of information about the threat actor and cyber-attack by using various concepts such as threat actor skill, motivation, IoC, TTP and incidents. The reason for considering CTI is that it provides evidence-based knowledge relating to the known attacks. This information is further used to discover unknown attacks so that threats can be well understood and mitigated. CTI provides intelligence information with the aim of preventing attacks as well as shorten time to discover new attacks.
- Secondly, we applied ML techniques and classification algorithms and mapped with the CTI properties to predict the attacks. We use several classification algorithms such as Logistic Regression (LG), Support Vector Machine (SVM), Random Forest (RF) and Decision Tree (DT) for this purpose. We follow CTI properties such as Indicator of Compromise (IoC) and Tactics, Techniques and Procedure (TTP) for the attack predication.
- Finally, we consider widely used cyberattack dataset to predict the potential attacks [6]. The predication focuses on determining threats relating to Advance Persistent Threat (APT), command and control and industrial espionage which are relevant for CSC [7]–[9]. The result shows the integration of CTI and ML techniques can effectively be used to predict cyberattacks and identification of CSC systems vulnerabilities. Furthermore, our prediction reveals a total accuracy of 85% for the TPR and FPR. The results also indicate that LG and SVM produced the highest accuracy in terms of threat predication.

The rest of the paper is organised as follows: Section 2 presents an overview of related works including CSC security, cyber threat intelligence and Machine Learning for CSC. Section 3 provides the concepts necessary for the proposed approach and the meta model. Section 4 provides an overview of the proposed approach including the integration of CTI and ML. Section 5 presents the underlying process for the threat analysis and predication. Section 6 implements the process for the threat predication using the widely used Microsoft malware datasets. Section 7 discusses the results and compares the work with the existing works in the literature. Finally, Section 8 provides conclusion and future direction of the work.

II. RELATED WORK

There exists several widely used CTI and ML models in cyber security domain. This section presents the existing works that are relevant with our work.

A. CYBER SUPPLY CHAIN(CSC) SECURITY

The CSC security provides a secure integrated platform for the inbound and outbound supply chains systems with third party service provider including suppliers, and distributors to achieve the organizational goal [10]. Cybersecurity from supply chain context involves various secure outsourcing of products and information between third party vendors, and suppliers [11]. This outsourcing includes the integration of operational technologies (OT) and Information technologies (IT) running on Cyber Physical Systems (CPS) infrastructures. However, there are threats, risks and vulnerabilities that are inherent in such systems that could be exploited by threat actors on the operational technologies and information technologies of the supply inbound and outbound chains systems. The outbound chain attacks include data manipulations, information tampering, redirecting product delivery channels, and data theft. The IT risks include those attacks on the cyber physical and cyber digital system components such as distributed denial of service (DDoS) attacks, IP address spoofing, and Software errors [12]. Regarding CSC security, NIST SP800 [13] proposed a 4 tier framework approach for improving critical infrastructure cybersecurity that incorporates the cyber supply chain risk management framework into it as one of its core components. Tier 1 considers the organizations CSC risk requirement strategy. Tier 2 considers the supply chain associated risk identifications including products and services in the supply inbound and outbound chains. Tier 3 implementation considers the risk assessments, threats analyses, associated impacts and determine the baseline requirements for governance structure. Tier 4 consider real-time or near-time information to understand supply chain risk associated with each product and service. However, the approach and tiers considered risks management but did not emphasize on ML and threat prediction for future trends in the CSC domain. Additionally, [14] proposed a supply chain attack framework and attack patterns that structured and codifies supply chain attacks. The goal of the framework was to provide a comprehensive view of supply chain attacks of malicious insertion across the full acquisition lifecycle to determine the associated threat and vulnerability information.

B. CYBER THREAT INTELLIGENCE (CTI)

Cyber threat intelligence (CTI) gatherings and analysis have become one of the relevant actionable intelligences used to understand both known and unknown threats [4]. The impact of cyberattacks and emerging threats on CSC systems and

its devastating effects on business process, data, Intellectual Property, delivery channel, and cost of recovery has increased the surge for CTI approach. The CTI process includes identification, threat analysis and information disseminating to stakeholders. Considering CTI for cybersecurity, ENISA in [4] explored the opportunities and limitations of current threat intelligence platforms by considering CTI implementation process and threat intelligence programs (TIP) from strategic, tactical and operational goals. The authors proposed a threat intelligence program model that collects, normalize, enrich, correlate, analyse and disseminate threat related information to stakeholders. The strategic CTI goals consider factors that support executive decision makings, tactical goals consider the CTI process and TIP programs that identifying intelligence gap and prioritizing them for risk reduction. The operational goals provide a process that provides an understanding of the threat actors motives, modes of operation, intents, and TTPs and capabilities. However, the processes do not incorporate ML threat predictions. Additionally, [15] proposes a threat intelligence-driven security model that considers six CTI phases and processes lifecycle required to identify intelligence goals. The CTI phases include direction, collection, process, analysis, dissemination, and feedback. The author incorporated internal sources such as network traffic, logs, scans; external sources such as vulnerability database, threat feeds; and human sources such as the dark web and social media into the model for the threat intelligence modelling. The threat intelligence driven security model emphasizes on using network traffics, logs and scans and not ML algorithms for the prediction. Further, [16] develop cyber threat Intelligence metrics that consider assets, requirement business operations, adversary, and consumer intelligence places emphases on value and organizational benefits. The author's approach considers four key stages in the threat intelligence process including intelligence requirements, information collection, analyses, dissemination, and intelligence usage. However, the approach does not consider machine learning for predicting invisible attacks. Furthermore, [17] proposed a CTI model that operationalizes and analyses adversarial activities across the lifecycle of an organization business process to determine actions taken by the attacker. The author's approach was based on the organizational intelligence requirements, information gathering, analyses and disseminate to protect assets for strategic, tactical and operational understanding and situational awareness. However, the works emphasized more on attacker motive and intent and not on ML for the threat predictions. The CTI functional process is to collect metrics and trend analysis for the business risk assessment, prioritization, and decision support with less emphasis on ML for CSC security.

C. MACHINE LEARNING IN CSC SECURITY

There are several works that consider Machine Learning classifiers in various cybersecurity application domains such as spam filters, antivirus and IDS/IPS to predict cyberattack trends [18], [23], [24]. Considering ML for Security [11], proposed ML classification of HTTP attacks using a decision tree algorithm to learn a dataset for performance accuracies and automatically label a request as valid or attack. The authors developed a vector space model used commonly for information retrieval to build a classifier to automatically label the request as malicious in the URL. The approach achieved high precision and recall comparatively. However, the work did not focus on ML and threat prediction in the CSC environment. Further, [20] carried out the feasibility of a study on machine learning models for cloud security to test the models in diverse operation conditions cloud scenarios. The authors compared Logistic Regression, Decision Tree, Naïve Bayes, and SVM classification algorithms techniques to learn a dataset for performance accuracies. The algorithms represent supervised schemes and are used in network security. The result shows an accuracy of 97% in anomalous packet detections. However, the work did consider CSC security from threat prediction in the supply chain environment. Furthermore, [21] surveyed data mining and ML methods for cybersecurity detection methods for cyber analytics in support of intrusion detection in cybersecurity applications. The authors used Artificial Neural Network, Association rules, Fuzzy Association rules and Bayesian Networks classifiers to learn the datasets and provided comparison criteria for the machine learning and data mining models to recognize the types of the attack (misuse) and for detection of an attack (intrusion). However, the techniques and methods used are not ML models and did not focus on ML and threat prediction in the CSC environment. Additionally, [22] review the cybersecurity dataset for ML algorithms used for analysing network traffic and anomaly detection. The author compared the machine learning techniques used for experiments, evaluation methods and baseline classifiers for comparison of the dataset. The results show significant flaws in some dataset during feature selection and are not relevant for modern intrusion detections datasets. However, the review did not stress on the current dataset we used from the Microsoft Malware Threat Prediction website for the prediction. Moreover, [23] explored the classification of logs using ML techniques on a decision tree algorithm to learn a dataset that models the correlation and normalization of security logs. The goal of the ML techniques is to evaluate if the algorithm can predict the performance of classification as an attack or not after a training phase. The dataset used contains anomalous and some identified attacks. The result shows that the DT algorithm was model on internet logs to develop a framework for the normalization and correlation of the classify with an accuracy of 80%. However, the classification model did not compare other classification algorithms such as SVM, LR and RF that are relevant for ML better performance accuracies and threat analysis.

Another initiative [24] explores the viability of using machine learning approaches to predict power systems disturbance and cyberattack discrimination classifiers and focuses specifically on detecting cyberattacks where deception is the core tenet of the event [24]–[30]. The authors in [24]

evaluated the classification performances on, NNge, OneR, SVM, RF, JRpper and Adaboost algorithms to learn the dataset and focused specifically on detecting cyber attacks where deception is the core tenet of the event. For example, in [25], the authors proposed a SCADA power system cyber-attack detection approach by combining a correlation-based feature selection (CFS) method and K-Nearest-Neighbour (KNN) instance-based learning (IBL) algorithm. The combination was useful to reduce the extremely large number of features and to maximize cyberattack detection accuracy with minimum detection time cost. In [26], an ensemble-learning model for detecting the cyberattacks of SCADA-based IIoT platform is proposed. The model was based on the combination of a random subspace (RS) learning method with random tree (RT). The authors in [29] proposed a deep-learning, feature-extraction-based semi-supervised model for cyberattack protection in the trust boundary of IIoT networks. The proposed approach was adaptive to learn unknown attack. However, the works did not consider CSC attacks from supplier inbound and outbound chains.

Regarding ML predictive analytics on various datasets, [28] predicted cybersecurity incidents using ML algorithms to distinguish between the different types of models. The authors used text mining methods such as n-gram, bag-of-words and ML techniques to learn dataset on Naive Bayes and SVM algorithms for classification performance. The experiment was to predict classification accuracies of malware incidents response and actions. The approach did not consider CTI and ML in the CSC system environment. Further, [29] proposed a risk teller system that analyses binary file appearance logs of a machine to predict which machines are at risk of experiencing malware infection in advance. The authors used a random forest algorithm and semi-quantitative methods to build a risk prediction model that creates a profile to capture usage patterns. The results associate each level of risk to a machine infection incident with 95% true positive precision. Besides,[30] characterize the extent to which cybersecurity incidents can be predicted based on externally observable properties of an organization's network. The authors used Verizon's annual data breach investigation report to forecast if an organization may suffer cybersecurity incidents in future. A random forest classifier was used against over 1000 incident reports taken from various datasets. The predictive result achieved an overall accuracy of 90% true positives. However, the work did not provide any inference and map the prediction to existing attacks. All these works above are important and contributed towards the improvement of cyber security by using various ML techniques. However, there is a lack of focus on the overall CSC security context. A limited works emphasize on threat intelligence data for the attack predication. For instance, due to the invisibility nature of cyberattacks, an attack on the CSC system network node has the potential to cascade to other nodes on the supply chain system. Therefore, it is necessary to use ML analytics to predict cyberattacks, threats and the underlying vulnerabilities. Additionally, there is a need to understand an organisational context for the threat analysis. CTI can effectively support to achieve that goal. This work contributes towards this direction. We have integrated CTI for threat gathering and analysis with the ML for the threat prediction so that organizations can determine the suitable control measure for the overall CSC security improvement.

III. FRAMING CONCEPTS

This section presents the conceptual view of the proposed approach by combining concepts from both CTI and CSC.

A. CSC THREAT MODELLING CONCEPTS

This section considers the concepts that are necessary to determine CSC vulnerabilities, goals, requirements, attacks the cyber supply inbound and outbound chains security and the CTI domain [2]. Threat modelling provides a systematic approach to identify and address the possible threats based on a specific context. It provides an understanding of threat actor who can attack the system and possible assets which can be compromised. The proposed approach considers a list of concepts that aid understand the threts and possible mitigation. The concepts provide a view of the relationships between organizational and security goal, requirements, threat actors, attacks, vulnerability, TTPs and indicators of compromise for understanding of the threat. An overview of the concepts is given below:

Goal: A goal represents the strategic aim of an organization. Properties for the goal include the organizational goal, the tangible assets required such as infrastructures to achieve the goal and intangible asset such as credit card information, health record, and other sensitive data for the security goal. The organizational goal is the process, product or service that is carried out. The assets are tangible and intangible assets including the network infrastructures. The security goal is the mechanism, configuration, and control put in place to achieve the goal.

Actor consists of perpetrators, system users, the systems, the third-party vendors, and companies whose services and networks systems are attached to the main organization's supply chain system. The threat actors are those consist of users, agents, cybercriminals, and other systems that aims at compromising the CSC systems and the security goal [8]. The threat actor could be an internal or external attacker. The CSC system includes the various integrations of network nodes that make up the supplier chain system. The third-party vendors include the organization on the supplier inbound and outbound chains that could be attacked, manipulated, or compromised.

Inbound and Outbound Supply Chain: In a CSC environment, the network nodes and communication channels are those that integrate with the inbound and outbound supply chains systems. These are vendors, SMEs, suppliers, and distributors that are on the supply chain. The inbound suppliers are those with external remote access to the CSC system. The outbound chains are those that the organization distributes including individuals, institutions,

and vendors. The organization can experience attacks on the supply inbound and outbound chain that supports the application processes [8]. The threat actor could initial injection attacks or insert a redirect script into the vendor's website and breach the software developed by the manufacturer that is used by the organization's internal employers to distribute services to vendors and individuals. The goal of the attack could be to manipulate, alter or divert products and services after gaining access into the system.

Vulnerabilities: CSC vulnerabilities are the loopholes and configuration flaws that exist on the supply chain system and network nodes that could be exploited by an attack, threat actor or a threat agent. These network vulnerabilities [36] are those that exist on the supply inbound and outbound chains including the network nodes, switches, IP addresses, and firewalls. The vulnerable spots on the CSC system could be identified from various sources including the software, the network, website, the user, processes, the application, and configuration or the third-party vendor. Properties include asset type, source, node, effect and criticality.

Attack: An attack is any deliberate action or assault on the supply chain system with the intent to penetrate a system, to be able to gain access then manipulate and compromise processes, procedures, and delivery channels of electronic products, the information flows, and services [2]. Properties include the type of attack, pattern, prerequisites, and vectors. We consider attack inputs and outputs parameters for our study and the attack concepts for our prediction. Inputs of attack include the tools, capabilities, vectors and knowledge of the vulnerabilities of the domain to exploit. Outputs of the attacks are the patterns, access gained by the threat actor, the methods deployed, TTPs, the loopholes exploited, and the extent of malware propagation and cascading effects. This includes those attacks on cyber physical and cyber digital systems such as hardware, network, IP addresses, and software. The OT and IT delivery mechanisms could be manipulated before the product gets to the consumer [8].

Tactics, Techniques and Procedures (TTPs) consist of the specific adversary behaviour exhibited in an attack [14]. It leverages on resources such as tools, infrastructures, capabilities and personnel. It provides information on the victim's target (who, what or where), that are relevant to exploit targets being targeted, intended effects, kill chain phases, handling guidance and resources of the TTP information [8], [9]. Threats actors' mode of operation is to commit attacks such as Hijacking, social engineering, and footprints, privilege escalation, and reconnaissance penetrate a supply chain.

CSC Requirement: CSC requirements are the constraints and security expectations for the system required to support CSC stakeholders and business needs. The data gathered from stakeholders inform business processes, system infrastructures, internal and external user expectations required for the supply chain system developments and operations [2]. The requirements process and constraints that are generated during the requirements engineering phase forms the basis for the system constraints and statements that support the user and system requirements used to achieve the organizational goal. The requirements consist of attributes such as user categories, stakeholders, description, user ID, acceptance criteria, time constraints, owners and sources. The requirements concepts include properties such as organizational requirements, business requirements, system, user, and operational requirements. The organizational requirements describe the organizational high-level objectives that must be performed to achieve the organizational goal. The business requirements explain the requirement specifications and the properties include customer needs and expectations that must be integrated to meet the system requirements. Systems requirements demand specific properties of the application, architecture and the technical requirements need to be able to describe the features and how the system must function. These system requirements properties include the constraints, assumptions and acceptance criteria and the external entities that will be interacting with the system. They include supply chain systems processes and constraints that are generated during the requirements engineering phase that forms the basis for the system.

Indicators: Indicators are parameters that express an attack of this type, whether it is imminent, in progress or has occurred [32]. Properties required to determine the indicators of compromise includes incident type, source, date & time, impact, motive and intents. The properties are used to determine threat activities, adversary behaviours, TTPs, risky events, or state of the incident to determine what could serve as an indicator of compromise. CSC attack incidents and course of actions provide intelligence about the nature of cyberattack indicators and TTPs that can be deployed on the supply chain especially from the third-party vendor's perspective. Indicators convey specific observable patterns combined with contextual information intended to represent artefacts and or behaviours of interest within a cybersecurity context.

Cyber incident report: Cybersecurity incident is defined as a breach of system security to affect its integrity or availability. It includes unauthorized access or attempted to access a system or causing a disruptive event to essential services. Cybersecurity incident reporting platform provides individuals and organizations with a system to reports cyber incidents they have experienced unexpectedly or any unusual network issues, or suspected fraud or cybercrime activities [31]. Properties for cyber incident reporting include attack type, date and time of the incident, source of the attack, cause of an attack, duration, impact on service, impact on staff and public safety Cyber incident report system is required for cyber threat analysis and to determine the threat level and categorizing. It is used to predict cyberattacks and generate intelligence require to mitigate cyberattacks and for threat information sharing.

Threat information sharing: Threat information sharing is used to provide information necessary to assist an organization in identifying, assessing, monitoring, and responding to cyber threats [32]. Cyber threat information includes

indicators of compromise, tactics, techniques, and procedures used by threat actors, security alerts and threat intelligence reports. It provides findings from the analysis of cyber incidents and suggests actions to take to prevent cyber-attacks, detect, protect, contain, and mitigate cyber incidents. Properties for cyber threat information sharing include information-sharing goals, information sources, scope, sharing community and support. Some rules govern and protect information sharing, such as information sensitivity and privacy, sharing designations, and tracking procedures [32]. It provides a basis for an organization to leverage their combined knowledge, information, experience, and competencies to gain intelligence and understanding of potential threats for remediation and controls.

Controls: Controls are security mechanisms that are put in place to secure organizational business operations and processes. They are security strategies and measures formulated and implemented to ensure that the organizational goal and objectives are achieved [2], [13]. These controls include directive, detective, preventive, corrective and recovery. Directive controls are more strategic and relevant with the specific supplier inbound and outbound chain requirements. These are intended to align organizational and security goals with that of supplier and third-party vendors on the supply chain and provide guidelines for system usage and processes. Preventive controls are policies that are put in place for the technical and physical infrastructures protection. These are derived from standard measures intended to preclude actions violating policy or increasing third party risks to the supply chain system resources. Detective Controls use supply chain attack indicators to identify practices, processes, and tools that identify and possibly react to security violations. These include Firewall, IDS, IPS and the various configurations required for the supply chain systems. Corrective controls involve physical, administrative, and technical measures. Recovery controls includes backup plans, regular updates and contingency planning to ensure integrity or availability of the CSC in the event of an incident. Once an incident occurs on the CSC system that results in the compromise of integrity or availability, the implementation of recovery controls is necessary to restore the system or operation to a normal operating state. These include countermeasures, backups, segmentation, and an incidence response strategy.

The meta-model in Figure 1 explains relationships among the concepts. The organizational goal is determined by the product and services that are produced. The security goal is to ensure that the supply chain systems that support these products and services are secured. CSC organization needs a list of requirements to satisfy for achieve its goals. The TTP as a CTI properties exploits both inbound and outbound vulnerabilities for a successful attack. Cyber incident report provides a detailed about the incident including vulnerability, indicator and incident time frame. This report needs to share among the CSC stakeholders. There are controls which are required to tackle the threats.

IV. THE PROPOSED APPROACH

This section discusses the proposed approach that aims to improve the CSC security. It includes an integration of CTI and ML and a systematic process (presented in the Section 5). Additionally, the underlying concepts of the proposed approach such as actor, goal, TTP, vulnerability, incident, and controls, is also mentioned in Section 3. The approach considers both inbound and outbound chains for the vulnerability so that CSC organisation can focus on the possible system flaws. The approach adopts the CTI process to gather and analyse the threat data and ML techniques to predicate the threat. ML techniques are used on classification algorithms to learn a dataset for performance accuracies and predictive analytics. The rationale for integrating CTI and ML for threat prediction is that the CTI lifecycle process supports input parameters for detecting known attacks whereas ML provides output parameters for predicting known and unknown attacks for future trends.

A. INTEGRATION OF CTI AND ML

The approach combines CTI processes with ML techniques for cyber threat predictive analytics. The goal is to detect vulnerabilities and indicators of compromise on CSC network system nodes using known attacks to predict unknown attacks. We apply the CTI techniques to gather threats (Known attacks) and ML techniques to learn the dataset to predicate cyber threats (unknown attacks) on CSC systems. The inputs are the attacks and TTP that are deployed by threat actors to compromise a system. The attack feature uses properties such as attack type, pattern, attack vectors, and prerequisites to determine the nature of the attack that was deployed. The TTP consists of attack patterns and attack vectors deployed by the threat actor. The TTP parameter includes the capabilities of the threat actor and threat indicators. The threat actor feature uses properties such as user, system and third-party vendors to determine the vulnerable spots and type of tools used for the attack to determine the attack pattern. Tools are the attack weapons or software codes used by the threat actor for reconnaissance and to initiate an attack. For instance, the threat actor could use Nmap tool for scanning a network, Kali Linux tool for penetration and, Metasploit tool for exploiting loopholes in a network. The output parameters are the vulnerabilities and indicators of compromise that are used as threat intelligence. The capability of the threat actor could be determined by the ability to penetrate a system and course Advance Persistent threat (APT) attack and take command and control C&C) the extent of propagation is used to determine the indicators. Finally, we consider various controls such as directive, preventive, detective corrective and recovery required to secure the CSC system.

The rationale for our predictive analytics approach is based on the premise that the cyberattacks phenomenon includes a lot of invincibility, and uncertainties and the makes the threat landscape unpredictable. Similarly, due to the changing organizational requirements, various integrations, varying business processes and the various delivery mechanisms,

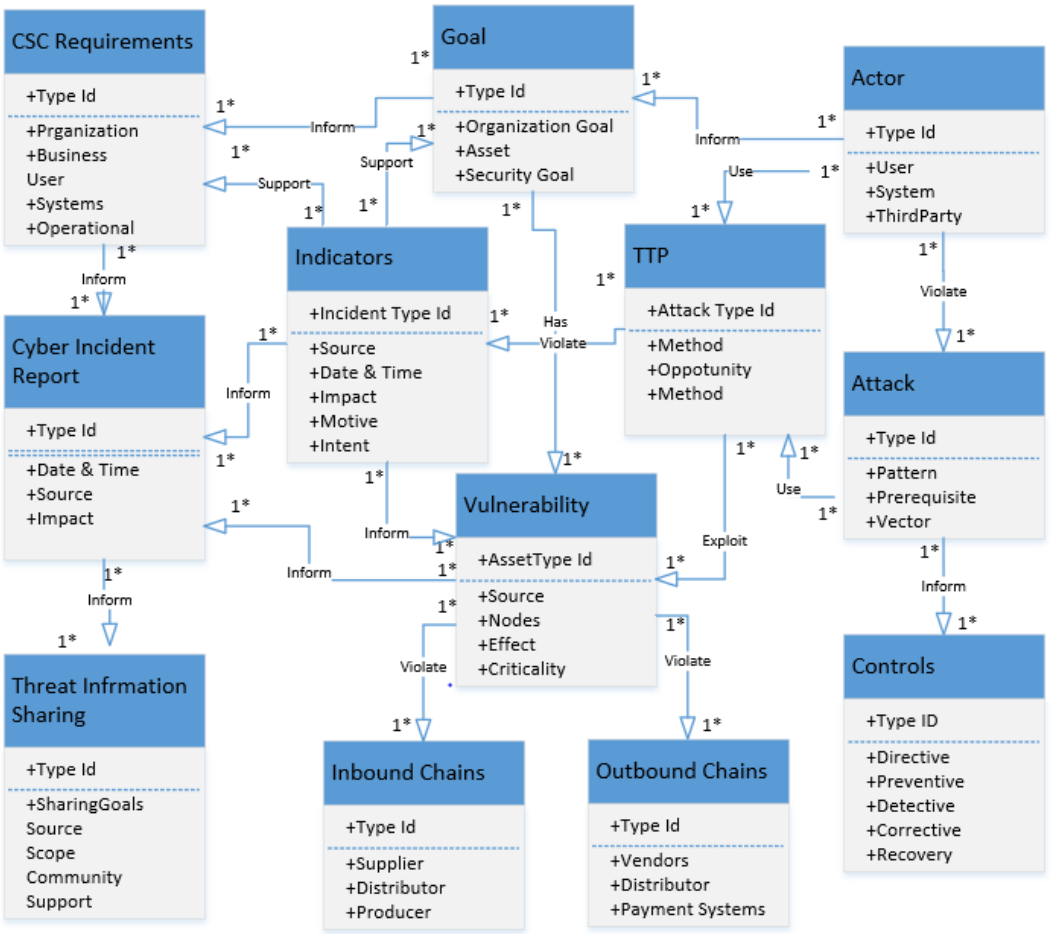


FIGURE 1. Meta-model for the proposed conceptual view of CSC system security.

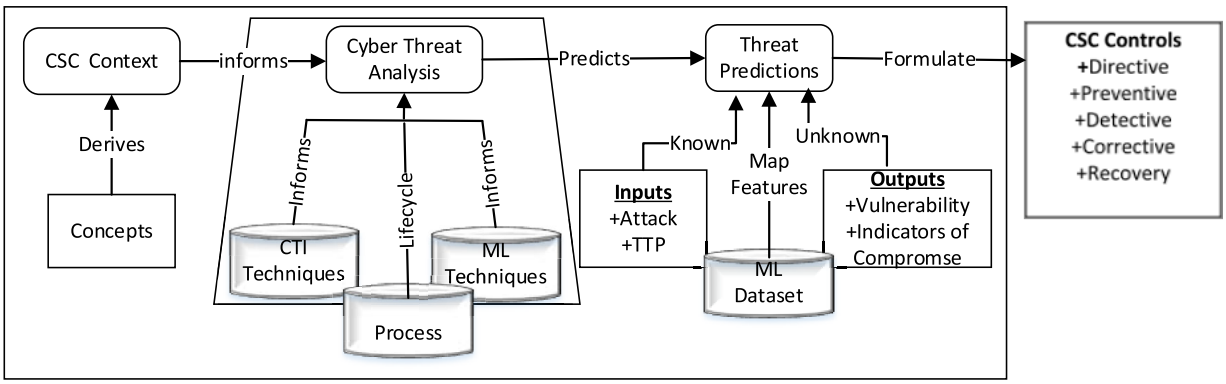


FIGURE 2. Applying CTI and ML for threat intelligence and predictive analytics.

predicting cyberattacks in the CSC organization context has been challenging. To achieve that, first, the proposed approach considers relevant related works and the meta-model concepts to model the CSC attacks and CTI phases. For instance, we identify supply inbound and outbound chain attack indicators and integrate them into CTI phases. Further, the concepts are analysed using the CTI process lifecycle and ML techniques to learn the dataset for our prediction. Furthermore, we use the input and output parameters as indicators for our threat prediction. Finally, the threat prediction results are evaluated to provide informed intelligence regarding the various attacks and future threats that are unknown for appropriate control mechanisms. Figure 2 indicates the proposed approach.

V. THREAT ANALYSIS AND PREDICTION PROCESS

This section discusses the overall process for the CSC threat analysis, prediction, and control in line with the proposed

approach in Section 3. The process includes four sequential phases. It follows a methodical approach and a causal process for each phase to determine strategy, threat analysis, threat prediction, and controls. Each phase includes steps and activities required to achieve the purpose of the phases as shown in Figure 3. The activities include identifying the organization's CSC and security strategy, ML classifications, infrastructures, attack context, input and output parameters for our prediction. The activities for the threat analysis phase include the identification and gathering of threat information, risk assessment and analysis to determine the threat actor, threat profile, TTP and IoC. The activities for the threat prediction phase consider the input parameters for the ML algorithms, predict threats and for performance evaluation by using ML techniques to learn datasets. The control activities include identifying required controls for the CSC systems including internal and external audits to formulate security policies and control mechanisms. We expound on the phases and process further by following the process flow as shown in Figure 3.

A. PHASE 1: DETERMINE STRATEGY

CSC security strategy combines CTI and cybersecurity risk strategy including mechanisms, resources and plans to determine how security goals and controls will be formulated, implemented, and achieved in line with organization goal and objectives. It includes identifying, analysing, reviewing and evaluating organizational assets including infrastructures, resources and implementation procedures. CSC security strategy combines, CTI and cybersecurity risk assessment strategy to gather intelligence and formulate policies. Strategic, tactical and operational management roles and responsibilities are recursive and support each other to ensure security goals are achieved. Strategic management uses intelligence decision to support plans that determine security goals and assign responsibility including executive authorization of blueprints and budget allocation. Tactical management decision regarding the execution of strategic management blueprints including security requirements capturing, third party audit, configuration management plans, uses indicators of compromise to determine controls and validations. The operational level managers ensure the day-to-day implementation of the security goals including monitoring, determining TTPs and escalating threat alerts for remediation and controls. CTI Strategy provides management evidence-based knowledge gathered about threats actors, attacks, patterns, vectors, vulnerabilities, TTPs, motives, intents and capabilities of the adversary. Risk Assessment Strategy considers the organizational goal and assets and develops an overall CSC risk strategy that determines the policies required to guide the organizational business processes. It includes risk assessment, CSC requirements capturing and business function. The risk strategy also considered implementation strategies and procurement policies for OT and IT acquisitions and integrations of assets.

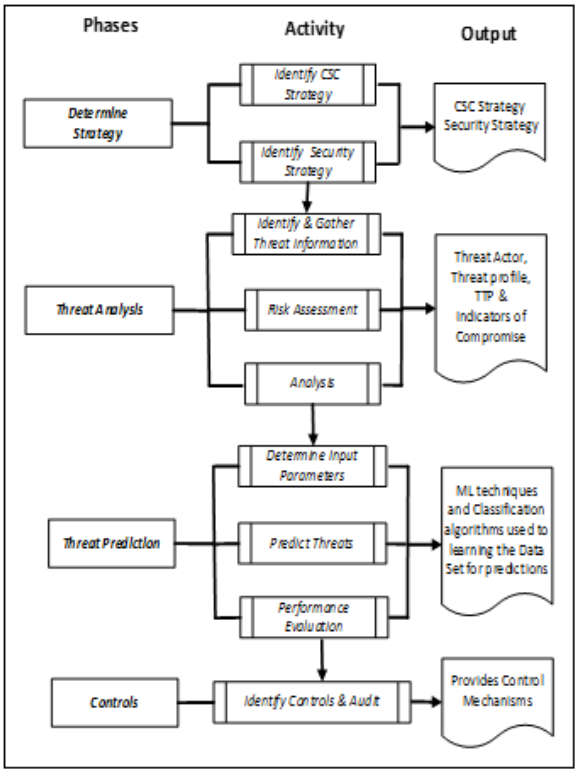


FIGURE 3. Predictive analytics process.

B. PHASE 2: THREAT ANALYSIS

This threat analysis phase follows the CTI techniques to determine and analyse the threats of the CSC context. It requires the CSC strategy information for his purpose and includes three activities.

Activity 1: Identify and Gather Information

This step identifies all vulnerable spots on the supply inbound and outbound chains on the meta-model that is used as indicators for an attack. For instance, in case of a malware attack, this activity looks for the relevant information such as the source of the attack, the tools, patterns and the attack vectors from the analysis of the malware attack that used as our indicator. To determine the indicators of an attack, we use threat activities, adversary behaviours, risky events, or state of the incident to determine what could serve as an indicator. The indicators may be used to identify any inherent vulnerabilities that could be exploited by a threat actor. If necessary, the activity carrying out penetration testing, vulnerability assessment test and threat propagation exercises to determine the supply inbound and outbound chains on the OT and IT by following the below stages [2].

Activity 2: Identify and Gather Information

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

we use threat activities, adversary behaviours, risky events, or state of the incident to determine what could serve as an indicator. The indicators may be used to identify any inherent vulnerabilities that could be exploited by a threat actor. If necessary, the activity carrying out penetration testing, vulnerability assessment test and threat propagation exercises to determine the supply inbound and outbound chains on the OT and IT by following the below stages [2].

- Stage 1. Reconnaissance: The threat actor uses APT methods to gather intelligence and searches the organization's websites to gather footprints and identify vulnerable spots on the network nodes.
- Stage 2. Experiment: The threat actor uses penetration testing and vulnerability assessment methods various attack patterns, TTP methods, and tools to explore vulnerable spots. The attacks include spear phishing malware or Remote Access Trojan.
- Stage 3. Exploit: the threat actor initiates attack to gain access to the system and other resources of the system. The attack could manipulate, alter and redirect deliveries or initiate and propagate malware.
- Stage 4. Command and Control**:** The threat actor maintains a continuous presence on the system and can change his password to maintain a presence on the CSC using advanced persistent threat attack, remote access command to steal intellectual properties and cause cyber espionage attacks. Most organizations use automated password changing system that prompts users to change their password periodically and that could be exploited by the threat actor. The threat actor can change the password and obfuscate in a Command & Control environment [2].

Activity 3: Risk Assessments

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

Activity 4: Analysis

This activity focuses on analysis of the threats to determine the actual source of the attack, the type of attack, the attack pattern, the TTP and attack vectors. This will assist to assign the IoC required and what controls are needed. The threat analysis techniques include:

- Stage 1. Threat Activity: Determine the nature of attack, pattern and sources of penetration on the CSC.
- Stage 2: Threat Manipulation: Determines the nature of cybercrimes committed and the extent of the penetration to understand the capabilities, motives and intents of the attacker.
- Stage 3: Threat Impact: Determines the severity of the attack, malware propagation and the cascading effects on the supply chain. These determinants influence the risk factors and the degree of severity of the attacks.

C. PHASE 3: THREAT PREDICATION

The phase considers CSC system nodes that are vulnerable to cyberattacks by integrating CTI and ML to obtain attack predictions of known and unknown attacks using three sequential activities.

Activity 1: Determine Input Parameters

The input parameters mainly consider the attack and TTP to demonstrate how the attackers penetrate a system. In particular, threat actors' properties such as capability and attack vector, tools are used for the input parameters.

- Step 1: Feature Selection: This step includes different ML techniques to select the available features that exist in the data. These feature selection techniques include dimensionality reductions in large datasets for effective and reliable training, testing and prediction. The features we use for our prediction are malware, spyware, spear phishing and Rootkit attacks.
- Step 2: Choosing a Classifier and Performance Metrics: We classify the various algorithms such as LR, DT, SVM and RF in VM to determine (1) the different types of responses based on an attack and (2) different types of response give the TTP deployed. For our study, we use the binary classification as it supports AUC-ROC in distinguishing between the probabilities of the given classes. Further, its precisions can predict correct instances, provides a harmonic mean of precision and recall for the F-score. Determining the right performance metrics to evaluate the algorithms, influences the performance measures and how the algorithm are compared with others. Not using the right metrics could cause overfitting problems and impact on how we evaluate our predictions.

Activity 2: Predict Threats

This activity aims to predicate vulnerabilities and IoC as output feature. The vulnerabilities provide the organization intelligence about areas that are exploitable and the IoC provides the indicators of penetrations, cybercrimes compromises, APTs and C&Cs. Using the cyber threat analysis and the inputs features, we use ML techniques and dataset to predict the output features. The vulnerable spots include network nodes, firewalls, antivirus and anti-malware. The IoC includes the unknown attacks and the extent of cybercrime manipulations, alteration, deletions, exfiltration and redirections that the threat actor could deploy on the system. The stealthy nature of such attacks is so uncertain it cannot be determined on the face value. This includes gathering various attack probabilities and their propagation effects on the CSC using ML techniques to train and test dataset to learn and to gain accurate predictions. The process involves:

- Applying ML techniques to learn the data events from IDS/IPS and firewall logs to collect signatures, threat indicators and, antimalware logs from the various supply chain endpoints. The ML techniques consider LR, SVM, DT, RF and MV algorithms to determine the accuracies of our predictions.
- Determining false positives and false-negative rates.
- Analyse ML results, logs and alerts to understand the attack trends as identified in the initial process to gather intelligence as to what happened, how, why, when, who and where the attack is initiated from.

Activity 3: Performance Evaluation

The performance of the models will be evaluated based on the following values: True Positive (TP), True Negative (TN), False Positive (FP) and False Negative (FN). Further, the FP and FN will be determined based on the elements of the confusion matrix. We follow the following steps for the performance evaluation.

Step 1: Using Confusion Metrics to Determine TP and FP Outcomes

A confusion matrix is a two-dimensional matrix that evaluates the performance of a classification model with respect to a specific test dataset. It basically compares the actual target values with those predicted by the machine learning model. It provides a better understanding of the values by calculating the data in the matrix and analyse them to determine any positive or negative classifications. Four outcomes are determined when classifying the instances of the dataset. These include True Positive (TP), True Negative (FP), False Positive (FP) and False Negative (FN) rates. For instance, in an event where an instance is positive, and the outcome is classified as positive, its TP else its FP. Where the instance is negative and the outcome is classified as negative, it is counted as TN, else it is FN [15]. 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 that are considered as accurate. We use the following equation below to determine the TPR, TNR, FPR, FNR and the entropy.

$$AC = \frac{TP + TN}{TP + FP + TN + FN} \tag{1}$$

The recall or true positive rate (TPR) is the proportion of the total number of correct predictions. We consider the equation as:

$$TPR = \frac{TP}{FN + TP} \tag{2}$$

Finally, precision (P) is the proportion of the predicted positive cases that were determined as correct. Hence the formula:

$$P = \frac{TP}{FP + TP} \tag{3}$$

F-measure of F1 – Score (F) is used as the harmonic mean to determine the combinations of precision and recall. We use the formula as:

$$F = \frac{2(Precision\ X\ Recall)}{Precision + Recall} \tag{4}$$

Step 2: Determine Mean Absolute Error (MAE) and Mean Square Error (MSE)

MAE determines the sum of the absolute mean or normal curve of the difference vector between predicted and real values. Whereas MSE determines the mean or normal difference by taking the absolute value of the square root of the mean and convert the units back to the original unit of the output variable and provide a gross idea of the magnitude of the error. For us to predict real numbers or regressions, we used MAE and MSE. The activities include Import AUC-ROC Function, Import Mean Absolute Error, Import Mean Square Error, and Set Entropy Criterion. Entropy is a concept used in information theory to determine the measure of uncertainty about the source of data. It is a unique function that satisfies the four uncertainties axions in a confusion matrix and gives us the degree of disorganization in our data. In an event where a given set of data may contain random collections of unstructured data, and entropy formula is used to separate the positive and negative rates as follows:

$$\text{Entrophy(E)} = -a \log_2 a - b \log_2 b \tag{5}$$

where a = Proportion of positive examples and b = Proportion of negative examples. We use the formula to determine the results in our experiment. We ask the following question to derive the answer from the performance.

- TP = Did the model predicted correctly for the positive class as positive?
- TN = Did the model predicted correctly for the negative class as negative?
- FP = Did the model predicted incorrectly the negative class as positive?
- FN = Did the model predicted incorrectly the positive class as negative?

D. PHASE 4: CONTROL

This final phase aims to identify a list of controls that are to tackle the threat. The controls should ensure that the required security strategic and mechanism are put in place to mitigate the threats. This includes identifying security requirements, internal and external audit as well as threat monitoring and reporting. The process includes identification and review of existing controls, third-party audit and finally information sharing.

VI. IMPLEMENTAION

This section follows the implementation of the proposed approach to determine the applicability of our threat prediction. We only follow threat identification, prediction, and control phases for the implementation.

A. THREAT ANALYSIS

Threat analysis phase uses CTI approach to gather threat. We identify vulnerabilities on the network nodes, IP address,

IEDs and the threats that are linked to the organizational goal that provide us with threat indicators. This includes the TTP used by threat actors and their modes of operations. For our analysis, we adopt the attack concepts and the properties from the meta-model to determine the attack pattern and the TTP deployed on the CSC. The phase involves gathering sources of attacks, vulnerable spots, risks TTPs. Data are gathered from firewalls logs, collecting a signature, threat indicators and events from IDS/IPS, antimalware logs from the various endpoints.

B. THREAT PREDICATION

Further to the discussion in Section 4, threat prediction involves using ML techniques to learn dataset for threat predictions of known and unknown attacks. We follow the ML process for our threat prediction.

1) DESCRIPTION OF DATA

We have considered the widely used dataset from a Microsoft Malware website for the implementation [6]. The dataset is about malware attacks in the Microsoft endpoint system. The data was collected by Microsoft Windows Defender with over 40,000 entries, with 64 columns and each row represents different telemetry data entries. The data represents malware attacks identified on various endpoint nodes from different locations with machine identities, timestamps, organizational identifier and default browser identifiers designed to meet various business requirements. The rationale for using the dataset is that the dataset does not represent Microsoft customer's machine 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 the business process and interoperability.

The feature description includes MachineIdentifier that considers individual machine ID on the network, GeoNameIdentifier, provides IDs for the geographic region a machine is located in. DefaultBrowsersIdentifier, provides ID for the machine's default browsers. OrganizationIdentifier, provides ID for the organization the machine belongs in. Is protected, provides a calculated field derived from the Spynet Report's AV Products field. Processor considers the process architecture of the installed operating system. HasTpm, indicates true if the machine has TPM (Trusted Platform Module). Over, looks at the version of the current operating system. OsBuild, information indicating the build of the current operating system. Census_DeviceFamily AKA DeviceClass, indicates the type of device that an edition of the OS is intended for desktop and mobile. Firewall, this attribute is true (1) for Windows 8.1 and above if windows firewall is enabled, as reported by the service [6].

2) DATA PREPARATION

The activity involves uploading the data from a website APIs or an HTML file and selecting the data we need then save it as CSV file. We prepare the data by converting the average of the columns of the dataset. Furthermore, we loaded the data from a pre-prepared dataset by calling the categories of the machine learning identifier: The output generated 40,000 training datasets with 62 variables. Handling NaN (Not a Number) in 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 prints $62 - 8 = 54$. (8 columns removed).

3) FEATURE SELECTION

The main features are identified from the primary dataset that are relevant to our work. There were 62 features in the primary data and the focus is on the concepts of attacks, tools and vulnerabilities from our previous work. We characterized threat actor activities, including presumed intent and historically observed behaviour, for the purpose of ascertaining the current threats that could be exploited. Further, we identified eight vulnerable spots and their probability that the cyber attacker could exploit those spots namely the: Firewall, IDS/IPS, Vendors CSC system, Network, IP Addresses, Database, Software, and Websites.

4) BUILDING NEW FEATURES INTO THE DATASET

The features considered as input parameters for the predictions are the attack and TTP as discussed in Section 3.2. To achieve that, we determine the types of attack, tools, vectors, and capabilities for the input. we build the features in line with the existing dataset feature description in [6]. Further, features for predicting the attack inputs and outputs are identified by deriving new features that are in line with the existing datasets and features [6] in Table 2. These features and variables are related to the dataset for our work. Attack patterns are an abstract mechanism for describing how a type of observed attack is executed [32]. The output parameters are determined after our evaluation using the attack pattern, TTPs, vulnerabilities as indicators of compromise. Furthermore, the attack profiles for the ML prediction are built-in dataset. The main goal of our work is to be able to build attack profiles for our ML to predict which node is vulnerable and likely to be attacked. We may not be able to use exact features, but we consider characteristics that are correlated with them and are relevant to represent how the attacks are initiated and the vulnerabilities are exploited for our future prediction. Hence, many features that we analysed were chosen to represent the CTI and security awareness of the stakeholders.

5) CHOOSING AN OPTIMIZATION ALGORITHM FOR THE CLASSIFIERS

For us to choose the classifiers as discussed in Section 4.1.3. activity 1, step 2. we used a pipeline to connect the various classifications. We use the 10-Fold cross-validation to determine the parameter estimation. The 10-Fold cross-validation run and validate the parameter ten times on each algorithm as the values may change and may not generate the accurate

TABLE 1. Matrix to compute the accuracy, precision, recall and the F-score.

Number = 185	Predicted Yes	Predicted No
Actual Yes	TP = 180	FN = 20
Actual No	FP = 40	TN = 120

result when we run it only ones. For the test, we used 10-fold cross validation for more accurate predictive results. The GridsearchCV provides an exhaustive search over specified parameter values for an estimator. We combine all the four algorithms using Majority Voting (MV) algorithm in the classifiers to determine the mean score of the total results. Finally, we use ROC-AUC to distinguish between the accuracies of the binary classification for the predictions [32].

6) EVALUATING THE ACCURACY OF THE THREATS

We consider the following method to understand the confusion matrix as discussed in Section 5. The accuracy of the confusion metrics is the proportion of the total number of predictions that are considered as accurate. Using the equation in Section 5, we evaluate the accuracies (AC) of the metrics to answer the performance of the TP, TN, FP, FN rates in (V) as follows:

$$AC = \frac{180 + 120}{180 + 120 + 40 + 20} = 0.83 \tag{6}$$

Using the Table 3, and the algorithm, we answer the following question to derive the values for the performances. The False positive rate (FPR) determines the rate of negative cases that were incorrectly classified as positive.

• FP = Did the model predicted incorrectly the negative class as positive rates?

$$AC = \frac{40}{120 + 40} = 0.23 \tag{7}$$

The result indicates that FPR of 0.25 negative cases were incorrectly classified as positive. Whereas the true negative rate (TNR) is defined as the number of negative cases that were classified.

• TN = Did the model predicted correctly for the negative class as negative?

$$TNR = \frac{120}{40 + 120} = 0.75 \tag{8}$$

The result indicates TNR of 0.75 were the number of negative cases that were classified as negative.

Further, the false negative rate (FNR) is the proposition of positive cases that were incorrectly classified as negative.

• FN = Did the model predicted incorrectly the positive class as negative?

$$TNR = \frac{20}{180 + 20} = 0.1 \tag{9}$$

The results indicate that the FNR of 0.1 was the proposition of positive cases that were incorrectly classified as negative. The recall or true positive rate (TPR) is the proportion of the total number of correct predictions. We consider the equation as:

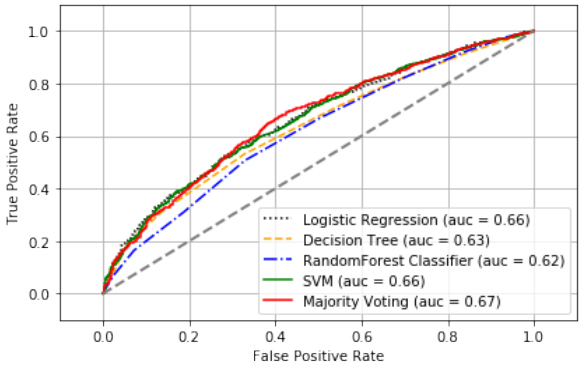


FIGURE 4. Plot the accuracy of all the algorithms in ROC curve for the LG, DT, RF, and SVM in MV.

• TP = Did the model predicted correctly for the positive class as positive?

$$TPR = \frac{180}{180 + 20} = 0.9 \tag{10}$$

The result indicates that the Recall or TPR of 0.9 was the proportion of the total number of instances that were identified correctly from the positive classes. To predict positive cases, we use precision (P) to determine the number of the proportion of instances is considered as correct. Hence the formula:

$$TPR = \frac{180}{180 + 40} = 0.81 \tag{11}$$

The final precision (P) of 0.81 was determined as the proportion of the total number of positive instances that were predicted correctly. The results show that the precision, recall and F-Score used to determine the accuracy and precision of the predictions are considered as accurate between the positive and negative rates. The result indicates that the F-Score of 0.85 was the harmonic mean between precision and recall. The Entropy is 0 if all member of E belongs to the same class, or 1 if they have the same number of samples in each group. The function entropy varies in range from 0 or 1.

7) ACCURACY OF THE ALGORITHMS IN ROC-AUC

Figure 4 depicts the ROC curve that determines the binary classifier system that determines the thresholds of the algorithms. We used AUC_ROC (Area Under Curve – Receiver Operating Characteristics) to model the selection metric for the bi-multiclass classification problem to distinguish between the probabilities of the given classes. AUC_ROC determines the True Positives Rates and False Negatives Rates. We plot the accuracy of all the algorithms in ROC. A 10-fold cross validation was used to determine the accuracy of the LR, DT, SVM and RF algorithms in the ROC. The black, orange, blue and green colours represent the algorithms. The x-axis represented as True Positive Rate and y-axis as False Positive rate. We used a python script to plot the graph as given in Figure 4:

8) 10-FOLD CROSS-VALIDATION

- [*ROCAUC* : 0.66 (+/ − 0.02) *LogisticRegression*]
- *ROCAUC* : 0.63 (+/ − 0.02) [*DecisionTree*]
- *ROCAUC* : 0.62 (+/ − 0.02) [*RandomForest*]
- *ROCAUC* : 0.66 (+/ − 0.02) [*SVM*]
- *ROCAUC* : 0.67 (+/ − 0.02) [*MajorityVoting*]

The results indicate that LG and SVM produced the highest results after we have used the ROC-AUC.

9) DETERMINING THE F-SCORE USING RECALL AND PRECISION RATES

For us to determine the precision, recall, and F-score, we answer the following questions regarding Table 1. Precision: how many positive instances were predicted correctly? Recall: how many instances were identified correctly from the positive classes? F-score: what is the harmonic mean between precision and recall? Using the results from evaluations in (I), we determine the F-Score and used the figures from the recall (0.9) and precision (0.81) to calculate the harmonic mean.

$$F = \frac{2 * 0.81 * 0.9}{0.81 + 0.91} = 0.85 \tag{12}$$

10) INCORPORATING ML AND CASE STUDY FOR EXPERIMENTATION

For us to determine the level of penetration, manipulation and the probability of an attack. We used a case study scenario of the remote CSC attack in [2] as below. The percentages figures were determined using the formula for calculating conditional probabilities in [2] from a low of 1 to a high of 100. The percentage figures in the penetration list are used for the result. The following is the scenario and the table from [2].

11) SCENARIO 1. REMOTE ATTACK ON THE CSC SYSTEM

The organization security team found that an adversary had intruded in the CSC system. The threat actor had compromised the workstation of the CMS that interfaced with suppliers, distributors, and third-party vendors. The organization's electronic products had been altered for some time. The CMS generated inaccurate customer electricity consumptions, which compromised the amount the customers were paying for their utility bills, their online payments, and third-party vendor systems. The organization used two types of payment systems, the prepaid system and post-paid system, that were all integrated into the CMS and HEMS. Using the formula for calculating conditional probabilities [2] and Activity 1 and Table 4, we determined the vulnerable spots, the severities of manipulation in percentages, and threat indicators. The percentages figures were calculated using the formula for calculating conditional probabilities. Further, the figures in penetration list are used to calculate the precision, recall and F-Score in Section 6 for the results.

VII. EXPERIMENTAL RESULTS

This section presents and analyses the results of the threat prediction. We follow a number of assessment parameters such as attack probability, TTP, vulnerable spots, and IoC for this purpose. The attack probability figures are derived from Table 2. The propagation is determined using a probability scale of 0–100%. A percentage score was given after calculating the degree of severity of each manipulation. Form low (≤15%), medium (16% to 59%), or high (above 60%).

- *Prediction of an attack probability.*

Table 3 presents the performance of the classifications of LR, DT, SVM, RF algorithms in identifying the various responses of cyberattacks based on the given malicious attack. From the table, LR achieved an accuracy of 66%, DT, 63% SVM 62% and RF 66%. Comparing the performance of the classifiers, LR and RF both performed better for the Precision, Recall and F-Score, whilst DT and SVM received a low precision, recall and F-score. Comparing that to the attack's categories signifies that Malware, Ransomware and spyware attacks identified different types of responses with 85% accuracy.

- *Prediction of TTP deployed based on the response of the cyberattacks.*

Table 4 presents the performance of the classification algorithms in identifying the various TTPs deployed, and responses based on the given attack vectors. Comparing the TTPs against the attack categories, XSS, session hijacking and RAT attack, DT and SVM achieved a low content for the low precision recall and F-score. However, LR received the highest precision and F-score for malware attack with 83% accuracy for TTPs deployed. Furthermore, ransomware and spyware attacks identified different types of responses for the TTPs with 83% accuracy for the harmonic mean in identifying the attack vectors being rootkit, email attachments and RAT.

- *Prediction of vulnerable spots based on the different types of responses of cyberattacks*

Table 5 presents the performance of the various classifications of the LR, DT, SVM and RF algorithms in identifying the vulnerable spots based on the different types of responses of cyberattacks. The vulnerable spots were identified from the CSC system probable threats table in [2] and used the manipulations figures for precision, recall and F-Score. LR and RF achieved a similar accuracy of 87% for the precision and F-score the successful attacks that signify the probability of exploits on the network nodes. Further, attacks such as malware and ransomware received higher precision based on the exploits and TTPS deployed with 92% accuracy. Whilst spear phishing, session hijacking and DDoS performs lower with the DT and SVM classifiers.

- *Predication of indicators of compromise (IoC).*

Table 6 presents the performance variations of the various classifications algorithms that identify what constitutes as indicators of compromise. With DDoS attack, RF presented the highest precision values of 83% compare to SVM indicating the extent of compromises on the network. LR received

TABLE 2. Probability and threat indicators.

Scenario	Vulnerable Spots	Penetration	Manipulation (%)	Probability	Threat Indicators
1	Firewall	Y	70	High	Wrong Firewall
2	IDS/IPS	Y	60	High	Configuration
3	Vendor	Y	80	High	Audit
4	Network	Y	40	Medium	Sub-netting
5	IP	Y	55	Medium	Segmentation
6	Database	Y	75	High	Sanitizations
7	Software	Y	75	High	Reprogram
8	Website	Y	90	High	SSL/TLS

TABLE 3. Predict the probability of an attack from the various endpoints.

ALGORITHMS	R			DT			SVM			RF		
ACCURACY (%)	**66**			**63**			**62**			**66**		
ATTACKS	**P**	**R**	**F**	**P**	**R**	**F**	**P**	**R**	**F**	**P**	**R**	**F**
XSS/Session Hijacking	0.88	0.38	0.65	0.58	0.42	0.68	0.55	0.38	0.63	0.88	0.38	0.65
Spyware/Ransomware	0.90	0.55	0.75	0.85	0.37	0.70	0.65	0.45	0.63	0.90	0.55	0.75
Spear Phishing	0.81	0.17	0.71	0.55	0.28	0.66	0.58	0.36	0.63	0.81	0.17	0.71
Session Hijacking	0.73	0.36	0.62	0.48	0.35	0.61	0.55	0.38	0.63	0.73	0.36	0.62
Rootkit/DDoS	0.56	0.37	0.65	0.57	0.33	0.58	0.53	0.35	0.63	0.56	0.37	0.65
RAT/Island Hopping	0.68	0.30	0.73	0.55	0.22	0.69	0.51	0.25	0.63	0.68	0.30	0.73
Ransomware/Malware	0.88	0.53	0.60	0.59	0.26	0.71	0.54	0.31	0.63	0.88	0.53	0.60
Malware/Spyware	0.81	0.48	0.68	0.58	0.51	0.73	0.55	0.45	0.63	0.81	0.48	0.68
DDoS	0.78	0.36	0.65	0.55	0.33	0.55	0.51	0.32	0.53	0.78	0.36	0.65

TABLE 4. Identify the different TTP deployed based on the response of the cyberattacks.

ALGORITHMS	LR			DT			SVM			RF		
ACCURACY (%)	**66**			**63**			**62**			**66**		
ATTACKS	**P**	**R**	**F**	**P**	**R**	**F**	**P**	**R**	**F**	**P**	**R**	**F**
XSS/Session Hijacking	0.82	0.26	0.55	0.55	0.31	0.61	0.55	0.27	0.56	0.82	0.26	0.55
Spyware/Ransomware	0.88	0.51	0.71	0.65	0.33	0.62	0.65	0.31	0.61	0.88	0.51	0.71
Spear Phishing	0.71	0.23	0.61	0.53	0.22	0.56	0.58	0.36	0.59	0.71	0.23	0.61
Session Hijacking	0.63	0.26	0.58	0.52	0.28	0.52	0.56	0.38	0.48	0.63	0.26	0.58
Rootkit/DDoS	0.51	0.27	0.63	0.51	0.31	0.58	0.48	0.35	0.57	0.51	0.27	0.63
RAT/Island Hopping	0.68	0.28	0.68	0.54	0.21	0.61	0.51	0.25	0.58	0.68	0.28	0.68
Ransomware/Malware	0.86	0.44	0.66	0.58	0.22	0.65	0.59	0.31	0.62	0.86	0.44	0.66
Malware/Spyware	0.79	0.41	0.67	0.65	0.51	0.63	0.55	0.45	0.61	0.79	0.41	0.67
DDoS	0.71	0.36	0.61	0.55	0.33	0.55	1.55	0.32	0.53	0.71	0.36	0.61

TABLE 5. Predict vulnerable spots based on the different types of responses of cyberattacks.

ALGORITHMS	LR			DT			SVM			RF		
ACCURACY (%)	**66**			**63**			**62**			**66**		
ATTACKS	**P**	**R**	**F**	**P**	**R**	**F**	**P**	**R**	**F**	**P**	**R**	**F**
XSS/Session Hijacking	0.63	0.60	0.61	0.65	0.61	0.62	0.61	0.59	0.60	0.62	0.59	0.61
Spyware/Ransomware	0.85	0.83	0.80	0.86	0.81	0.83	0.82	0.79	0.81	0.83	0.78	0.80
Spear Phishing	0.68	0.62	0.66	0.63	0.59	0.61	0.64	0.60	0.62	0.63	0.61	0.68
Session Hijacking	0.66	0.61	0.64	0.65	0.61	0.64	0.62	0.59	0.60	0.63	0.60	0.62
Rootkit/DDoS	0.64	0.60	0.61	0.63	0.61	0.58	0.61	0.57	0.59	0.64	0.38	0.58
RAT/Island Hopping	0.64	0.61	0.63	0.65	0.62	0.64	0.64	0.61	0.62	0.64	0.33	0.58
Ransomware/Malware	0.84	0.81	0.82	0.85	0.81	0.84	0.61	0.58	0.60	0.75	0.55	0.62
Malware/Spyware	0.82	0.77	0.81	0.86	0.83	0.85	0.85	0.81	0.83	0.66	0.45	0.69
DDoS	0.65	0.61	0.62	0.64	0.60	0.63	0.62	0.59	0.61	0.75	0.33	0.62

the highest precision and F-score for malware and spyware attacks, whereas RF and LR received the similar precision, recall and F-score.

VIII. DISCUSSIONS

The results for the predictive analytics are analysed in AUC_ROC as indicated in Figure 4. A 10-Fold cross-validation was used to run each algorithm to determine the parameter estimation and validated the accuracies. The evaluation of the accuracies of the metrics to answer the performance of the TPR, TNR, FPR, FNR as shown in Table 3. We determine the harmonic mean for the proportion of the total number of accuracies for the precision, recall, and F-score. The proportion for the precision is 220 for the

TABLE 6. Indicators of compromise (IOC). FOR performance variations of the various classifications algorithms.

ALGORITHMS	LR			DT			SVM			RF		
ACCURACY (%)	66			63			62			66		
ATTACKS	**P**	**R**	**F**	**P**	**R**	**F**	**P**	**R**	**F**	**P**	**R**	**F**
XSS/Session Hijacking	0.68	0.63	0.66	0.55	0.42	0.61	0.51	0.38	0.63	0.68	0.37	0.71
Spyware/Ransomware	0.80	0.8	0.75	0.85	0.55	0.70	0.65	0.45	0.63	0.78	0.52	0.76
Spear Phishing	0.81	0.17	0.71	0.55	0.65	0.70	0.55	0.45	0.63	0.77	0.17	0.68
Session Hijacking	0.73	0.66	0.62	0.55	0.65	0.70	0.55	0.45	0.63	0.73	0.65	0.62
Rootkit/DDoS	0.56	0.37	0.60	0.55	0.65	0.70	0.55	0.45	0.63	0.56	0.37	0.59
RAT/Island Hopping	0.68	0.30	0.33	0.55	0.65	0.70	0.55	0.45	0.63	0.68	0.30	0.63
Ransomware/Malware	0.70	0.33	0.62	0.55	0.65	0.70	0.55	0.45	0.63	0.72	0.33	0.60
Malware/Spyware	0.74	0.48	0.65	0.55	0.65	0.70	0.55	0.45	0.63	0.71	0.48	0.65
DDoS	0.68	0.56	0.65	0.55	0.65	0.70	1.55	0.45	0.63	0.68	0.56	0.57

TABLE 7. Mapping the attack category and predictive analytics.

Attack Category	CSC Attack Features	Threat Descriptions for Probable Cause of Attack	Threat Predictions (%)
1	XSS/Session Hijacking	Default Browser vulnerabilities and injecting a code in the URL or website	80
2-5	Spyware/Ransomware	Outdated Antivirus/Patches that are not updated regularly	90
6-7	Spear Phishing	Use Reconnaissance to identify vulnerable spots and attach email with a virus	80
8-9	Session Hijacking	Exploit Unchanged Hard-Coded password in software bought off the shelf	75
10-14	Rootkit/DDoS	Attack on BIOS or attach a virus to a USB key to cascade when booting.	80
15-20	RAT/Island Hopping	Attacks from Vendor systems to gain access to the organizational system	70
21-28	Ransomware/Malware	Exploiting outdated OS versions and encryptions especially TLS/SSL	60
29-35	Malware/Spyware	Packet injection and Resonance attacks	70
36-38	DDoS	Exploit IP Address Systems and Packet injections	55

number of positive instances that were predicted correctly. The proportion of recall (0.9) instances was identified correctly from the positive classes. The F-score of (0.85) was the harmonic mean between precision and recall. Hence, an accuracy of 85% is the total number of predictions that are considered accurate for the TPR and FPR. Further, we have a slight variation in our predictions of the TPF and FPR comparing the LR, DT, SVM, and RF algorithms in the pipeline and using MV for running them. However, the accuracy of the proportion of the total number of predictions remains accurate with an average of 65% and 30% as the combine values for the TPR and FPT respectively. Additionally, the results indicate that LG and SVM produced the highest results after we have used the ROC-AUC. The predictive analysis of our evaluation after we have used the CTI to gather information, gain knowledge and understanding of the organizational context and the situational awareness remains acceptable as compared to other literature that focused on ML only for predictions. The Table 7 shows the list the attack categories and threat predictions.

Table 6 combines the probability of attacks identified from previous work and map them with the feature descriptions of the threats to explains the predictive analytics [2]. The mapping includes attack categories, CSC attack features, and the threat describes for probable cause of attacks from the telemetry data and Microsoft endpoint protection threat report for the predictions. The attack categories were determined from the dataset of various threat descriptions from the telemetry data [23] that contains the properties of the various families of malware generated by the Windows defenders. The CSC attack features were derived from the various families of malware that has the probability of infecting the various CSC endpoint nodes. The threat descriptions were gathered by the threat report collected by the Microsoft Windows Defender [23]. The results specify that spyware/ransomware scored 90%. All the attack categories that score 80% indicated that an XSS or session hijacking could be deployed on the CSC website as uses public facing IPs it connects to various vendors. These could lead to spear phishing, rootkit and DDoS attacks. The rest of the threat prediction scores are explained in Table 7.

The paper reveals several observations made from the CSC attacks to using CTI lifecycle processes for intelligence gatherings, and ML for predictive analysis for the overall Smart CPS security improvement. The study revealed that several challenges are facing the organization in securing their systems as attackers are executing arbitrary commands on the supply chain systems remotely and manipulating systems.

A. MAPPING CYBERATTACKS ON CSC FOR PREDICTIVE ANALYTICS OF INDICATORS OF COMPROMISE

Table 8 provides details of how we mapped the cyberattacks on the CSC system for predictive analytics to determine the indicators of compromise. We used the threat modelling concepts in Section 3, and the properties to identify the

TABLE 8. Output parameters for indicators of compromise.

Cyberattack	Attack Pattern	Vulnerability	TTPs	IoCs
Malware	Insert a program in software	Untested Software	Insert Rootkit in code to hide in the system	Cascade to other networks nodes/ bypass antimalware
RAT	Hide in executable program, Backdoor code in an email attachment. HTTP Request Splitting, downloads	Network, Web and application server, Social Engineering, Phishing	Inject entry point identifier in the Explore Phase	Downloads itself when the user opens an email and provides access to the attacker
XSS	Embed malware in web browser content.	Programs that allow the remote host to execute codes and scripts.	Inject XSS payload and response split syntax in the user control input or URL	Injected scripts cascade to resources accessed by the applications
Ransomware	Social Engineering, Trojan, Botnets and Exploit kits to encrypt system files	Targets outdated antivirus and unpatched MS Windows application system	Map user environment, with documents, pictures and recycle bin and report content to C&C.	Calculate entropy of all file contents on the various systems, encrypt and propagate
Session Hijacking	Uses unauthentic HTTP cookies request from users.	Unencrypted websites, HTTP sessions, and open Wi-Fi connections	Insert network traffic that is not encrypted. Man-in-the-Middle attacks	Gain access and commits, APT, C5C and industrial espionage attacks.

TABLE 9. CSC security controls.

CSC Control	Descriptions	Asset	Approach	Implementation
Directive	Strategic management controls derived from the CTI and ML processes intended for policy formulation.	Identify Critical Assets and Security Framework that meet organizational goal	Map CTI gatherings and ML predictive analytics results to security goal	Assign controls to security teams to oversee the implementation. Adopt a framework or standard to support the development
Preventive	Proactive measures that are required to be implemented. Financial, physical, and technical measures intended to preclude actions violating policy or increasing risk to system resources.	Determine attacks that can exploit assets. Assign risks and threat levels to assets using CSCRM.	Determine Mitigations goals including internal and external audit controls	Create awareness by organize training and workshops to train users
Detective	Develop business impact assessment. Involve the use of practices, processes, and tools that identify and possibly react to security violations.	Implement periodic and ad-hoc security assessment using penetration testing and vulnerability assessment to pre-empt cyber threats	Use impact analysis and cost benefit analysis to determine the cost of alternatives of not investing in detection tools	Configure devices and automate passive tools on CSC systems to flag threats, run and monitor reports of firewalls, IDS/IPS, anti-malware and system updates
Corrective	Involve configurations and countermeasures designed to react to the detection of an incident to reduce or eliminate the zero-day attacks.	Design security policies that inform what must be done in the event of an incident	Develop Asset Inventory of all network nodes connected to the CSC organizational network including DHCP security	Implement Policies and business continuity plan to repair CSC systems, hard drive, patches systems, quarantine CSC systems
Recovery	Recovery strategy, Incident response and back up plans, regular updates, and contingency planning to ensure integrity or availability of the CSC system	Design policies and business impact assessment that can assist to restore the system or operation to a normal operating state upon any compromise as soon as possible.	Develop disaster recovery plan that will restore system to its operational state.	Form a team and Organize training and workshops to train staff to understand and be aware of the DRP implementations.

cyberattack, the attack pattern that were used, the vulnerable spots that were exploited, and the TTPs that are deployed by the threat actor on the CSC systems as the indicators of compromise (IoC). Indicators of compromise are parameters used

to express whether an attack-type is imminent, in progress or has occurred. Refer [2] further reading on threat modelling. Threat actors use sophisticated and stealthy methods to inject a virus, worms, bugs or a Trojan into software or in an HTTP request in an 'Island Hopping' attack. The intent is to penetrate the network or gain access to the webserver when a request is being processed. The motive could be to manipulate the vulnerable spots, alter the software and delivery channels and maintain APT and command & control presence.

Using the C&C methods, the attacker can modify products during manufacturing, manipulate it during distributions and the various domain attacks. These attacks could cascade to other nodes on the supply inbound and outbound chains. The table below provides a matrix that blends the input and output parameters for the prediction. Our observation is that the following vulnerabilities exist in the cyber supply chain system:

- The supply chain variables are accessible to the threat actor due to the business applications used for the supply chain variables and that could be exploited using incorrect user data.
- Information retrieved through inputted data is not configured properly due to poor validation.
- The variables are not well encapsulated to prevent software redirect. For instance, setting an input variable as public in a class when developing the software source codes makes the website open to external attackers.

B. MACHINE LEARNING FOR PREDICTIVE ANALYTICS

Machine learning approach to cybersecurity has been effective in analyzing and predicting future attacks and attack trends. We use ML techniques and classification algorithms including LD, SVM, DT, RF, and MV to develop threat intelligence techniques that can predict which nodes on our CSC system are venerable to attacks. We plot the accuracy of all the algorithms in ROC. AUC_ROC to determine the true positives and true negative rates. The results show that the best parameter result was SVM with an accuracy of 0.66. ML provides us with the ability to combine algorithms to determine which of them produced the highest accuracy and output for the best parameter for our prediction. However, it does not provide us with the ability to understand the threat actor's motives and intents.

C. COMPARING RESULTS WITH EXISTING WORKS

A stated in the related works, there have a lot of attention of using ML classifiers for cyber security. A vector space model is used for information retrieval for HTTP attacks using a decision tree algorithm to automatically label the request as malicious in the URL[11]. A number of classification algorithms LR, DT, NB, and SVM are considered for cloud security and tested the models in diverse operational conditions using cloud security scenarios[20]. Further, [21] used data mining and ML methods on Artificial Neural Network, Association rules, Fuzzy Association rules and Bayesian Networks classifiers for cybersecurity detection and analytics in intrusion detection security applications. Furthermore, [22] compared ML datasets used for analyzing network traffic and anomaly detection relevant for modern intrusion detections datasets. Moreover, [23], explored the classification of logs using a decision tree algorithm that models the correlation and normalization of security logs. Similarly, [24] compared NNge. LF, DT, Naïve Bayes, and SVM classification algorithms performance and ML predictions for power system disturbance and cyberattack discriminations. Then, [25] used an instance-based learning classification algorithm to learn a dataset for feature reduction and detection techniques to detect cyberattacks on smart grid. Additionally, [26] used an ensembled learning model based on the combination of a random subspace with random tree to detect cyberattacks on Industrial IoT networks. Likewise, [28] explored mitigating techniques on IoT cybersecurity threats in a smart city by using ML techniques to learn dataset on LR, SVM, DT, RF, ANN and KNN classifiers for anomaly detections. Further, [29] proposed a novel adaptive trust boundary protection for Industrial IoT network by using deep learning on a semi supervised model for detecting unknown cyberattacks. Furthermore, [30] used deep neural network discriminator on a down sample encoder cooperative data generator train the algorithm to capture actual distribution of attack model on industrial IoT attack surface. Additionally, authors in [31] predicted cybersecurity incidents by using Naive Bayes and SVM algorithms to investigate and analyse various datasets collected from SMEs. Finally, [32] model a risk teller system that used ML to predict which machines are at risk of getting infected or are clean and forecast if an organization may experience cybersecurity incidents in the future. Though all the works are relevant and contribute for the cyber security improvement. However, there is a lack of focus on the overall CSC security and ML classifiers are mainly used datasets for the threat predication. The proposed work presents a conceptual view by integrating relevant concepts from CSC and CTI domain. It provides a systematic threat analysis using the CTI techniques and integrates ML classifiers for the threat predication. Additionally, we considered LG, DT, SVM, RF algorithms in Majority Voting to learn the malware threat prediction dataset.

D. CSC SECURITY CONTROLS

There are various security controls in existence, whose effectiveness are based on existing CSC attacks and risks including CIS Controls 2018 and ISO27002:2011. We recommend the approach to address the CSC security using threat intelligence gathered from known and unknown attacks in line with organizational objectives and provide security recommendations. Some organizations provide a recommendation, however, not all may be relevant to the cyber supply chain organizational objective. Table 9 identifies basic concepts that are required to maintain security controls in the supply chain environment. To incorporate cybersecurity controls into a cyber supply chain system, we use knowledge of actual

CSC attacks that have occurred in the past. A compromised supply chain system provides us with the knowledge of previous attacks to continually learn from and build effective and practical defences mechanisms. To ensure proper CSC security controls, the organization must form a strategic team to identify, investigate, review and evaluate the supply chain system processes and applications.

E. THREAT INFORMATION SHARING

Threat information sharing is essential for any cyber physical system and specifically for the CSC context. It helps supply chain organisations and its stakeholders to aware about the current threat trends so that appropriate control can be identified to tackle the attacks. The CTI information includes threat landscapes, TTPs, tools, and intelligence reports. The threat intelligence is shared amongst the various organizations, institutions, vendors and businesses on the CSC system for strategic management decision making. It designates information and creates situational awareness on the various security alerts, assess and monitor threats, risk and existing controls. Due to the sensitive nature of the intelligence and privacy rules, these organizations are required to sign an agreement to ensure the following:

- Establish Information sharing rules
- Establish security system and audit rules
- Establish rules that govern the sharing of sensitive information
- Establish information classification rules. (Need to Know)

Challenges facing information sharing include the sensitivity nature of cyberattacks and the fact that it could lead to reputational damage, and sometimes legal ramifications. Most organizations are reluctant to share information relevant to CSC security.

IX. CONCLUSION

The integration of complex cyber physical infrastructures and applications in a CSC environment have brought economic, business, and societal impact for both national and global context in the areas of Transport, Energy, Healthcare, Manufacturing, and Communication. However, CPS security remains a challenge as vulnerability from any part of the system can pose risk within the overall supply chain context. This paper aims to improve CSC security by integrating CTI and ML for the threat analysis and predication. We considered the necessary concepts from CSC and CTI and a systematic process to analyse and predicate the threat. The experimental results showed that accuracies of the LG, DT, SVM, and RF algorithms in Majority Voting and identified a list of predicated threats. We also observed that CTI is effective to extract threat information, which can integrate into the ML classifiers for the threat predication. This allows CSC organization to analyse the existing controls and determine additional controls for the improvement of overall cyber security. It is necessary to consider the full automation of the process and industrial case study to generalize our findings. Furthermore, we are also planning to consider evaluating the existing controls and the necessary of future controls based on our prediction results.

REFERENCES

[1] National Cyber Security Centre. (2018). *Example of Supply Chain Attacks*. [Online] Available: https://www.ncsc.gov.uk/collection/supply-chain-security/supply-chain-attack-examples

[2] A. Yeboah-Ofori and S. Islam, "Cyber security threat modelling for supply chain organizational environments," *MDPI. Future Internet*, vol. 11, no. 3, p. 63, Mar. 2019. [Online]. Available: https://www.mdpi.com/1999-5903/11/3/63

[3] B. Woods and A. Bochman, "Supply chain in the software era," in *Scowcroft Center for Strategic and Security*. Washington, DC, USA: Atlantic Council, May 2018.

[4] *Exploring the Opportunities and Limitations of Current Threat Intelligence Platforms, Version 1*, ENISA, Dec. 2017. [Online]. Available: https://www.enisa.europa.eu/publications/exploring-the-opportunities-and-limitations-of-current- threat-intelligence-platforms

[5] C. Doerr, TU Delft CTI Labs. (2018). *Cyber Threat Intelligences Standards—A High Level Overview*. [Online]. Available: https://www.enisa.europa.eu/events/2018-cti-eu-event/cti-eu-2018-presentations/cyber-threat-intelligence-standardization.pdf

[6] Research Prediction. (2019). *Microsoft Malware Prediction*. [Online]. Available: https://www.kaggle.com/c/microsoft-malware-prediction/data

[7] A. Yeboah-Ofori and F. Katsriku, "Cybercrime and risks for cyber physical systems," *Int. J. Cyber-Secur. Digit. Forensics*, vol. 8, no. 1, pp. 43–57, 2019.

[8] CAPEC-437, Supply Chain. (Oct. 2018). *Common Attack Pattern Enumeration and Classification: Domain of Attack*. [Online]. Available: https://capec.mitre.org/data/definitions/437.html

[9] Open Web Application Security Project (OWASP). (2017). *The Ten Most Critical Application Security Risks, Creative Commons Attribution-Share Alike 4.0 International License*. [Online] Available: https://owasp.org/www-pdf-archive/OWASP_Top_10-2017_%28en%29.pdf.pdf

[10] US-Cert. (2020). *Building Security in Software & Supply Chain Assurance*. [Online]. Available: https://www.us-cert.gov/bsi/articles/knowledge/attack-patterns

[11] R. D. Labati, A. Genovese, V. Piuri, and F. Scotti, "Towards the prediction of renewable energy unbalance in smart grids," in *Proc. IEEE 4th Int. Forum Res. Technol. Soc. Ind. (RTSI)*, Palermo, Italy, Sep. 2018, pp. 1–5, doi: 10.1109/RTSI.2018.8548432.

[12] J. Boyens, C. Paulsen, R. Moorthy, and N. Bartol, "Supply chain risk management practices for federal information systems and organizations," *NIST Comput. Sec.*, vol. 800, no. 161, p. 32, 2015, doi: 10.6028/NIST.SP.800-161.

[13] *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*, NIST, Gaithersburg, MD, USA, 2018, doi: 10.6028/NIST.CSWP.04162018.

[14] J. F. Miller, "Supply chain attack framework and attack pattern," MITRE, Tech. Rep. MTR140021, 2013. [Online]. Available: https://www.mitre.org/sites/default/files/publications/supply-chain-attack-framework-14-0228.pdf

[15] C. Ahlberg and C. Pace. *The Threat Intelligence Handbook*. [Online]. Available: https://paper.bobylive.com/Security/threat-intelligence-handbook-second-edition.pdf

[16] J. Freidman and M. Bouchard, "Definition guide to cyber threat intelligence. Using knowledge about adversary to win the war against targeted attacks," iSightPartners, CyberEdge Group LLC, Annapolis, MD, USA, Tech. Rep., 2018. [Online]. Available: https://cryptome.org/2015/09/cti-guide.pdf

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

[18] A. Yeboah-Ofori and C. Boachie, "Malware attack predictive analytics in a cyber supply chain context using machine learning," in *Proc. ICSIoT*, 2019, pp. 66–73, doi: 10.1109/ICSIoT47925.2019.00019.

[19] B. Gallagher and T. Eliassi-Rad, "Classification of HTTP attacks: A study on the ECML/PKDD 2007 discovery challenge," Lawrence Liverpool Nat. Lab., Livermore, CA, USA, Tech. Rep., 2009, doi: 10.2172/1113394.

[20] D. Bhamare, T. Salman, M. Samaka, A. Erbad, and R. Jain, "Feasibility of supervised machine learning for cloud security," in *Proc. Int. Conf. Inf. Sci. Secur. (ICISS)*, Dec. 2016, pp. 1–5, doi: 10.1109/ICISSEC.2016.7885853.

[21] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 2, pp. 1153–1176, 2nd Quart., 2016, doi: 10.1109/COMST.2015.2494502.
[22] O. Yavanoglu and M. Aydos, "A review on cyber security datasets for machine learning algorithms," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Dec. 2017, pp. 2186–2193, doi: 10.1109/BigData.2017.8258167.
[23] E. G. V. Villano, "Classification of logs using machine learning," M.S. thesis, Dept. Inf. Secur. Commun. Technol., Norwegian Univ. Sci. Technol., Trondheim, Norway, 2018.
[24] R. C. B. 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 *Proc. 7th Int. Symp. Resilient Control Syst. (ISRCS)*, Denver, CO, USA, Aug. 2014, pp. 1–8, doi: 10.1109/ISRCS.2014.6900095.
[25] A. Gumaei, M. M. Hassan, S. Huda, M. R. Hassan, D. Camacho, J. D. Ser, and G. Fortino, "A robust cyberattack detection approach using optimal features of SCADA power systems in smart grids," *Appl. Soft Comput.*, vol. 96, Nov. 2020, Art. no. 106658, doi: 10.1016/j.asoc.2020.106658.
[26] M. M. Hassan, A. Gumaei, S. Huda, and A. Almogren, "Increasing the trustworthiness in the industrial IoT networks through a reliable cyber-attack detection model," *IEEE Trans. Ind. Informat.*, vol. 16, no. 9, pp. 6154–6162, Sep. 2020, doi: 10.1109/TII.2020.2970074.
[27] J. Abawajy, S. Huda, S. Sharmeen, M. M. Hassan, and A. Almogren, "Identifying cyber threats to mobile-IoT applications in edge computing paradigm," *Elsevier Sci. Direct Future Gener. Comput. Syst.*, vol. 89, pp. 525–538, Dec. 2018, doi: 10.1016/j.future.2018.06.053.
[28] M. M. Rashid, J. Kamruzzaman, M. M. Hassan, T. Imam, and S. Gordon, "Cyberattacks detection in IoT-based smart city applications using machine learning techniques," *Int. J. Environ. Res. Public Health*, vol. 17, no. 24, p. 9347, Dec. 2020, doi: 10.3390/ijerph17249347.
[29] M. M. Hassan, S. Huda, S. Sharmeen, J. Abawajy, and G. Fortino, "An adaptive trust boundary protection for IIoT networks using deep-learning feature-extraction-based semisupervised model," *IEEE Trans. Ind. Informat.*, vol. 17, no. 4, pp. 2860–2870, Apr. 2021, doi: 10.1109/TII.2020.3015026.
[30] M. M. Hassan, M. R. Hassan, S. Huda, and V. H. C. de Albuquerque, "A robust deep-learning-enabled trust-boundary protection for adversarial industrial IoT environment," *IEEE Internet Things J.*, vol. 8, no. 12, pp. 9611–9621, Jun. 2021, doi: 10.1109/JIOT.2020.3019225.
[31] A. Mohasseb, B. Aziz, J. Jung, and J. Lee, "Predicting cybersecurity incidents using machine learning algorithms: A case study of Korean SMEs," in *Proc. INSTICC*, 2019, pp. 230–237, doi: 10.5220/0007309302300237.
[32] L. Bilge, Y. Han, and M. D. Amoco, "Risk teller: Predicting the risk of cyber incidents," in *Proc. CCS*, 2017, pp. 1299–1311, doi: 10.1145/3133956.3134022.
[33] Y. Liu, A. Sarabi, J. Zhang, P. Naghizadeh, M. Karir, and M. Liu, "Cloud with a chance of breach: Forecasting cyber security incidents," in *Proc. 24th USENIX Secur. Symp.*, Washington, DC, USA, 2015, pp. 1009–1024.
[34] *Guide to Cyber Threat Information Sharing*, document NIST 800-150, 2018, doi: 10.6028/NIST.SP.800-150.
[35] S. Barnum, "Standardizing cyber threat intelligence information with the structured threat information expression," V1.1. Revision, STIX, USA, Tech. Rep., 2014, vol. 1. [Online]. Available: https://www.mitre.org/publications/technical-papers/standardizing-cyber-threat-intelligence-information-with-the
[36] A. Yeboah-Ofori, S. Islam, and E. Yeboah-Boateng, "Cyber threat intelligence for improving cyber supply chain security," in *Proc. Int. Conf. Cyber Secur. Internet Things (ICSIoT)*, May 2019, pp. 28–33, doi: 10.1109/ICSIoT47925.2019.00012.
[37] A. Boschetti and L. Massaron, *Python Data Science Essentials*, 2nd ed. Dordrecht, The Netherlands: Springer, 2016. [Online]. Available: https://link.springer.com/content/pdf/10.1007/BF00994018.pdf
[38] A. Yeboah-Ofori, "Classification of malware attacks using machine learning in decision tree," *IJS*, vol. 11, no. 2, pp. 10–25, 2020. [Online]. Available: https://www.cscjournals.org/manuscript/Journals/IJS/Volume11/Issue2/IJS-155.pdf
[39] W. Wang and Z. Lu, "Cyber security in smart grid: Survey and challenges," *Elsevier Comput. Netw.*, vol. 57, no. 5, pp. 1344–1371, Apr. 2013.
[40] C. Cortes and V. Vapnik, "Support-vector networks," *Mach. Learn.*, vol. 20, pp. 273–297, Sep. 1995, doi: 10.1023/A:1022627411411.

ABEL YEBOAH-OFORI received the B.Sc. degree in computing and information systems from UEL, the M.Sc. degree in information security and computer forensics, and the Ph.D. degree in cyber security from the School of Architecture, Computing and Engineering (ACE), University of East London, U.K. He is currently a Lecturer with the University of West London. He holds a Postgraduate Certificate in Higher Educations Practices (PgCert) and a Fellow of the British Higher Education Academy (FHEA). He is a Prince 2 Project Management Practitioner, Certified Cyber Security and Digital Forensics Investigations practitioner. He has published journal articles, reviewed a few articles, and provided consultancy services. He was invited in 2018 to participate in Cyber Security Maturity Assessment Program with the Global Cyber Security Capacity Centre, USA, Oxford University, and the World Bank. He was invited to an Advisory and Review Workshop 2017 on National Cyber Security Policy and Strategy by MoC and Council of Europe (CoE) as part of GLACY+ activities. His research interests include cyber security, digital forensics, cyber threat intelligence, cyber-attack modeling, cyber supply chain security and risks, and machine learning.

SHAREEFUL ISLAM was a Visiting Researcher with the National Institute of Informatics (NII), Japan, and SBA Research, Austria. He is currently working as a Senior Lecturer and a Programme Leader with the Cyber Security and Network Program, School of ACE, University of East London, U.K. His research interests include in the area of cyber security, requirement engineering, information systems, and risk management. He has pioneered work in developing risk assessment and treatment method using business and technical goals, modeling language for cyber security risk management. The works are implemented in various application domain including cloud migration, critical infrastructure, and information system. He has published more than 70 articles (H-index 23) and he has led and/or participated in projects funded by the European Union (FP7), Innovate U.K., FwF, and DAAD. He has experience of acting as an Evaluator for national and international funding bodies, including the EPSRC, FwF, and CHIST-ERA. He is a Fellow of the British Higher Education Academy (HEA) and a certified PRINCE 2 and Management of RISK (MoR) practitioner.

SIN WEE LEE received the B.Eng. degree (Hons.) in electronics and computing from Nottingham Trent University, U.K., and the Ph.D. degree in neurocomputing from Leeds Beckett University, U.K. He is currently working with the School of Architecture, Computing and Engineering (ACE), University of East London, U.K. He has published more than 40 refereed articles in high-quality journals and international conferences in neural networks, data analytics, and machine learning. His main research interest and field of expertise are in the neural networks and machine learning for data analytics.

ZIA USH SHAMSZAMAN (Senior Member, IEEE) received the Master of Engineering (M.Eng.) degree from the Department of CICE, Hankuk University of Foreign Studies, South Korea, and the Ph.D. degree from the Insight Centre for Data Analytics, National University of Ireland Galway, Ireland. He is currently working as a Senior Lecturer in computer science with the Department of Computing and Games, Teesside University, U.K. He was involved in several research projects funded by FP7, SFI, Cisco Inc., and ETRI. He worked in the ICT industry over seven years and also achieved few professional certifications, such as CEH, CDCP, CCNA, and JNCIA-ER. His research interests include the IoT, the social IoT, CPS, cybersecurity, artificial intelligence, deep learning, semantic web, and ontologies. He is an Advisory Panel Member in Elsevier.

KHAN MUHAMMAD (Member, IEEE) received the Ph.D. degree in digital contents from Sejong University, Seoul, South Korea, in 2019.

He is currently an Assistant Professor with the Department of Interaction Science and the Director of the Visual Analytics for Knowledge Laboratory (VIS2KNOW Lab), Sungkyunkwan University, Seoul. His research interests include intelligent video surveillance (fire/smoke scene analysis, transportation systems, and disaster management), medical image analysis, (brain MRI, diagnostic hysteroscopy, and wireless capsule endoscopy), information security (steganography, encryption, watermarking, and image hashing), video summarization, multimedia data analysis, computer vision, the IoT/IoMT, and smart cities. He is serving as a reviewer for over 100 well-reputed journals and conferences, from IEEE, ACM, Springer, Elsevier, Wiley, SAGE, and Hindawi publishers. He is an associate editor of four journals and an editorial board member of five journals.

METEB ALTAF received the Ph.D. degree from Brunel University London, London, U.K., in 2009. Since 2009, he has been with the KACST as an Assistant Research Professor. He was appointed as the Director Assistant for Administrative Affairs and the Director Assistant for Scientific Affairs with the National Center for Robotics and Intelligent Systems. After that, he was appointed as the Director of the National Robotics Technology and Intelligent Systems Center before it become known as the National Center for Robotics Technology and Internet of Things. He has been promoted as a Research Associate Professor. In the meantime, he became the Director of the Innovation Center for Industry 4.0, King Abdulaziz City for Science and Technology. He is currently the Director of the Advanced Manufacturing and Industry 4.0 Center. During his career life, he published number of articles in different well-known ISI journals and in well recognized conferences as well as he is lecturing at the Biomedical Technology Department, King Saud University. He has supervised more than 20 research projects locally and internationally as technology transfer projects.

MABROOK S. AL-RAKHAMI (Member, IEEE) received the master's degree in information systems from King Saud University, Riyadh, Saudi Arabia, where he is currently pursuing the Ph.D. degree with the Information Systems Department, College of Computer and Information Sciences. He has worked as a Lecturer with King Saud University, Muzahimiyah Branch, and taught many courses, such as programming languages in computer and information science. He has authored several articles in peer-reviewed IEEE/ACM/Springer/Wiley journals and conferences. His research interests include edge intelligence, social networks, cloud computing, the Internet of Things, big data, and health informatics.

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 13 June 2024, accepted 22 July 2024, date of publication 25 July 2024, date of current version 6 August 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3433404

RESEARCH ARTICLE

Research on Quantitative Prioritization Techniques for Selecting Optimal Security Measures

JANG JISOO[1], SUBONG JUNG[2], MYUNGKIL AHN[3], DONGHWA KIM[3], JAEPIL YOUN[4], AND DONGKYOO SHIN[1,5,6]

[1]Department of Computer Engineering, Sejong University, Seoul 05006, South Korea
[2]Defense Future Technology Laboratory, LIG System, Seoul 03130, Republic of Korea
[3]Cyber Technology Center, Agency for Defense Development, Seoul 05771, Republic of Korea
[4]Department of Joint Education, Joint Forces Military University (JFMU), Nonsan-si, Chungcheongnam-do 33021, Republic of Korea
[5]Department of Convergence Engineering for Intelligent Drones, Sejong University, Seoul 05006, South Korea
[6]Cyber Warfare Research Institute, Sejong University, Seoul 05006, South Korea

Corresponding author: Dongkyoo Shin (shindk@sejong.ac.kr)

This work was supported by the Defense Acquisition Program Administration and the Agency for Defense Development Project Name: Cyber Warfare Mission Impact Analysis Tool Development Prototype under Project UC220012XD.

ABSTRACT Many organizations and researchers, such as NIST, FIRST, MITRE, etc. in the United States, are conducting various cybersecurity research to counter the evolving cyber threats. Research on improving the security level of systems and networks by checking the network environment is one of the main areas of continuous research. To choose the right security countermeasures, you need to ensure that the defense techniques they contain are appropriate for your systems and networks. However, how to determine this is a difficult and complex issue, and as cyber threats evolve, how to determine this will need to evolve with them. To address these issues, this study quantitatively designed six metrics for defense technologies based on system and network environments and used them to conduct experiments on the entire network, as well as experiments on security countermeasures after a cyber-threat has caused damage in a virtual network environment. The proposed method was able to cover a large number of vulnerabilities relative to the number of mitigation techniques applied, and the prioritized list of mitigation candidates allowed us to select the appropriate list of defense techniques for the network. This research can be developed into an automated technology that collects vulnerabilities for the entire system of the network environment to be applied in the future, measures the defense level, prioritizes the complementary defense technologies, and lists them as defenses.

INDEX TERMS Cybersecurity, cyberspace, cyber warfare.

I. INTRODUCTION

Traditionally, anti-malware and anti-virus tools have been the primary tools and techniques for preventing cybercrime [1]. However, the complexity and diversity of current cybercrime has surpassed the capabilities of these traditional security tools. As a result, cybersecurity researchers believe that the development of new and effective security systems to counter threats is an urgent task [2]. Furthermore, one of the reasons for the in-crease in cyber threats is that cybersecurity policies need to be understood in the context of the ever-changing cybersecurity landscape. To this end, it is important to understand other countries' tactics, and most countries' cybersecurity policies focus on big picture issues such as national security, healthcare, and defense [3]. While cybersecurity technology is constantly evolving through research, cyber threat technology is also evolving. The U.S. has a number of cybersecurity research efforts to address evolving cyber threat technologies, including the National Institute of Standards and Technology's (NIST) Cybersecurity Framework,

The associate editor coordinating the review of this manuscript and approving it for publication was Alba Amato.

FIRST's The Common Vulnerability Scoring System (CVSS) 4.0, MITRE's Adversarial Tactics, Techniques and Common Knowledge (ATT&CK), and D3FEND. In addition, various studies have been conducted to block threats with similar patterns by learning known threats through machine learning, and this is a topic that will continue to be researched in the future [4], [5], [6], [7]. However, these studies are limited to responding to new cyber threat technologies because they only enhance security with threats with similar patterns within a set defense technology. To address these issues, this study investigated how to select appropriate cybersecurity technologies against cyber threats. The metrics were designed based on MITRE's ATT&CK [8], which categorizes information about the latest cyberattack techniques into a knowledge graph, and D3FEND [9], which categorizes cybersecurity technologies. The metric can quantify the latest security technologies as updated by D3FEND and ATT&CK. To validate the designed metrics, a virtual network environment with vulnerabilities was designed. Then, cyber-attack scenarios were designed and tested. As a result, we have selected a list of cybersecurity techniques that are optimized for network environments with limited resources. This means that the proposed method can be adapted to continuously evolving network and system environments, security technologies, and threats to improve the overall security level of enterprises and countries.

This research consists of five chapters. Section II describes related work, including MITRE's attack and defense technologies that serve as the background for this research, the current state of research by various organizations and researchers, and defense policies. Section II describes the structure of the methodology proposed in this study, including the design and methodology of metrics to quantitatively measure defensive behavior against cyberattacks. Section III describes the experiments using the method, and Section IV concludes with conclusions, future research directions, and comparisons with other studies.

II. RELATED WORK

A. MITRE's ATT&CK, D3FEND

ATT&CK [8], developed by MITRE Corporation, is a framework used in the field of cybersecurity. It is designed to effectively organize and share knowledge about cyberattacks and provides a cybersecurity standard terminology and taxonomy to provide information about attacker behavior patterns and attack techniques. This allows organizations to develop defensive strategies against specific threats and attack techniques and improve detection and response to security issues. ATT&CK can be broadly categorized into Techniques, Tactics, and Defenses, with "Techniques" and "Tactics" being more related to attacks, and "Defenses" being more related to defense. Tactics represent the attacker's larger strategic goals to achieve their end goal, while Techniques describe the attack techniques as the specific actions within each Tactic. Finally, Finally, "Mitigation," a subset of "Defense," describes defenses and mitigations against specific attack techniques or tactics, providing specific actions or enhancements to detect or prevent attacks. These ATT&CKs are used by security professionals and solution developers to better understand specific attacks and develop defense strategies.

D3FEND [9] is a knowledge graph of cybersecurity countermeasures researched by MITRE, and it does not score cybersecurity technologies by defining digital artefacts, but rather breaks them down by function to help users make more accurate judgements and build security architectures. The framework is constantly being updated, and while the initial release had 5 Tactics, it now has a total of 6 Tactics and 22 sub-techniques, including Models, with further subdivisions below. The D3FEND framework can look up a relevant defense technology by its Technique ID in ATT&CK, and describes the techniques of that defense technology, as well as providing information about the associated digital artefacts. Figure 1 shows the connection between these ATT&CK and D3FEND.

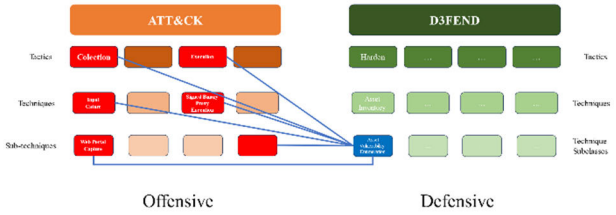


FIGURE 1. Example mapping relationship between ATT&CK and D3FEND.

B. EVALUATE CYBERSECURITY SCORES

Ahmed et al. [10] describe an empirical analysis of a cybersecurity scoring system. Security scores, which are quantitative indicators of an organization's security, generally a higher score indicates that an organization is more secure. However, these scores can vary depending on the organization providing the metric. Additionally, security scores typically use only externally accessible data and are comprised of three sources: external data, publicly available data, and proprietary algorithms. While a high security score indicates that an organization is well secured, even a high-scoring organization may be subject to more attacks than a low-scoring organization if the data it is handling is of a high level of importance compared to other organizations [11]. Therefore, while a security score can be a good indicator of security excellence and a low breach success rate, it is an assessment of an organization's overall security and may be low or too high for the level of criticality of the data [12]. As a result, to ensure fair and accurate assessments, the U.S. Chamber of Commerce has adopted six principles to guide its security ratings. These principles are shown in Figure 2. As a security rating company, BitSight uses data that feeds into a proprietary algorithm based on the six principles to generate a security score ranging from 250 to 900. The metrics consist of a compromised system score comprising five risk vectors, a diligence score focusing on management, such as security

updates to software, and a user behavior score measured by user activity.

Through this analysis, Ahmed et al. [10] point out that no two companies' networks are the same when it comes to measuring security scores, and that the number of users in a network should be considered when measuring scores. They also note that different companies face different types of threats depending on what they need to secure, so security incentives should be based on the criticality of the asset. Finally, it's important to ensure that the network infrastructure is trustworthy.

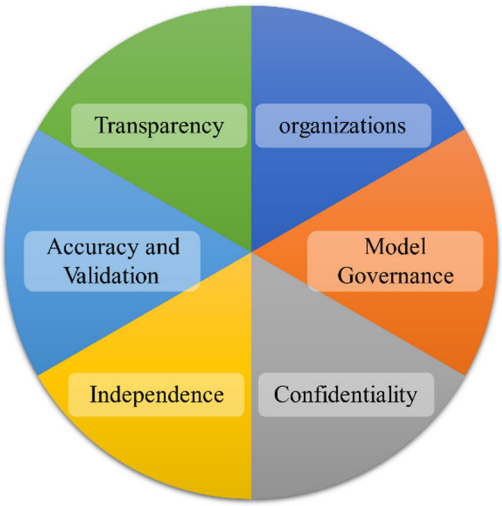


FIGURE 2. Six security rating principles adopted by the U.S. chamber of commerce.

In order to determine and benchmark the cybersecurity risk of an organization, Yampolskiy et al. [13] collected non-intrusive data related to the organization, processed the security information extracted from the collected data and calculated a security score. The calculated security score is assigned based on the correlation between the extracted security information and the overall cybersecurity risk determined by analyzing previously breached companies in the same industry. A patent has been filed to calculate an entity's overall cybersecurity risk score based on the calculated security score and as-signed weights.

C. CYBERSECURITY POLICY-RELATED PROPERTIES

Mishra et al. [14] identified 14 common cybersecurity attributes across seven countries (USA, EU, Australia, Canada, China, India, Malaysia): telecommunications, networks, cloud computing, e-commerce, online banking, smart grid, consumer rights, cybercrime, cryptography, privacy, identity theft, digital signatures, data security, and spam. While these attributes are self-contained, the interdependencies between them can be further specified for specific contexts. To combat cybercrime, the key characteristics of CS need to be identified and well-defined so that a comprehensive policy can be developed. While various stakeholders contribute to the development of CS policy, governments are the primary actors in the creation and revision of policy. Identifying common policies across countries can help academics and policymakers develop cybersecurity policies.

D. CYBERATTACK TARGETS

Cyberattacks are conducted in seven stages: reconnaissance, weaponization, dissemination, exploitation, installation, command and control, and goal achievement [15]. In addition, creating an attack graph for a target network is effective in identifying the attack path from the attack launch point to the target [16]. Identifying vulnerabilities in a network is important to prepare for cyber threats because attackers use vulnerabilities in the target network to identify the optimal attack path.

Common Platform Enumeration (CPE) is a structured naming scheme for software and packages. It consists of 11 attributes, including part, vendor, product, version, update, edition, language, and sw_edition of the software installed on the workstation, expressed as "cpe:2.3:a:microsoft:office:2013:-:-:*:-:-:x64:*". The product, version, update, target_hw, etc. of the CPE name can be used to match the corresponding vulnerability, and multiple CVEs can be matched for a single CPE [17].

Common Vulnerabilities and Exposures (CVEs) are a list of publicly known computer security flaws maintained and overseen by MITRE with financial support from the Cybersecurity and Infrastructure Security Agency (CISA). CVE IDs, the identifiers for CVEs, are assigned by the CVE Numbering Agency (CNA), which includes companies representing major IT vendors. When a security flaw is discovered, it is forwarded to the CNA, which assigns a CVE ID to the information, writes a brief description with references, and distributes it. CVE IDs are issued in the form of a CVE-Year-Serial number [18].

CVSS is an open framework that helps assess security threats by quantifying the nature and severity of software vulnerabilities. It is maintained by FIRST, an international association of incident response and security teams, and currently exists in v3.1 and v4.0 preview. CVSS has three main metrics: foundation, time, and environment, and each metric is composed of subcomponents [18]. The National Vulnerability Database (NVD) allows you to look up the CVSS score by CVE ID and provides a calculator so you can calculate it yourself. It is used by many organizations and vulnerability management programs because it can be used as an indicator of the severity of a vulnerability.

The Common Weakness Enumeration (CWE) is a list of common software and hardware vulnerability types that affect security. A vulnerability is a condition in software, firmware, hardware, and service components that can lead to vulnerability under certain circumstances. The CWE describes and discusses software and hardware weaknesses in a common language and identifies weaknesses in existing software and hardware products. It assesses the coverage of tools targeting these weaknesses and utilizes a common baseline standard for weakness identification, mitigation,

and prevention efforts [19]. These CWEs are related to MITRE's Common Attack Pattern Enumeration and Classification (CAPEC), which focuses on application security and describes common attributes and techniques used by attackers to exploit known weaknesses in cyber-enabled capabilities [20]. In addition, because CAPEC includes the technology numbering of ATT&CK, information about ATT&CK technologies can be obtained through CAPEC and vice versa.

E. CYBER SECURITY STRATEGIES

Varma [21] proposed a methodology to improve cyber resilience by integrating cyber threat detection and mitigation strategies using artificial intelligence (AI). The proposed methodology analyzes various AI-based models and algorithms to evaluate the accuracy and efficiency of cyber threat detection. It analyzes network traffic data using machine learning and deep learning techniques to detect anomalous patterns, and proposes a system that utilizes AI to detect threats in real-time and automatically execute response strategies. Measure detection rate, false positive rate, and response time as performance metrics for threat detection systems. The AI-integrated system is designed to adapt to dynamic cyber threats, and the study demonstrates that AI-based systems are effective in quickly responding to new attack vectors and enhancing an organization's security posture. The proposed system was experimentally validated using various cyber-attack scenarios, and the results showed high detection rates and low false positives compared to traditional security systems. This means that adapting to dynamic cyber threats and choosing a rapid response strategy is crucial to enhance cybersecurity.

Riggs et al. [22] categorize different types of cyber-attacks, including denial of service (DoS), ransomware, man-in-the-middle (MITM) attacks, phishing, and false data injection attacks (FDIA). The researchers also study the specific vulnerabilities associated with these attacks and the mitigation strategies to counter them. For example, DoS attacks can be mitigated through network traffic monitoring and intrusion detection systems (IDS). We proposed a defense-in-depth strategy that incorporates multiple layers of security measures to protect critical infrastructure. This approach involves using intrusion detection systems, encryption, and regular security audits to ensure the resilience of critical systems against cyber threats. They also emphasized the importance of adhering to cybersecurity standards provided by ISO and NIST, which provide frameworks and best practices for developing secure information systems. The authors noted that the rapid increase in cyberattacks on critical infrastructure requires a proactive and adaptive approach to cybersecurity, and by continually updating security measures and leveraging advanced technologies, organizations can better protect their critical assets from evolving cyberthreats.

III. METRICS DESIGN FOR DEFENSIVE SECURITY COUNTERMEASURES

This chapter suggests one metric to quantitatively assess the effectiveness of each defense measure and six metrics to calculate the score.

A. COUNTERMEASURE RECOMMENDATION METHOD PROCESS

An attack vector is created to progress an attack from the network to the cyber attacker's target asset. The assets along the attack path will have multiple vulnerabilities, and there will be multiple defenses that can be applied to the assets. It is possible to select only the vulnerabilities exploited by the attacker and select them as security measures. However, the defensive technologies included in the security countermeasures may not be the optimal security measures for each asset due to cost limitations, lack of equipment, or inability to respond quickly. It is very difficult to select cybersecurity measures while considering these various issues. Therefore, this study proposes a cybersecurity countermeasure recommendation including a three-step algorithm. The algorithm classifies only the defense technologies applicable to the network among the defense technologies identified through the vulnerabilities present in the assets, and finally recommends them through prioritization by measuring the quantitative evaluation score. As preliminary work for the algorithm, we describe the CPE-CVE-CWE-CAPEC-D3FEND mapping methodology.

1) IDENTIFYING CVES VIA CPES

Various vulnerabilities present in an asset can be identified by analyzing the network inside the organization or by knowing the program information used (vendor name, version, product name, etc.), i.e., CPE.

2) CWE MAPPING

For identified CVEs, CWEs are extracted from the 'Observed Examples' column of the CWE dataset or through the CWE-CVE root cause mapping methodology (available on the official page).

3) CWE AND ATT&CK UTILIZING CAPEC

CAPEC has CWE information in the 'Related Weakness' column and ATT&CK attack technique values as 'Entry ID' in the 'Taxonomy Mappings' column.

4) ATT&CK TO D3FEND

D3FEND officially supports mapping with ATT&CK.

By utilizing these mappings, you can effectively find defenses against CVEs identified through network analysis or CPE. The overall structure is shown in Figure 3, and the three-step algorithm is as follows.

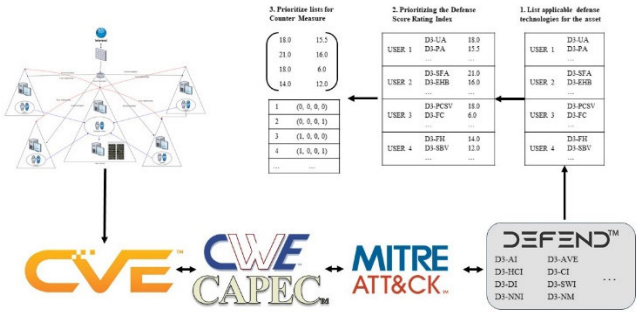


FIGURE 3. Countermeasure recommendation method process.

a: LISTING APPLICABLE DEFENSE TECHNIQUES FOR THE ASSET

Extract a list of applicable D3FEND defense techniques based on the defense techniques based on the vulnerabilities of each asset and the attacker's chosen attack technique (ATT&CK's technique) through the mapping methodology of the previous work.

b: PRIORITIZING THE DEFENSE SCORE RATING INDEX

Sort and prioritize the defense technology rating index calculated for each asset in descending order. The Defense Score Rating Index is described in III-C.

c: PRIORITIZING LISTS FOR CYBERSECURITY COUNTERMEASURES

Provide a prioritized list of defense technologies to recommend various cybersecurity countermeasures to security personnel and administrators. To achieve this, the two levels of asset-specific defense measure lists are determined into a single two-dimensional matrix, which can be prioritized by permutation [23] to provide different combinations of defense countermeasures.

The above procedure allows security personnel to select the appropriate cybersecurity measures for their network environment.

B. DESIGN AND DEFINE METRICS

Two of the six metrics are designed to be related to vulnerabilities. This is a result of accepting the importance of the security update score among the scores mentioned by Ahmed et al. [10]. The rest consisted of factors related to the network environment and position against attack techniques. The six designed metrics are as follows.

1) COST

The cost of applying defenses to your network. This includes both human and physical assets expended to apply the defense behavior. The higher the cost, the better the performance of the mitigation technique, but it is not directly proportional, so it is a good metric for selecting defenses that perform well at a lower cost. The lower the cost, the higher the score.

2) DEFENSE PHASE

Based on the four phases of breach incident response (IR) proposed by the US NIST [24] and the incident response phase consisting of a six-step process proposed by Kral in [25], it is composed of four phases: detection, initial response, recovery response, and investigation and analysis.

3) LEVEL OF DIFFICULTY

The concept of the difficulty of applying defense techniques, which is calculated based on the vulnerability of the asset in the network environment. Vulnerability is calculated based on CVSS and can be measured based on CVSS prediction algorithms [26] for new CVEs due to the constantly evolving cyberspace.

4) ASSET POSITION IN ATTACK PATH

This score is measured by determining the location of network assets targeted by detected threats along the attack path, from the attack launch point to the end goal. If you can proactively stop the threat at an asset close to the origin of the attack, you will score high.

5) EFFECT SCORE

A measure of the effectiveness of a defense technology when applied to a network environment. It is measured by the likelihood that a vulnerability in the network will be eliminated by applying the defense. The effectiveness metric, like the difficulty metric, is based on the CVSS prediction algorithm, which can respond to new vulnerabilities.

6) APPLICABILITY TIME

Ensuring that you can quickly apply defenses and stop threats from the point of attack detection is critical to improving cybersecurity, hence the metric that measures the time it takes to apply defense technique.

7) SINGLE DEFENSE SCORE

The above six metrics are equally weighted, and the higher the score of the remaining metrics relative to the cost metric, the higher the defense evaluation index.

C. CALCULATION METHOD

The six metrics are calculated as follows, and after all calculations, they must be normalized to the same range of values to produce the Defense Assessment Index.

1) COST

It is measured by the network assets, human assets of the network to which the defense technology is applied and is measured by the judgement of the managers and experts of the organization, or by the amount of hiring security experts. However, if the defensive technology is related to security equipment, the cost is calculated by including the cost of such equipment if the organization does not own such equipment, and the human cost is calculated.

When measuring costs, you should consider the following First, the amount of money available depends on the purpose of use (defense, private enterprise, etc.), network environment, security equipment you have, etc. The second is. it is not fixed due to many variables: labor costs, fluctuating market prices of resources, etc. For this reason, it can be measured differently depending on when it is measured and who is measuring it.

The calculated cost is normalized using the min-max normalization algorithm by finding the maximum and minimum cost of all defense technologies. (0 <= Cost <= 1).

2) DEFENSE PHASE

As mentioned in Section III-B, there are four phases and identify the defense phases that can be applied to each defense technique. A defense technique can have multiple defense phases, but for the purposes of this study, it is assumed to have a maximum of two defense phases. Each defense phase is scored from 1 to 5, with detection (4), initial response (5), recovery response (3), and investigation and analysis (1). (1 <= Phase <= 5).

Detection is a defense focused on identifying and alerting to cyber threats and can include network traffic analysis, log monitoring, and anomaly detection. Initial Response is the immediate action taken immediately after a threat is detected. This could be adjusting firewall rules, tightening access controls, or quarantining malicious code. Recovery Response involves steps to repair the damage, such as restoring data backups, reconfiguring systems, and patching vulnerabilities. Investigation and Analysis: Steps to determine the cause of the attack and prevent the same type of attack in the future. Examples include forensic analysis, log analysis, and threat intelligence research.

3) LEVEL OF DIFFICULTY (LVL)

The more vulnerabilities an asset has, the more difficult it is to apply defensive techniques. It is calculated as the sum of the vulnerability scores corresponding to the asset ($AssetCVSS_n$) over the sum of the scores of all vulnerabilities in the attack path ($\sum AssetCVSS$) as shown in Eq. 1. (0 <= Lvl <= 10)

$$Lvl = AssetCVSS_n / \sum AssetCVSS \tag{1}$$

4) ASSET POSITION IN ATTACK PATH (POSITION)

It is measured based on the position of the asset on the cyber attacker's attack path and is calculated as the position of the selected asset relative to the total number of assets on the path. (0 <= Position <= 1).

5) EFFECT SCORE

Based on the vulnerabilities of the asset, it is calculated as the CVSS average of the vulnerabilities after eliminating the vulnerabilities corresponding to the defense technology among the vulnerabilities existing in the asset through the relationship of CPE-CVE-CWE-CAPEC-ATT&CK-D3FEND as shown in Eq 2. (0 <= Effect <= 10).

6) APPLICABLE TIME (TIME)

Calculates the effectiveness of a mitigation technique over the time it takes to apply and complete. If the defensive action can be applied immediately, the effect is good, and the closer the calculated value is to 1, the greater the effect. It is calculated from the time of application, completion, and detection of the at-tack, and the variables as shown in Table 1 are defined based on Minute and calculated as shown in Eq 2. (0 <= Time <= 1)

$$Time = 1 - (TimeDA - TimeAD)/(TimeDC - TimeAD) \tag{2}$$

TABLE 1. The time matric calculations method's parameter and definitions.

Parameter	Definition
$Time_{DA}$	When to apply mitigation techniques
$Time_{DC}$	When defense techniques are applied
$Time_{AD}$	When the attack was detected

7) NORMALIZATION

The above metrics cannot be calculated with the same weight be-cause they all have different ranges of values, so they are normalized to make all the metrics equal, with values between 1-5.

Figure 4 shows how to replace values between 0-1 with values in the range 1-5. Values between 0 and 10 are replaced with values in the range 1-5 by multiplying the value below (the raw value before normalization) by 10.

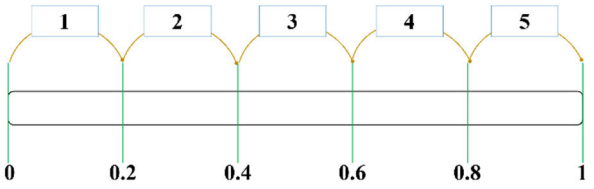


FIGURE 4. Normalization methods.

8) SINGLE DEFENSE SCORE (DS)

The higher the sum of the other metrics relative to the cost, the higher the score. The calculation method is shown in Eq 3.

$$DS = (Step + Lvl + Position + Effect + Time)/Cost \tag{3}$$

The above formula for calculating the defense evaluation index can be further refined by adding weights to the indicators based on the judgement of managers and experts.

Figure 5 is an example of network information and attack scenarios for selecting cybersecurity measures. Figure 6 is an example of a prototype showing the cybersecurity countermeasure priorities calculated based on Figure 5 and the defense techniques included in the countermeasure.

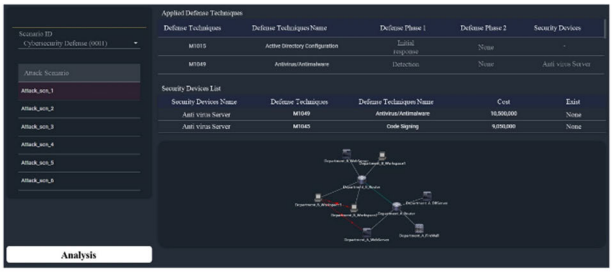


FIGURE 5. Examples of network information and attack vectors.

FIGURE 6. Cybersecurity countermeasures list and examples of defensive technologies included in the cybersecurity countermeasures.

IV. EXPERIMENTS

Due to the unreliability of the prototype, we conducted a logical experiment to verify the proposed method. For this purpose, we constructed a network for experiments. After performing scenarios with cyber-attack vectors on the configured network, we applied the proposed method to verify the results.

A. DESIGNING A NETWORK CONFIGURATION

Design a network for the experiment. The target networks of this study are military networks and corporate networks. Because using a real network environment may leak the organization's vulnerabilities and network information, we constructed a virtual network in this paper. However, in real-world implementations, vulnerability information and attack paths should be measured by security personnel, while other metrics can be helped by external organizations.

Fencl et al. [27] describe an algorithm for network topology design, noting that randomizing the network design can lead to problems with data transmission time delays and topology configuration costs. In addition, the design of network topology is important because if the network is poorly designed, it cannot be guaranteed to be safe from various cyber threats. In addition, conducting experiments to conduct various analyses in a virtual network environment similar to the real network environment is an important step to evaluate the advantages and ultimately deploy the solution before actually using it [28]. Therefore, in this study, we built a virtual network environment rather than a real network environment to conduct our experiments. Although the virtual network environment we designed is based on a private network, the methodology in this study can be applied to different types of networks, including closed networks with limited access and enhanced security measures, corporate networks, and public networks. This adaptability means that the proposed defense metrics can effectively protect against cyber threats regardless of the architecture or accessibility of the network. Conducting experiments in virtual network environments not only mitigates the potential risks associated with real-world testing, but also demonstrates the versatility of the approach to accommodate the unique requirements and challenges presented by different network environments.

The main experiments were conducted in a military network-based virtual environment, a small organization network; however, the military network-based environment is not disclosed in this paper. Therefore, we use a small office/home office network environment designed based on [29], [30], and [31]. Table 2 summarizes the elements required in the designed network, and the designed network is shown in Figure 7.

TABLE 2. Using network topology components.

Component	Example	Required scope
Network devices	Workstation, Printer, Laptop, Switch, etc.	Workstation, Printer, Switch, Server, Router, DB Server
Security devices	Fire Wall, IDC, IPS, etc.	All
Communication information	Packet, Delay time, Connection information, etc.	Connection information
System information	IP, Software information, Data file, User information, etc.	CVE

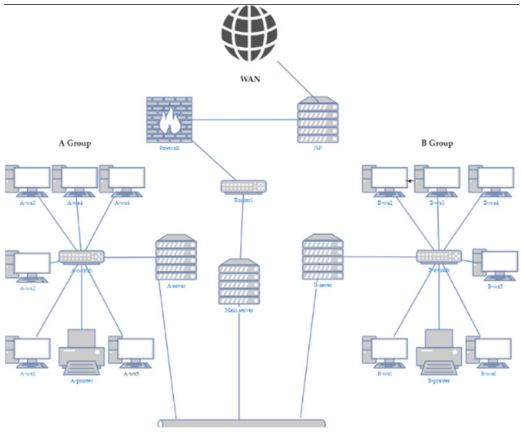


FIGURE 7. Designed network topology.

B. DESIGN ATTACK SCENARIOS

In order to compare the before and after of the proposed method, a cyber-attack must occur. By creating and performing a cyber-attack scenario, it is possible to identify the vulnerability of the network, and by performing the cyber-attack scenario again after applying the proposed

method, it is possible to identify the enhancement of cybersecurity. In addition, in order to demonstrate that the proposed method is a universal method and can be used in various environments, the attack scenarios are subject to the following assumptions and restrictions.

1) Based on ATT&CK's attack techniques, an attacker can use any attack technique that corresponds to the vulnerabilities present in the network. Utilize available attack techniques based on the CVE to D3FEND mapping method mentioned in III-A.
2) Cyber-attack attempts have a 100% success rate and can only be defended by D3FEND's defense technology. This is to evaluate the pure effectiveness of the defense technology by ensuring that it is not affected by rulesets such as security equipment or physical security.
3) To reach the final target network asset, the attack must traverse at least three assets, which means the minimum attack path is three hops, and is designed to allow the attack to progress through a variety of paths.
4) Based on the network topology designed in Section IV-A, the attacker goes through B-ws2, B-ws3, and A-ws5 to reach the final attack target (A-ws4). Figure 8 shows the CPE of the designed network Workstation and some of the CVEs corresponding to the CPE. Furthermore, the defense techniques applied are shown in Table 3 and the attack path is shown in Figure 9. The yellow line shows the direct access path from the network, and the red arrow line shows the flow of the attack path.

List of CPEs on a workstation

workstation name	CPE	vendor	product	version	target HW
A-ws1	cpe:2.3:a:microsoft:outlook:2013:-:-:*:-:-:x64:*	Microsoft	Outlook	2013	x64
A-ws1	cpe:2.3:a:microsoft:office:2013:-:-:*:-:-:x64:*	Microsoft	Office	2013	x64
A-ws2	cpe:2.3:a:microsoft:outlook:2013:-:-:*:-:-:x64:*	Microsoft	Outlook	2013	x64
A-ws2	cpe:2.3:a:microsoft:office:2013:-:-:*:-:-:x64:*	Microsoft	Office	2013	x64
A-ws3	cpe:2.3:a:microsoft:outlook:2013:-:-:*:-:-:x64:*	Microsoft	Outlook	2013	x64
A-ws3	cpe:2.3:a:microsoft:office:2013:-:-:*:-:-:x86:*	Microsoft	Office	2013	x86
A-ws4	cpe:2.3:a:microsoft:outlook:2013:-:-:*:-:-:x86:*	Microsoft	Outlook	2013	x86

List of CVEs mapped to CPEs

CPE	CVE
cpe:2.3:a:microsoft:outlook:2013:-:-:*:-:-:x64:*	CVE-2023-35311, CVE-2017-17689, CVE-2018-0850, CVE-2013-3905, CVE-2007-4040, CVE-2006-6659, CVE-2000-0216, CVE-2000-0160
cpe:2.3:a:microsoft:outlook:2013:-:-:*:-:-:x86:*	CVE-2023-35311, CVE-2017-17689, CVE-2018-0850, CVE-2013-3905, CVE-2007-4040, CVE-2006-6659, CVE-2000-0216, CVE-2000-0160
cpe:2.3:a:microsoft:outlook:2016:*:*:*:*:*:x64:*	CVE-2023-36763, CVE-2023-36893, CVE-2022-35742, CVE-2021-31949, CVE-2021-28452, CVE-2020-17119, CVE-2019-1084, CVE-2019-1200
cpe:2.3:a:microsoft:outlook:2016:*:*:*:*:*:x86:*	CVE-2023-36763, CVE-2023-35311, CVE-2023-33131, CVE-2021-31949, CVE-2020-16949, CVE-2020-16947, CVE-2020-1483, CVE-2019-1200, CVE-2019-1084
cpe:2.3:a:microsoft:office:2013:-:-:*:-:-:x64:*	CVE-2014-1808, CVE-2014-1756, CVE-2014-2730, CVE-2013-5054, CVE-2013-1324, CVE-2013-3889, CVE-2007-3282, CVE-2007-3109, CVE-2006-4694, CVE-2004-0848
cpe:2.3:a:microsoft:office:2013:-:-:*:-:-:x86:*	CVE-2014-6362, CVE-2014-6364, CVE-2014-1809, CVE-2014-1756, CVE-2013-1324, CVE-2013-3889, CVE-2007-3282, CVE-2006-1311, CVE-2005-2127
cpe:2.3:a:microsoft:office:2016:*:*:*:*:*:x64:*	CVE-2023-36413, CVE-2023-41764, CVE-2023-36896, CVE-2022-38048, CVE-2022-34717, CVE-2022-22003, CVE-2022-21841

FIGURE 8. The CPE of a designed network workstation (left) and some of the CVEs corresponding to the CPE (right).

These assumptions and limitations allow us to evaluate different cyber-attack scenarios and demonstrate the validity of the proposed methodology. By using different attack types, we can quantitatively evaluate and compare the effectiveness of defense techniques in a network environment.

C. APPLYING THE METHOD

Three of the six indicators in the proposed methodology include the presence of defense equipment and the amount of money spent on defense technologies. Therefore, in order to calculate a single defense score, a preparatory step is required to pre-calculate the three indicators. The preparation phase has the following prerequisites and assumptions.

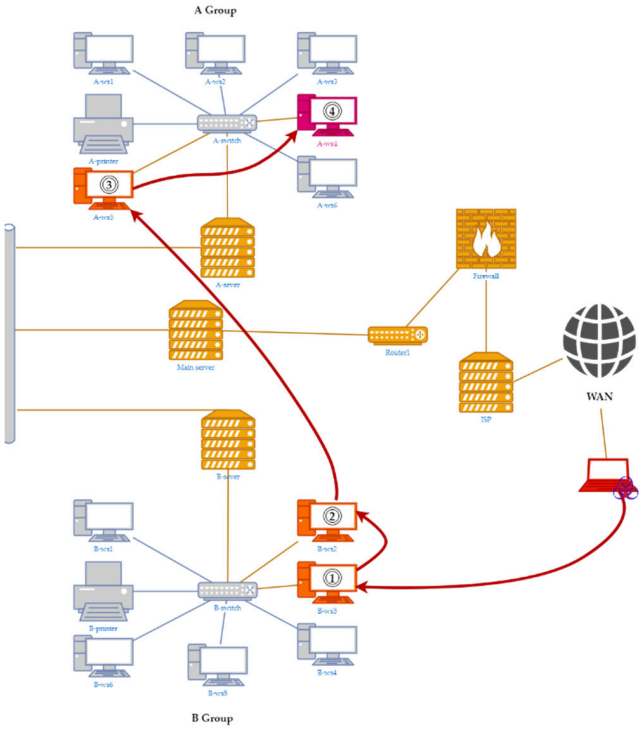


FIGURE 9. Designed attack scenario and route.

TABLE 3. List of defense techniques applied across the network.

Defense Techniques	Description	Device
D3-DNSDL	DNS Access Exclusion Policy	Firewall
D3-NTF	Network traffic filtering	Firewall
D3-BA	Authentication before bootloader programs	Workstations
D3-DE	Disk encryption	Workstations

1) COST

This is fluid as it includes the amount of human resources and equipment, so for the sake of fairness, all costs are calculated at the same amount. However, if defensive equipment is required, the cost of purchasing defensive equipment is taken into account. However, as mentioned in Section III-C, this would result in 0 and 1 for MIN-MAX normalization and 0 and 5 for the defense evaluation index, so we assumed a score of 5 for defense technologies that do not require security equipment and a score of 3 for defense technologies that require security equipment.

2) DEFENSE PHASE

You must set a Defense Phase for each Defense Technique. Set a minimum of one and a maximum of two defense skills.

TABLE 4. Summary of study comparisons.

Proposed Method	Important METRIC	Scope of use	Attack Type Coverage
J. Ahmed et al. [10]	Asset Criticality, Network Reliability, Number of network users	Organization	Botnet Infection, Spam, Malware Server, Unsolicited Communication
Stacy Collett [11]	Data Criticality	Organization	Not specified
Yampolskiy et al. [13]	About Data Security, Weight	Organization	Social Engineering Attacks, Malware, Botnet ifections, Hacker Sites
A. Mishra et al. [14]	Key Common Characteristics of Cybersecurity	Government	DoS, Cybercrime during COVID-19, Cross-border Cyber threats, Attacks on critical infrastructure
V. V. Varma. [21]	Connectivity, Communication Protocols	Organization	DDoS, IP Spoofing
H. Riggs, et al. [22]	Vulnerability Analysis, Anomaly Detection	Organization, Government	Ransomware, APTs
Proposed Method	Future-proofing Technologies, Flexible, Network Environment	Private, Organization, Government	DDoS, IP Spoofing, Brute Force

This is determined based on the description of the defense technology.

D3FEND ID	D3FEND Tactic	D3FEND Technique	D3FEND Technique Level 0 Name	Description
D3-DENCR	Harden	Platform Hardening	Disk Encryption	Disk Encryption
D3-BA	Harden	Platform Hardening	Bootloader Authentication	Authentication Before Bootloader Programs
D3-ANAA	Detect	Network Traffic Analysis	Administrative Network Activity Analysis	Analyze administrator network activity
D3-CA	Detect	Network Traffic Analysis	Certificate Analysis	Analyze network certificate health
D3-CSPP	Detect	Network Traffic Analysis	Client-server Payload Profiling	Analyze request and response packets to identify normal ranges and derive anomalies
D3-DNSTA	Detect	Network Traffic Analysis	DNS Traffic Analysis	Analyze DNS traffic to identify malicious behavior
D3-FC	Detect	Network Traffic Analysis	File Carving	Extract files from network traffic
D3-IPCTA	Detect	Network Traffic Analysis	IPC Traffic Analysis	Analyze IPC traffic (Ex: SMB)
D3-NTCD	Detect	Network Traffic Analysis	Network Traffic Community Deviation	Check frequently communicated sites and then check when accessing anomalous sites
D3-PHDURA	Detect	Network Traffic Analysis	Per Host Download-Upload Ratio Analysis	Analyze download/upload bandwidth range by host
D3-PMAD	Detect	Network Traffic Analysis	Protocol Metadata Anomaly Detection	Check network protocols for abnormalities (Ex: headers, request/response times)
D3-RTSD	Detect	Network Traffic Analysis	Remote Terminal Session Detection	Analyze remote terminal session access
D3-RTA	Detect	Network Traffic Analysis	RPC Traffic Analysis	Analyze remote procedure calls
D3-CAA	Detect	Network Traffic Analysis	Connection Attempt Analysis	Analyze the number of connection attempts
D3-ISVA	Detect	Network Traffic Analysis	Inbound Session Volume Analysis	Analyze access request session volume
D3-BSE	Detect	Network Traffic Analysis	Byte Sequence Emulation	Analyze shell code in network packets
D3-RPA	Detect	Network Traffic Analysis	Relay Pattern Analysis	Check for anomalies in external connections using proxies, forwarding, routing, etc.
D3-UDTA	Detect	User Behavior Analysis	User Data Transfer Analysis	Analyze user transferred data volumes
D3-DNSAL	Isolate	Network Isolation	DNS Allowlisting	DNS allow policy
D3-DNSDL	Isolate	Network Isolation	DNS Denylisting	DNS access exclusion policies
D3-EAL	Isolate	Execution Isolation	Executable Allowlisting	Executable allowlist
D3-PT	Evict	Process Eviction	Process Termination	Process termination

D3FEND ID	Cost	Defense Phase1	Defense Phase2	Applicable time	Applied Seq	Complate Seq
D3-DENCR	$100,000	2(Initial response)	-	0.65	$TIME_{AD}+4$	$TIME_{DA}+3$
D3-BA	$100,000	2(Initial response)	1(Detection)	0.75	$TIME_{AD}+3$	$TIME_{DA}+2$
D3-ANAA	$100,000	3(Investigative Analysis)	-	0.6	$TIME_{AD}+4$	$TIME_{DA}+4$
D3-CA	$100,000	3(Investigative Analysis)	-	0.65	$TIME_{AD}+3$	$TIME_{DA}+4$
D3-CSPP	$100,000	3(Investigative Analysis)	-	0.65	$TIME_{AD}+2$	$TIME_{DA}+5$
D3-DNSTA	$100,000	3(Investigative Analysis)	-	0.65	$TIME_{AD}+2$	$TIME_{DA}+5$
D3-FC	$100,000	3(Investigative Analysis)	-	0.65	$TIME_{AD}+3$	$TIME_{DA}+4$
D3-IPCTA	$100,000	3(Investigative Analysis)	-	0.65	$TIME_{AD}+2$	$TIME_{DA}+5$
D3-NTCD	$100,000	3(Investigative Analysis)	-	0.8	$TIME_{AD}+2$	$TIME_{DA}+2$
D3-PHDURA	$100,000	3(Investigative Analysis)	-	0.7	$TIME_{AD}+3$	$TIME_{DA}+3$
D3-PMAD	$100,000	3(Investigative Analysis)	-	0.65	$TIME_{AD}+3$	$TIME_{DA}+4$
D3-RTSD	$100,000	3(Investigative Analysis)	-	0.6	$TIME_{AD}+4$	$TIME_{DA}+4$
D3-RTA	$100,000	3(Investigative Analysis)	-	0.65	$TIME_{AD}+3$	$TIME_{DA}+4$
D3-CAA	$100,000	3(Investigative Analysis)	-	0.7	$TIME_{AD}+3$	$TIME_{DA}+3$
D3-ISVA	$100,000	3(Investigative Analysis)	-	0.75	$TIME_{AD}+2$	$TIME_{DA}+3$
D3-BSE	$100,000	3(Investigative Analysis)	-	0.55	$TIME_{AD}+5$	$TIME_{DA}+4$
D3-RPA	$100,000	3(Investigative Analysis)	-	0.65	$TIME_{AD}+3$	$TIME_{DA}+4$
D3-UDTA	$100,000	3(Investigative Analysis)	-	0.7	$TIME_{AD}+2$	$TIME_{DA}+4$
D3-DNSAL	$110,000	1(Detection)	4(Recovery)	0.85	$TIME_{AD}+2$	$TIME_{DA}+1$
D3-DNSDL	$110,000	1(Detection)	4(Recovery)	0.85	$TIME_{AD}+2$	$TIME_{DA}+1$
D3-EAL	$110,000	2(Initial response)	4(Recovery)	0.85	$TIME_{AD}+1$	$TIME_{DA}+2$
D3-PT	$110,000	4(Recovery)	-	0.95	$TIME_{AD}+0$	$TIME_{DA}+1$

FIGURE 10. Three metrics set in the preparation phase: cost, defense level, and time to apply.

3) APPLICABLE TIME

The time from the time of application of the defense technology to the completion of application depends on the ability of the security expert applying the defense technology and the possession of defense equipment. Therefore, this study assumes that all defense equipment is possessed and is calculated based on the Description. It is also assumed that the time from the time of attack detection to the application of the defense technology and the time from the start of application of the defense technology to the completion of application are performed by one security expert.

The Figure 10 shows some of the metric values for the Preparation phase based on the above prerequisites and assumptions.

After all the preparations, we identified the optimal security countermeasures for the attack vectors shown in Figure 9, and the prioritized defense countermeasures for each asset are shown in Figure 11. In B-ws3, A-ws5, and A-ws4, D3-FE, a defense technology related to file encryption, scored the highest, and D3-EDL, which blocks file execution through poli-cy changes, scored the second highest.

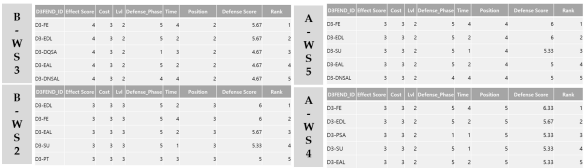


FIGURE 11. Table of defense technology prioritization results for assets.

Based on the workstation's list of defense technologies, the best security countermeasure produced by the permutation was the addition of D3-FE alone (Total 24.0), while the combination of permutations that removed duplicates from all four workstations yielded a score of 22.67: D3-FE (5.67), D3-EAL (5.67), D3-EDL (6.00), and D3-SU (5.33).

V. CONCLUSION

The purpose of this research is to provide effective and efficient security countermeasures for multiple assets with less effort in preparation for cyberattacks or in the event of damage caused by cyber-attacks. Furthermore, this research aims to prepare for the evolving cyber threats in the evolving cyberspace. To validate this, a virtual network environment was built, attack scenarios were written, and experiments were conducted. When cybersecurity countermeasures were selected through the process shown in Figure 4, it was found

that in the case of a small network with fewer paths, only one additional security technology was selected, but it was found to be the most efficient security technology in that network environment. By reversing the mapping relationship of ATT&CK-CAPEC-CWE-CVE-CPE with the defense technologies identified in the experimental results, we found that on average, more than 10 vulnerabilities can be compensated out of the average number of 16.75 vulnerabilities in the assets. We further experimented in a real-world network environment using 10 workspaces and found that they were able to cover an average of 5.4 out of 10 vulnerabilities, which was not significantly different from the results in the virtual environment.

Based on the experimental results, we compared the differences with previous studies. Ahmed et al. [10] emphasized the importance of measuring security scores based on the criticality of assets and network trust. While scores measured by security scoring companies are important, it is important to evaluate the criticality of the data because the criticality of the data determines the likelihood of being targeted by an attacker. Yampolskiy et al. [13] measured the security risk score by collecting data and extracting security information to determine the cybersecurity risk of a company, and Mishra et al. [14] stated that it is important to identify the main characteristics of common CS to develop cyber policies. Varma [21] emphasized the use of AI in cybersecurity to integrate threat detection and mitigation strategies. He designed an AI-integrated system to adapt to dynamic cyber threats and focuses on learning to quickly respond to new attack vectors and strengthen the organization's security posture. Riggs et al. [22] mention the need to incorporate multiple layers of security measures against various cyber threats. In conclusion, most cybersecurity strategy and response techniques studies emphasize collecting network security information, data information, etc. to measure cybersecurity scores in order to prepare for cyber threats. They also emphasize the use of AI techniques to perform automated response strategies to improve cybersecurity.These studies may not be universal and may not be prepared for new threats, and it may be difficult for administrators to justify the response strategies implemented by leveraging AI to perform response strategies or to modify response strategies based on the situation. However, in this study, we used ATT&CK, D3FEND, a knowledge graph-based framework of offensive and defensive techniques that is universal, continuously updated, and adaptable to new threats. We also designed, quantified, and prioritized six metrics for defensive techniques to allow for flexibility in modifying and selecting defensive strategies. This is one of the ways to select the right security measure for the network according to the evolving cybersecurity and attack technologies. In addition, we included CVEs and CVSS in the metrics, which are used globally to measure the security risk of network assets, so it can be used in various environments (individuals, organizations, countries, etc.). Table 4 summarizes a comparison of the results of these studies.

This research aims to help individuals, organizations, countries, etc. select efficient security measures with less effort in the modern world where cybersecurity is becoming increasingly important. To select efficient security measures, we proposed six metrics that can be set by users and automatically calculated according to different environments. We also indexed each column and generated permutations to prioritize them, and applied different defense techniques by removing redundancies, which means that the proposed cybersecurity mitigation procedures can be effectively applied in different network environments. The practical application of the method proposed in this study requires sufficient knowledge of the network environment, and providing this information to an external party may cause greater threats. Therefore, we mainly conducted experiments in a virtual network environment, and confirmed that it can be applied in an environment similar to a real network. For practical application, the administrator should be in charge, and the remaining indicators except vulnerability information and location information along the attack path can be helped by external personnel. In addition, efficiently utilizing frameworks that are continuously updated by leveraging CVSS prediction algorithms [26] or through APIs provided by frameworks (D3FEND, ATT&CK, CVE, etc.) can help adapt to evolving cyber threats. Therefore, the methodology proposed in this study has the following advantages. 1. by using a continuously updated framework and using a commonly used vulnerability management system, it is easy to manage the latest attack, defense, and vulnerability data. 2. By designing and quantitatively evaluating six metrics for defensive technologies, it is possible to understand why defensive technologies are recommended. Personnel can utilize them and use them as a basis for decision making. 3. The proposed methodology can be automated and used after the first network information collection. Finally, it is flexible, as the metrics are measured differently depending on the network information analyzed, and can be used in different network environments. However, this study has some limitations. First, all the frameworks used as mapping relationships may not be well matched due to their continuous updates. Furthermore, they will be unusable if they stop updating. Second, we need to collect system and network information about all the assets that make up the network in order to measure the designed metrics. Finally, while we tried to objectify the network used in our experiments, we conducted our experiments primarily in a virtual environment, which may lead to errors in generalization. In order to weight the designed metrics, it is essential to create various cyber-attack scenarios, collect data through extensive experiments, and then utilize machine learning models to identify and weight metrics that have a real impact on enhancing cybersecurity.

REFERENCES

[1] A. F. Brantly, "The cyber deterrence problem," in *Proc. 10th Int. Conf. Cyber Conflict (CyCon)*, Tallinn, Estonia, May 2018, pp. 31–54.

[2] A. Mishra, Y. I. Alzoubi, A. Q. Gill, and M. J. Anwar, "Cybersecurity enterprises policies: A comparative study," *Sensors*, vol. 22, no. 2, p. 538, Jan. 2022.

[3] T. Rajaretnam, "A review of data governance regulation, practices and cyber security strategies for businesses: An Australian perspective," *Int. J. Technol. Manage. Inf. Syst.*, vol. 2, no. 1, pp. 1–17, 2020.

[4] A. R. Ugale and A. D. Potgantwar, "Anomaly based intrusion detection through efficient machine learning model," *Int. J. Electr. Electron. Res.*, vol. 11, no. 2, pp. 616–622, Jun. 2023, doi: 10.37391/ijeer.110251.

[5] M. S. Akhtar and T. Feng, "Malware analysis and detection using machine learning algorithms," *Symmetry*, vol. 14, no. 11, p. 2304, Nov. 2022, doi: 10.3390/sym14112304.

[6] H. Jiwon, H. Kim, S. Oh, Y. Im, H. Jeong, and H. Kim, "Client-based web attacks detection using artificial intelligence," 2023. Accessed: Jul. 26, 2024, doi: 10.21203/rs.3.rs-2920883/v1. [Online]. Available: https://assets-eu.researchsquare.com/files/rs-2920883/v1_covered_9fd4d387-50c6-49d2-bde6-88f9b563c434.pdf?c=1711504235

[7] T. Z. Difaizi, O. P. L. Camille, T. C. Benhura, and G. Gupta, "URL based malicious activity detection using machine learning," in *Proc. Int. Conf. Disruptive Technol. (ICDT)*, Greater Noida, India, May 2023, pp. 414–418.

[8] B. E. Strom, A. Applebaum, D. P. Miller, K. C. Nickels, A. G. Pennington, and C. B. Thomas, "Mitre att&ck: Design and philosophy," MITRE Corp., Richmond, VA, USA, Tech. Rep. MP180360R1, 2018. Accessed: Jan. 4, 2024. [Online]. Available: https://www.mitre.org/sites/default/files/2021-11/prs-19-01075-28-mitre-attack-design-and-philosophy.pdf

[9] P. E. Kaloroumakis and M. J. Smith, "Toward a knowledge graph of cybersecurity countermeasures," M.S. thesis, MITRE Corp., 2021. Accessed: Jan. 4, 2024. [Online]. Available: https://d3fend.mitre.org/resources/D3FEND.pdf

[10] J. Ahmed. (2019). *Empirical Analysis of a Cybersecurity Scoring System*. Accessed: Jan. 4, 2024. [Online]. Available: https://digitalcommons.usf.edu/etd/7722

[11] S. Collett. (2016). *Whats in a Security Score?*. Accessed: Jan. 4, 2024. [Online]. Available: https://www.csoonline.com/article/557289/what-s-in-a-security-score.html

[12] J. Vijayan. (2014). *Target Attack Shows Danger of Remotely Accessible HVAC Systems*. Computerworld. Accessed: Jan. 4, 2024. [Online]. Available: https://www.computerworld.com/article/2487452/target-attack-shows-danger-of-remotely-accessible-hvac-systems.html

[13] A. Yampolskiy, R. Blackin, A. Heid, and S. Kassoumeh, "Calculating and benchmarking an entity's cybersecurity risk score," U.S. Patent 10 498 756, Nov. 22, 2016. [Online]. Available: https://patents.google.com/patent/US20160173521A1/en

[14] A. Mishra, Y. I. Alzoubi, M. J. Anwar, and A. Q. Gill, "Attributes impacting cybersecurity policy development: An evidence from seven nations," *Comput. Secur.*, vol. 120, Sep. 2022, Art. no. 102820, doi: 10.1016/j.cose.2022.102820.

[15] E. M. Hutchins, M. J. Cloppert, and R. M. Amin, "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains," in *Leading Issues in Information Warfare & Security Research*, vol. 1, Washington, DC, USA: API, 2011, pp. 113–125.

[16] I. Kotenko and A. Chechulin, "A cyber attack modeling and impact assessment framework," in *Proc. 5th Int. Conf. Cyber Conflict (CYCON)*, Tallinn, Estonia, Jun. 2013, pp. 1–24.

[17] B. A. Cheikes, D. Waltermire, and K. Scarfone, "Common platform enumeration: Naming specification version 2.3," U.S. Dept. Commerce, Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. 7695, 2011, doi: 10.6028/NIST.IR.7695. [Online]. Available: https://www.nist.gov/publications/common-platform-enumeration-naming-specification-version-23

[18] M. Adam et al. (2019). *Common Vulnerability Scoring System (CVSS) Version 3.1: Specification Document*. Accessed: Jan. 4, 2024. [Online]. Available: https://www.first.org/cvss/v3.1/specification-document

[19] S. Christey and C. Harris. (Oct. 2009). *Introduction to Vulnerability Theory*. MITRE. [Online]. Available: https://cwe.mitre.org/documents/vulnerability_theory/CWE-Introduction_to_Vulnerability_Theory.pdf

[20] N. Amon and J. Baker. (2021). *Security Control Mappings: A Starting Point for Threat-Informed Defense*. MITRE-Engenuity. Accessed: Jan. 4, 2024. [Online]. Available: https://medium.com/mitre-engenuity/security-control-mappings-a-starting-point-for-threat-informed-defense-a3aab55b1625

[21] V. V. Varma, "Enhancing cyber resilience by integrating AI-driven threat detection and mitigation strategies," *Trans. Latest Trends Artif. Intell.*, vol. 4, no. 4, 2023. Accessed: Jul. 7, 2024. [Online]. Available: https://ijsdcs.com/index.php/TLAI/article/view/396

[22] H. Riggs, S. Tufail, I. Parvez, M. Tariq, M. A. Khan, A. Amir, K. V. Vuda, and A. I. Sarwat, "Impact, vulnerabilities, and mitigation strategies for cyber-secure critical infrastructure," *Sensors*, vol. 23, no. 8, p. 4060, Apr. 2023. Accessed: 2024-06-07. [Online]. Available: https://www.mdpi.com/1424-8220/23/8/4060

[23] R. Arboretti, S. Bonnini, L. Corain, and L. Salmaso, "A permutation approach for ranking of multivariate populations," *J. Multivariate Anal.*, vol. 132, pp. 39–57, Nov. 2014, doi: 10.1016/j.jmva.2014.07.009.

[24] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, "Computer security incident handling guide," NIST, Special Publication 800.61, Tech. Rep. SP 800-61 Rev. 2, 2012, doi: 10.6028/NIST.SP.800-61r2.

[25] P. Kral. (2011). *The Incident Handlers Handbook*. Sans Institute. Accessed: Jan. 4, 2014. [Online]. Available: https://sansorg.egnyte.com/dl/6Btqoa63at

[26] M. R. Shahid and H. Debar, "CVSS-BERT: Explainable natural language processing to determine the severity of a computer security vulnerability from its description," in *Proc. 20th IEEE Int. Conf. Mach. Learn. Appl. (ICMLA)*, Pasadena, CA, USA, Dec. 2021, pp. 1600–1607, doi: 10.1109/ICMLA52953.2021.00256.

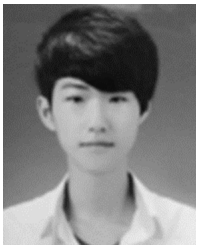
[27] Fencl et al., "Network topology design," *Control Eng. Pract.*, vol. 19, no. 11, pp. 1287–1296, 2011.

[28] A. Bavier, N. Feamster, M. Huang, L. Peterson, and J. Rexford, "In VINI veritas: Realistic and controlled network experimentation," in *Proc. Conf. Appl., Technol., Architectures, Protocols Comput. Commun.*, Italy, Aug. 2006, pp. 3–14, doi: 10.1145/1159913.1159916.

[29] L. Yang and Y. Ding, "The design of network topology big data platform in cloud computing," in *Proc. 2nd Int. Conf. Adv. Technol. Intell. Control, Environ., Comput. Commun. Eng. (ICATIECE)*, Bangalore, India, Dec. 2022, pp. 1–5, doi: 10.1109/ICATIECE56365.2022.10047353.

[30] J. L. Harrington, "Part two: Design and connectivity," in *Ethernet Networking for the Small Office and Professional Home Office*. Amsterdam, The Netherlands: Elsevier, 2010.

[31] W. Odom, *CCNA 200-301 Official Cert Guide*, vol. 2. Indianapolis, IN, USA: Cisco Press, 2019, Accessed: Jan. 4, 2024. [Online]. Available: https://www.cefracor.org/sites/www.cefracor.org/files/webform/documents/offre-complete/fichier/pdf-ccna-200-301-official-cert-guide-library-wendell-odom-pdf-download-free-book-eee99cc.pdf



JANG JISOO received the B.S. degree in computer science from Seoul Hoseo Occupational Training College, Seoul, South Korea, in 2021, and the M.S. degree in computer science from Sejong University, Seoul, in 2023, where he is currently pursuing the Ph.D. degree. From 2017 to 2019, he was an alternative to military service with a real estate company in South Korea, where he was responsible for website development and maintenance. His research interests include machine learning, cyberspace, cyber warfare, and military science.

SUBONG JUNG received the B.S. degree in electronic engineering from the Naval Academy, Gyeongsangnam-do, Republic of Korea, in 1993, and the M.S. degree in industrial engineering from Kyung Hee University, Suwon, Republic of Korea, in 2001. He is currently a Manager with the Defense Future Technology Research Institute, LIG Systems, Seoul, Republic of Korea. His research interests include cyber warfare, decision-making, and information protection.

MYUNGKIL AHN received the B.S. degree in information and communication engineering from Chungnam National University, Daejeon, Republic of Korea, in 1997, the M.S. degree in computer engineering from Sogang University, Seoul, Republic of Korea, in 2003, and the Ph.D. degree in electrical and electronics engineering from Chung-Ang University, Seoul, in 2021. She is currently a Principal Researcher with the Cyber Technology Center, Agency for Defense Development, Seoul. Her research interests include computer security and cyberwarfare modeling and simulation.

DONGHWA KIM received the B.S. and M.S. degrees from the School of Electrical Engineering, Korea University, Seoul, Republic of Korea, in 2004 and 2007, respectively. He is currently pursuing the Ph.D. degree in computer engineering with Sejong University. He is a Senior Researcher with the Cyber Technology Center, Agency for Defense Development, Seoul. His research interests include cybersecurity training systems, M&S systems, and cyber red/blue team automation.

JAEPIL YOUN received the B.S. degree in computational information processing from the Korea Army Academy at Yeongcheon (KAAY), Republic of Korea, in 2008, the M.S. degree in cybersecurity from Ajou University, Suwon, Republic of Korea, in 2017, and the Ph.D. degree in computer engineering from Sejong University, Seoul, Republic of Korea, in 2023. From 2018 to 2020, he was a Researcher with the Agency for Defense Development (ADD), Republic of Korea. From 2021 to 2023, he was an Officer for cyber operations planning and cyber operations training at the Army Cyber Operations Center (ACOC). He currently conducts research at the Joint Forces Military University (JFMU), where he studies advancements in defense policy, military strategy, defense planning, and joint coalition operations. His research interests include cyber intelligence surveillance and reconnaissance (ISR) and cybersecurity.

DONGKYOO SHIN received the B.S. degree in computer science from Seoul National University, South Korea, in 1986, the M.S. degree in computer science from Illinois Institute of Technology, Chicago, IL, USA, in 1992, and the Ph.D. degree in computer science from Texas A&M University, College Station, TX, USA, in 1997. He is currently a Professor with the Department of Computer Engineering, Sejong University, South Korea. From 1986 to 1991, he was with Korea Institute of Defense Analyses, where he developed database application software. From 1997 to 1998, he was a Principal Researcher with the Multimedia Research Institute, Hyundai Electronics Company, South Korea. His research interests include machine learning, ubiquitous computing, biosignal data processing, and information security.

IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 1 December 2023, accepted 19 December 2023, date of publication 1 January 2024,
date of current version 16 January 2024.

Digital Object Identifier 10.1109/ACCESS.2023.3349022

RESEARCH ARTICLE

A Systematic Analysis of Enhancing Cyber Security Using Deep Learning for Cyber Physical Systems

SHIVANI GABA[1], ISHAN BUDHIRAJA[1], (Member, IEEE), VIMAL KUMAR[1], (Member, IEEE), SHESHIKALA MARTHA[2], (Member, IEEE), JEBREEL KHURMI[3], AKANSHA SINGH[1], (Member, IEEE), KRISHNA KANT SINGH[4], S. S. ASKAR[5], AND MOHAMED ABOUHAWWASH[6,7]

[1]School of Computer Science Engineering and Technology, Bennett University, Greater Noida, Uttar Pradesh 201310, India
[2]School of Computer Science and Artificial Intelligence, SR University, Warangal, Telangana 506371, India
[3]Department of Computer Science, College of Technology, Jazan University, Jazan 45142, Saudi Arabia
[4]Delhi Technical Campus, Greater Noida 201306, India
[5]Department of Statistics and Operations Research, College of Science, King Saud University, Riyadh 11451, Saudi Arabia
[6]Department of Mathematics, Faculty of Science, Mansoura University, Mansoura 35516, Egypt
[7]Department of Computational Mathematics, Science and Engineering, College of Engineering, Michigan State University, East Lansing, MI 48825, USA

Corresponding author: Akansha Singh (akansha1.singh@bennett.edu.in)

This project is funded by King Saud University, Riyadh, Saudi Arabia. Researchers Supporting Project number (RSP2024R167).

ABSTRACT In this current era, cyber-physical systems (CPSs) have gained concentrated consideration in various fields because of their emergent applications. Though the robust dependence on communication networks creates cyber-physical systems susceptible to deliberated cyber related attacks and detecting these cyber-attacks are the most challenging task. There is the interaction among the components of the cyber and physical worlds, so CPS security needs a distinct approach from past security concerns. Deep learning (DL) distributes better performance than machine learning (ML) due to its layered architecture and the efficient algorithm for extracting prominent information from training data. So, the deep learning models are taken into consideration quickly for detecting cyber-attacks in cyber physical systems. As numerous attack detection methods have been proposed by various authors for enforcing CPS security, this paper reviews and analyzes multiple ways of attack detection presented for CPS using deep learning. We will be putting the excellent potential for detecting cyber-attacks for CPS concerning deep learning modules. The admirable performance is attained partly as highly quality datasets are eagerly obtainable for the use of the public. Moreover, various challenges and research inclinations are also discussed in impending research.

INDEX TERMS Cybersecurity, cyberattacks, cyber physical systems (CPSs), deep learning (DL), attack detection.

I. INTRODUCTION

As there is a fast growth of technology in various communication networks and the field of computer science leads, cyber-physical systems (CPS) are rising widely in both areas, such as academia and industries. The cyber-physical systems are measured and supervised by computer-based algorithms, which are combined with networks and users. The cyber-physical systems comprise interacting network units with physical and computational devices. The applications of CPS are making a disproportionate impact on businesses, such as in industrial sectors, healthcare, and manufacturing.

As soon as the Internet of Things (IoT) initiates, various devices with security susceptibilities are connected to cyber-physical systems, resulting in multiple attacks. It has been observed in past years that the incidents of CPS attacks have increased after the Stuxnet attack back in 2010 [1]. If cyber-physical systems attacks are not perceived and reduced rapidly, they can cause massive consequences such

The associate editor coordinating the review of this manuscript and approving it for publication was Engang Tian.

as damage to equipment, financial losses, and public safety. So the security of CPS is one of the vital paradigms for this. But securing cyber-physical systems is also a challenging task due to its heterogeneity of components, complex interactions among cyber-physical systems, and the attack surface's complexities [2]. It is observed that an intruder can randomly interrupt the dynamism of systems or encourage agitations to cyber-physical systems deprived of the security of various strategies of hardware or software, which leads to substantial social victims or the lives of humans [3], [4], [5], [6], [7], [8], [9]. If cyberattacks are perceived and positioned quickly, the loss to overall systems will be measured within the acceptable time limit. Much of the existing literature on the detection of attacks is dependent on centralized architectures [10], [11], [12], [13].The attack detection schemes are usually categorized into knowledge-based and data-driven approaches [14]. The residual generation method is one of the representative detection strategies in many knowledge-based systems [15], [16], [17]. Usually, residual is intended by comparison of measurements of sensors and systematic model of the system. Afterward, it is equated with the static or time-variant threshold for determining whether it is an attack or not. In the case of data-driven methods, deep learning approach and heuristic algorithms are used for building models of cyber-physical systems [18], [19]. If this does not follow these associations, then the attack is assumed. Apart from centralized systems, many kinds of distributed systems appear nowadays. The main challenge of designing a distributed attack detection method is monitoring cyber-physical systems without adequate information. Most cyber-physical systems lack various cyber security mechanisms, such as message authentication, which results in numerous challenges for detecting data injection attacks [20]. The absence of worldwide encryption, mainly on systems engaging in dated technologies, makes it exciting to secure in contradiction of eavesdropping attacks. So, it is required to refer replay attacks. According to the report on the global cyber-physical system market and data bridge market research, the historical market and forecast CAGR is 7.8%. The traffic in global cyber-physical systems is expected to account for USD 12,356.23 million by 2028. This increase in traffic increases the burden on the CPS systems as the market increases. To overcome this problem, the researchers of both academia and industry explored this market, and as a result, the various privacy preservation methods are explored.

A. PROBLEM FORMULATION

Although there are various advantages of cyber-physical systems, these systems are susceptible to numerous cyber or physical security threats, attacks, and challenges. This occurs due to its non-homogeneous nature and dependency on sensitive and private data. This kind of planned or accidental acquaintance with these systems leads to terrible effects, which results in complex security measures. Though this leads to the undesirable overhead of networks. So the security measures of a cyber-physical system are required to formulate. Figure 1 represents the review methodology of this paper. It represents the searching process and reviewing results. The authors have read the various papers for collecting the noticeable information and deliberate the cyber physical systems, fault and failures, cyber security standards, and various challenges.

B. WHY DEEP LEARNING FOR CYBER PHYSICAL SYSTEMS (CPS)

Deep Learning (DL) [21], [22], [23] gives better results as compared to machine learning (ML). In case of passable data, deep learning models provide the best results. Even deep learning models are applied for solving cyber-physical system cybersecurity issues compared to other fields. It is also experiential that various deep learning models are anticipated in current publications for detecting cyber-physical systems' cyber-attacks. The main is not only the way to describe the difficulty of cyber-attack detections on cyber-physical systems; the main complexity arises when superimposing cyber security over cyber-physical systems [24]. Various authors have not had a detailed discussion on applying deep learning methods for detecting cyber-attacks contrary to cyber-physical systems. The brief survey was given by authors [25] with a four-step framework that uses deep learning methods for detecting cyber-physical systems cyber-attacks. The biggest concern nowadays is the security of CPS. Deep Learning approaches are precisely intended to handle large datasets compared to small datasets with numerous features. These methods can approximate any function as deep learning has a rich class of models. All these methods are appropriate in cyber-physical systems due to the following reasons:

- Information gathered from CPSs is commonly high layered as information from countless physical sensors and cyber sensors.
- A steady development of information because of upgrades and openness to novel susceptibilities are there.
- The models should be continually refreshed with novel information to represent the drifting of the framework and further vector assaults.

1) DEEP LEARNING WITH CPS

Deep learning has emerged as a powerful technique for handling the complexities of Cyber Physical Systems (CPS). It has been applied to various CPS applications such as anomaly detection, fault diagnosis, control, and optimization.

Deep learning algorithms such as Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), and Deep Belief Networks (DBN) have been used for CPS applications. CNNs have been used for image and signal processing tasks in CPS, while RNNs have been used for time-series data analysis in CPS. DBNs have been used for fault diagnosis and anomaly detection in CPS.

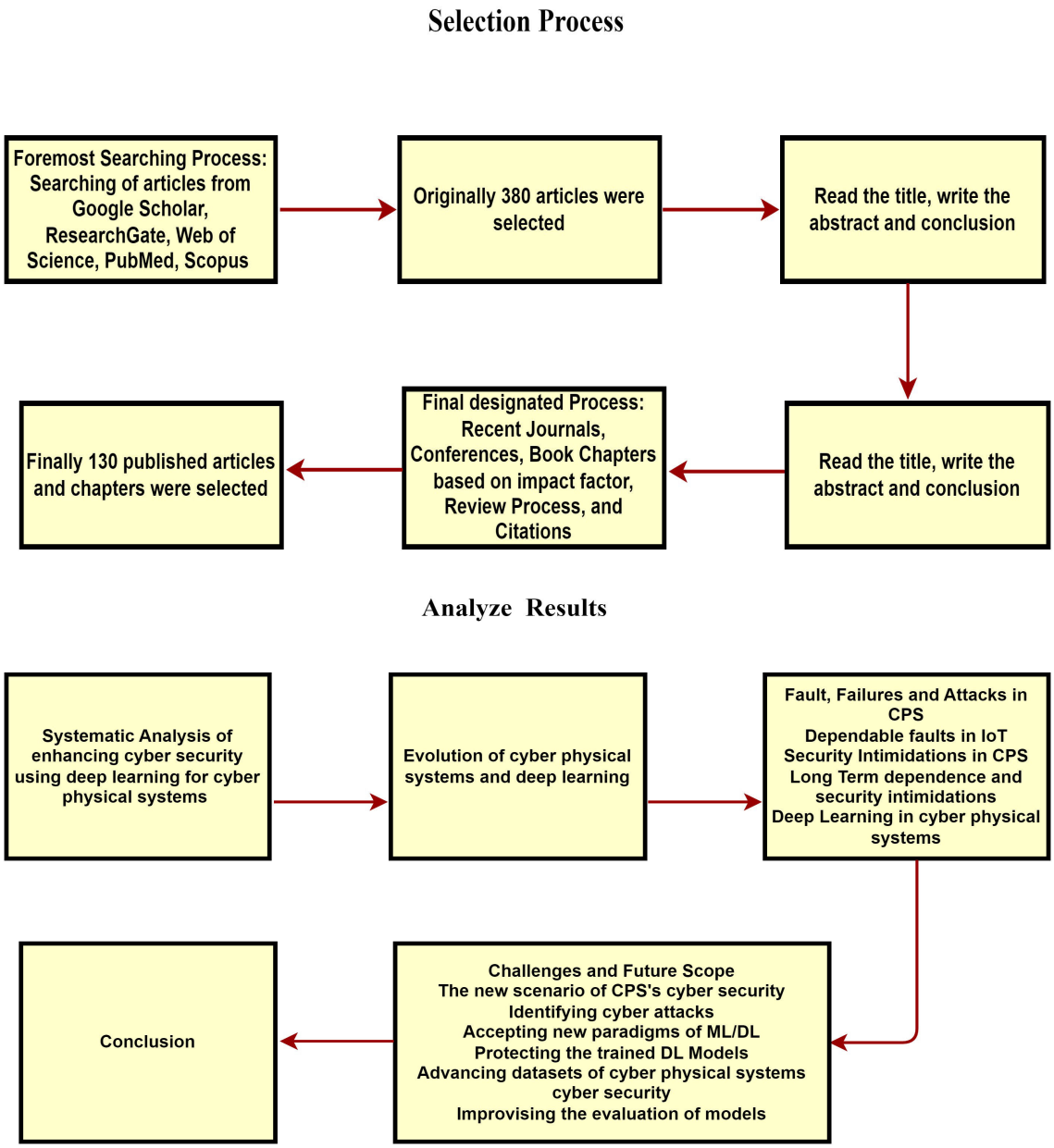


FIGURE 1. Methodology for selecting and analysing the survey.

Deep learning models require large amounts of data for training, and CPS data is often limited and expensive to collect. Transfer learning techniques have been applied to leverage pre-trained models and overcome this challenge. Additionally, the security of CPS can also be enhanced using deep learning techniques, such as using autoencoders for intrusion detection, and generative adversarial networks (GANs) for generating adversarial examples to improve the robustness of CPS. Overall, deep learning has shown promising results in various CPS applications and is expected to play a significant role in advancing the state-of-the-art in CPS.

C. QUANTUM LEARNING WITH CPS

Quantum machine learning is an emerging field that combines quantum computing and machine learning techniques to solve complex problems. However, quantum computing technology is still in its early stages of development, and its practical applications in the field of cybersecurity and CPS are still largely theoretical.

One of the potential advantages of quantum machine learning for CPS security is its ability to perform complex calculations faster than classical computing, which could potentially speed up the detection and response to cyber attacks. However, the development of quantum machine

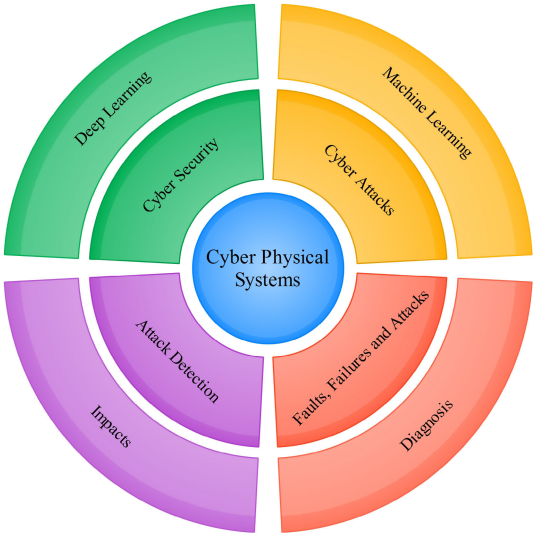


FIGURE 2. Broad division of concepts discussed in the paper.

learning algorithms and their integration into CPS systems is still a topic of ongoing research. Quantum learning with CPS is a promising area of research, but its practical applications in the field of cybersecurity and CPS are still largely speculative, and much work is needed to develop and test quantum machine learning algorithms for real-world CPS systems.

D. DEEP LEARNING AND QUANTUM LEARNING WITH CPS

Deep learning and quantum learning are two areas of research that can have potential applications in Cyber-Physical Systems (CPS).

Deep learning involves training deep neural networks to perform complex tasks, such as image and speech recognition, natural language processing, and even autonomous decision-making. In CPS, deep learning can be used to analyze large volumes of data generated by sensors and devices in real-time, detect anomalies and potential threats, and make accurate and timely decisions to ensure the safety and security of the system.

Quantum learning, on the other hand, uses the principles of quantum mechanics to process and analyze data. It involves the use of quantum algorithms and quantum computers to solve problems that are computationally infeasible using classical computers. In CPS, quantum learning can be used to optimize the performance of the system, reduce energy consumption, and enhance security by developing quantum-resistant encryption algorithms.

While both deep learning and quantum learning have potential applications in CPS, they are still in the early stages of development and require further research to fully understand their capabilities and limitations in this domain.

E. CONTRIBUTIONS

In this paper, we undertake an extensive investigation into the application of deep learning for cyber-attack detection within cyber-physical systems (CPS). Our contributions encompass:

- Here in this paper, authors have performed an exhaustive survey of contemporary methods and techniques for cyber-attack detection in CPS, harnessing the capabilities of deep learning.
- The authors have introduced a rigorous methodological framework that serves as the cornerstone of the research. This framework not only positions our work within the current landscape but also facilitates the systematic analysis and evaluation of recent developments in this domain.
- A comprehensive examination of reliability failures and security threats, specifically tailored to the various layers of CPS architecture.
- The authors have delved into the realm of solutions with meticulous attention to technical intricacies. The discussions provide in-depth insights into the implementation of security measures, considering factors such as encryption algorithms, anomaly detection thresholds, and real-time monitoring mechanisms.
- In an alignment with the core theme, the authors have engaged in a technical discourse surrounding challenges and future trends. This includes embracing novel paradigms in machine learning (ML) and deep learning (DL), devising techniques to safeguard trained DL models from adversarial attacks, advancing the construction of CPS cybersecurity datasets with a focus on data diversity and volume, and enhancing the technical rigor of model evaluation methodologies.

F. MOTIVATIONS

As soon as the intelligent computing systems introduce predictable intelligence towards the issues of cyber, so the researchers are more inclined to use intelligent computing for secure computations, as there are various challenges for detecting attacks also. The question is whether computation spectacle can help improve security concerns. The security of Cyber physical systems is a significant concern, and that's why it is mandated to study the safety of cyber physical systems. So an analysis of cyber security of the cyber physical system is required, and it is presented in this work.The taxonomy of paper is shown in Figure 3.

G. ORGANIZATION

The rest of the paper is categorized into various subsections: Section II describes the literature review of evolution of cyber physical systems and deep learning. Section III discusses the Mathematical Modeling Framework for Enhancing Cyber Security in Cyber-Physical Systems using Deep Learning. Section IV describes the fault, failures and attacks in cyber physical systems. Open issues for securing CPS are described in Section V.Challenges and Future Scope is described in Section VI. Finally paper is concluded in Section VII.

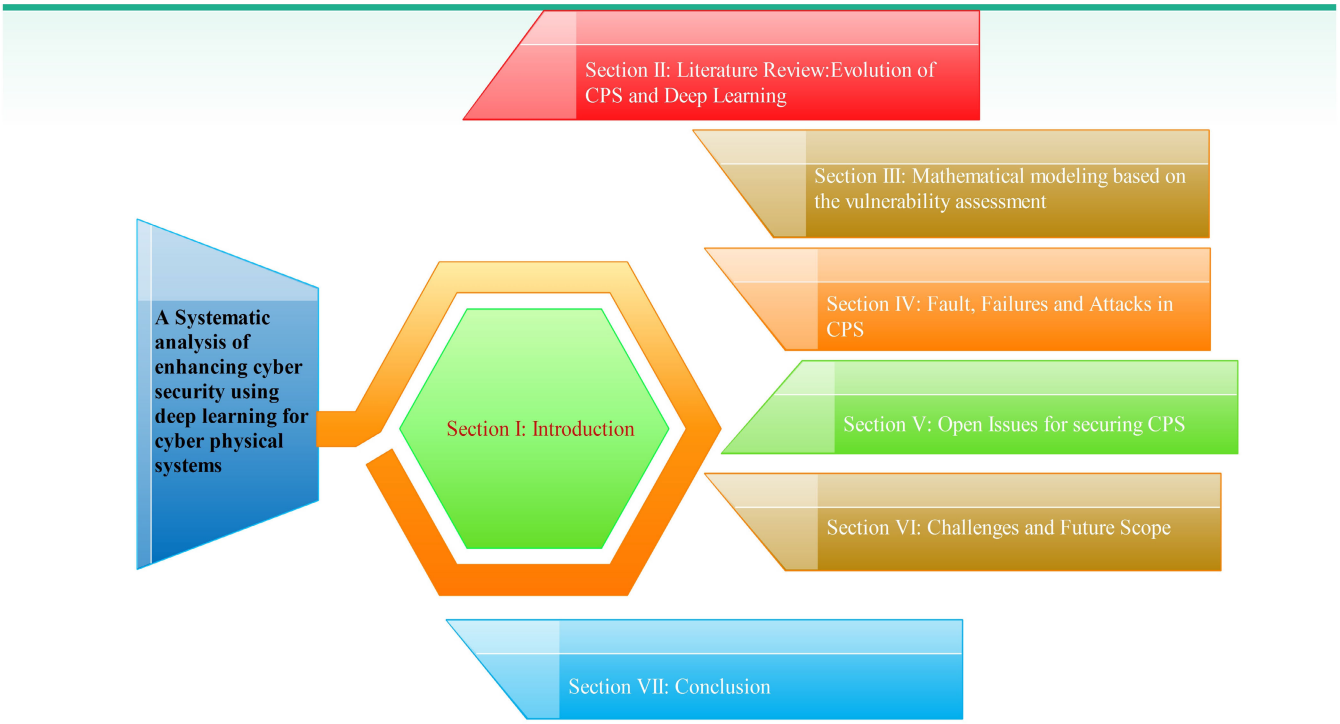


FIGURE 3. Organization of paper.

II. LITERATURE REVIEW: EVOLUTION OF CYBER PHYSICAL SYSTEMS AND DEEP LEARNING

Cyber-Physical System (CPS) is the coordination of computers with existing frameworks. The embedded computer screen, the actual control cycles, the feedback loops, and the physical approaches also influence calculations. Cyber-Physical System is near to convergence, with no association of the physical and the cyber world as a conceptual motivation. It consolidates designing representations and strategies from mechanical, ecological, typical, electrical, biomedical, compound, aeronautical, and modern designing with the models and techniques for software engineering. As the expressions ''the internet'' and ''cyber-physical system'' originate via a similar root, ''computer science,'' which is authored by Norbert Wiener [5], an American statistician who enormously affected the advancement of control frameworks theory, would be more precise. Wiener spearheaded innovation for the programmed pointing and shooting of hostile airplane weapons. Albeit the components he utilized didn't include computerized PCs, the standards contained are like those pre-owned nowadays in computer-based criticism controller frameworks [26]. The control rationale is a calculation, though one has done via simple circuits and mechanical portions, and consequently, computer science is the combination of actual cycles, analysis, and correspondence. The similitude is adept for control frameworks.

CPS is here and is mistaken for ''online protection,'' which concerns the secrecy, uprightness, and accessibility of information and has no characteristic association with actual cycles. The expression ''network protection'' along these lines is about the security of the internet and is subsequently, by implication, associated with computer science. CPS includes many testings security and protection concerns, yet these are in no way, shape, or form the main worries.

It is an innovation in that intelligence associates our actual world with our data world. Cyber Physical Systems is more essential and solid than these as it doesn't directly reference either execution draws near or precise applications like ''Industry'' in Industry 4.0. It centers as a substitute to the principal scholarly issue of adjoining the designing customs of the digital and an actual universe. One could discuss a CPS hypothesis like the ''direct frameworks hypothesis.'' CPS has turned out to be a common factor in critical infrastructure because of its massive influence and commercial assistance [6]. The growing reliance of crucial infrastructure on cyber-based skills has turned them susceptible to cyber-assaults like interference, auxiliary, and exclusion of data from the communique networks [7], [8], [9].' Therefore, the sanctuary of cyber-physical systems has become a perilous concern. A brief history of computer systems and cyber physical systems is illustrated in Figure 3.

Deep Learning (DL) has acquired huge consideration in previous years. It has worked on the state-of-art execution of numerous claims, remembering applications related to security for basic designs, like interruption identification, malware discovery, access control, and peculiarity recognition and orders [6]. DL was presented in the late twentieth era, which was begun with the investigation of Artificial Neural

FIGURE 4. Taxonomy of survey.

Networks (ANNs). Deep Neural Networks (DNN) comprise a set of layers that gain proficiency with a progression of hidden portrayals progressively [27], [28]. Higher-level descriptions contain enhanced parts of information tests that are helpful for segregation and stifle unessential highlights. Deep Learning models have worked on the cutting-edge execution in various assignments [10], [11]. The summary of related works of various methods and applications are shown in Table 1.

Figure 4 delineates the general idea of cyber-physical systems and the IoT for cyber physical systems. It displays current cyber-physical systems, how elements could be separated from such frameworks, conceivable deep learning models, and the benefits of utilizing deep learning [29]. Furthermore, the information gathered from existing digital frameworks is ordinarily high layered. Deep Learning models are explicitly intended to manage high layered information. Different attributes of CPS incorporate, proceed with the development of data, information float, and openness to new framework dangers. This way, it is crucial to assemble deep learning-based sanctuary models which are versatile and extendible with the information float, nonstop disclosure of new framework dangers and weaknesses [12].

This idea of "Generalization" is one significant issue for constructing security-based requests in cyber-physical systems as creating AI models for one situation is almost difficult to use, experiencing the same thing even in a similar setting. In this manner, it is a quintessence to zero in on speculation that deep learning models utilized in such applications are ordinarily high layered. Deep Learning models are explicitly intended to manage high-layered information. Different attributes of CPS incorporate, proceed

with the development of data, information float, and openness to new framework dangers. This way, it is crucial to assemble deep learning-based security models which are versatile and extensible by the information float, nonstop disclosure of new framework dangers and weaknesses [12]. This idea of ''Generalization'' is one significant issue for constructing security-based requests in cyber-physical systems as creating AI models for one situation is almost difficult to use, experiencing the same thing even in a similar setting. It is illustrative to zero in on speculation of deep learning models utilized in such applications [30], [31].

III. MATHEMATICAL MODELING BASED ON THE VULNERABILITY ASSESSMENT

The mathematical modeling framework for enhancing cyber security in Cyber-Physical Systems (CPS) using deep learning, based on the vulnerability assessment are stated below and explained in figure 5.

1) **Problem Formulation:** Minimize the objective function $J(\Theta)$, representing the cost or vulnerability.
2) **System Representation:** Define the CPS system as $CPS = \{C_1, C_2, \ldots, C_n\}$. Enumerate vulnerabilities as $Vulnerabilities = \{V_1, V_2, \ldots, V_m\}$.
3) **Threat Modeling:** Define a Threat Vector $T = [T_1, T_2, \ldots, T_k]$ representing potential threats.
4) **Deep Learning Integration:** Integrate deep learning models to process system information. Define the model's output as f_Θ(Input).
5) **Data Requirements:** Specify the dataset $D = \{(Input_1, Label_1), \ldots, (Input_N, Label_N)\}$ for model training.
6) **Mathematical Equations:** Develop equations to quantify vulnerability levels.

$$\text{Vulnerability Level} = g(\text{Threat Vector, Deep Learning Output})$$

7) **Quantification of Vulnerabilities:** Assign a vulnerability score based on the vulnerability level.

$$\text{Vulnerability Score} = h(\text{Vulnerability Level})$$

8) **Validation and Verification:** Establish validation metrics to evaluate model performance. $ValidationMetric = ValidationFunction(ModelOutput, GroundTruth)$
9) **Sensitivity Analysis:** Assess model sensitivity to parameter changes. $Sensitivity = \frac{\partial J}{\partial \Theta}$
10) **Limitations and Assumptions:** Clearly state any assumptions and limitations in the model.

$$\text{Assumption}_i : \ldots$$
$$\text{Limitation}_j : \ldots$$

11) **Comparative Analysis:** Develop metrics for comparing the model against other approaches.

$$\text{Comparison Metric} = \text{Compare(Model, Other Models)}$$

12) **Implications and Recommendations:** Discuss the implications of the findings. Provide recommendations for practical applications.

IV. FAULT, FAILURES AND ATTACKS IN CYBER PHYSICAL SYSTEMS

A failure is an occurrence that arises when an organization diverges as of its planned performance. The failure establishes because of its inadvertent state. The origin of a fault might be internal or external. The internal faults occur due to their physical nature (such as brokerage of the component connector), and faults occur due to their design (software or hardware-related bugs) [55]. Peripheral faults (External) initiate from the environmental cause like noise. Faults may be categorized into permanent and temporary faults. However, a temporary fault occurs for short time span. It may create an error, and this may lead to perpetual failure. Similarly, Physical faults and inputs can be temporary or it can be permanent, whereas the design faults are constantly permanent. The faults which could not be analytically imitated are usually known as irregular faults. This kind of fault can be led to soft errors.

The cyber-physical systems/Internet of Things (CPS/IoT) infrastructure is shown in the figure. Faults might arise at diverse layers of architecture, such as the physical layer or control layer, respectively [13]. The physical layer is susceptible to interruption, direct interference, or demolition of physical items. The network layer can make the connection of devices. The monitors and controllers in the control layer are susceptible to environmental uncertainties and handling of extents and control signals [55], [56]. The collection of information can be done by the information layer and is mainly vulnerable to issues related to secrecy and integrity.

A. DEPENDABLE FAULTS IN IoT

Internet of Things tends to communicate failures primarily due to its extent and heterogeneousness. Previously, traditional cyber-physical systems used to ignore or remove such failures by validating and verifying the design. Though IoT is involved in technology, it is growing in size with time. The subsequent faults might arise per cyber-physical systems layer:

- **Physical Layer: - Intrusion:** Interference of a signal. The quantity of associated devices and the radiation rises, affecting measurements of sensors, conveyed communications, or control indications.
- **Network Layer: - Collision of Messages:** In correspondence to intrusion, the quantity of interactive devices may activate communique failures such as crashes or overloading of the net- ' work. - Violation of Protocol:

TABLE 1. Summary of different methods and applications in the context of Deep Learning and CPS by various authors, along with challenges in ML algorithms.

Methods	Deep Learning	Application	Cyber Physical Systems	Reference	Challenges in ML Algorithms
Classification based techniques, Clustering based techniques, Statistical, anomaly recognition approaches	No	Cyber Interruption Detection, Detection of Fraud, etc	No	[32]	Limited labeled data, imbalanced datasets, model interpretability
Program Analysis	No	Commodity Internet of Things	Related but not fully covered	[33]	Scalability, real-time processing
Physical properties	No	Cyber Physical Systems	Yes	[34]	Sensor noise, environmental variability
Deep learning	Yes	Cyber Interruption Detection, Detection of Fraud	No	[35]	Model complexity, computational resources
Attack Based Tree, Model-based technique	No	Cyber Physical Systems (focus on SCADA)	Yes	[36]	Security of control systems, attack detection
Deep learning	Yes	Cyber Physical Systems	Yes	[37]	Scalability, real-time processing
Knowledge-Based technique, Behaviour-Based Interruption Recognition system	No	Cyber Physical Systems	Yes	[38]	Knowledge representation, anomaly detection
Interruption Detection system, Machine learning	No	Cyber Physical Systems	Yes	[39]	False positives, adaptive adversaries
-	-	Smart home IoT	Related but not fully covered	[40]	Privacy, device heterogeneity
Plant models based technique, Noise-based detection, State estimation based technique	No	Cyber Physical Systems	Yes	[41]	Model accuracy, noise robustness
Deep learning	Yes	Internet of Things	No	[42]	Energy efficiency, resource constraints

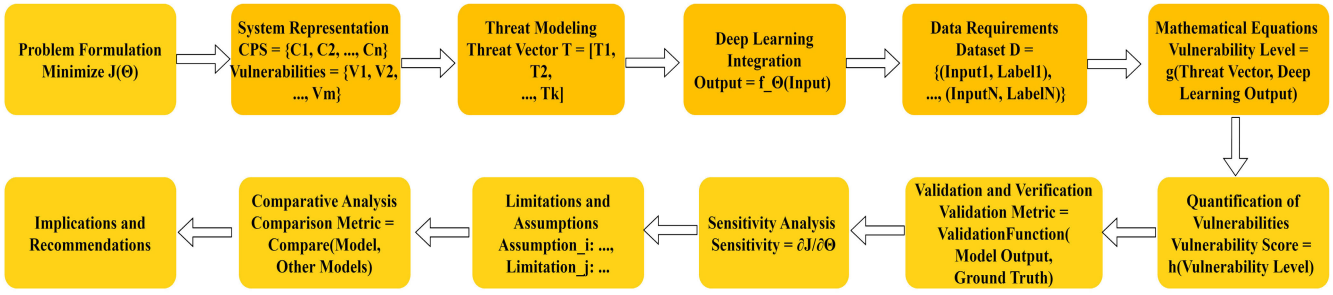


FIGURE 5. Mathematical modeling framework for enhancing cyber security in cyber-physical systems using deep learning.

The protocol violation occurs due to incorrect message content.

- **Control Layer: - Deadline Miss:** Delayed in the response of control signal. The Control loops has to survey the restraints related to timing of a cyber-physical system application. - Misusage: Sending erroneous inputs to a component
- **Information Layer: - Inaccessibility:** Lost data instigated by a skill apprise. The things might be linked, detached, or updated in the Internet of Things.

B. SECURITY INTIMIDATIONS IN CYBER-PHYSICAL SYSTEMS

Security has been one of the biggest concerns in computer networks to identify susceptibilities and avoid malicious attacks on the devices. Whereas in cyber-physical systems, more and more susceptibilities arise in the physical area and the indeterminate behavior of the physical atmosphere. The categorization of attacks applied per cyber-physical systems layer is given below:

- **Physical Layer: - Information Leakage:** Stealing perilous information from various devices such as private keys - Denial of Service: Manipulating various parameters for performing DoS attacks.
- **Network Layer: - Jamming:** Overloading the communication protocol by introducing false traffic. - Collision: Manipulation of timing, the power which leads to collision of data or violation of communication protocol. - Routing misdirects: Manipulating the routing mechanism leads to collision of data, flooding of data, and discriminating promoting of facts [57], [58].
- **Control Layer: - Desynchronizing:** Violating the timing or manipulation of clocks. This could lead to denial of service and leakage of information.
- **Information Layer: - Eavesdropping:** Stealing or sniffing of information. It is one of the biggest intimidations associated with confidentiality. Furthermore, data could also be deployed to accomplish various attacks. The potential intimidations and penalties could be stated in sanctuary intimidation models for cyber-physical systems.

TABLE 2. A systematic analysis of enhancing cyber security using deep learning for cyber physical systems" vs. existing survey papers.

Paper Reference	Scope and Focus	Methodological Approach	Technical Depth	Contributions	Originality
[43]	Smart Grid attacks, vulnerabilities, detection and defences	Review, analysis, and synthesis	Moderate	Identify key challenges, proposed solutions	Focused on existing attacks and defenses
[44]	IoT intrusion detection methods	Review, analysis, and synthesis	Moderate	Classification and detection techniques	Explores existing methods
[45]	ML techniques in CPS cyber security	Review, analysis, and synthesis	Moderate	Comparative analysis of methods	Emphasis on existing ML techniques
[46]	Survey on deep learning-based attack detection in CPS cybersecurity	Analytical survey of existing literature, summarizing key techniques and challenges	High technical depth, covers a wide range of deep learning techniques in the context of CPS security	Comprehensive analysis and insights into the state-of-the-art in deep learning -based attack detection for CPS cybersecurity	Original in presenting a holistic view of deep learning in CPS attack detection
[47]	Review of security analysis in CPS using machine learning	Literature review and analysis of machine learning applications in CPS security	Moderate technical depth, focuses on summarizing existing research in the domain	Provides a comprehensive review of security analysis in CPS using machine learning techniques	Original in presenting a consolidated overview of ML applications in CPS security
[25]	Survey on the generalization of deep learning for CPS security	Analytical survey of deep learning generalization techniques in CPS security	Moderate technical depth, emphasizing generalization aspects	Offers insights into the challenges and opportunities in applying deep learning for CPS security with a focus on generalization	Original in exploring generalization aspects in deep learning for CPS security
[48]	Survey on resilient machine learning for networked CPS	Analytical survey of machine learning security in the context of networked CPS	High technical depth, covers a range of resilient machine learning techniques	Provides a comprehensive survey on securing machine learning in networked CPS environments	Original in addressing resilience challenges in machine learning for networked CPS
[49]	Survey on deep learning-based anomaly detection in CPS	Analytical survey of progress, challenges, and opportunities in deep learning-based anomaly detection	High technical depth, explores various deep learning-based approaches	Offers a comprehensive overview of the progress and potential in deep learning-based anomaly detection for CPS	Original in presenting a state-of-the-art survey on anomaly detection in CPS using deep learning
[50]	Federated deep learning for intrusion detection in industrial cyber–physical systems	DeepFed: Federated deep learning	High	Intrusion detection, Federated learning	Novel approach in applying federated learning to industrial CPS
[51]	Attack graph model for cyber-physical power systems using hybrid deep learning	Hybrid deep learning approach	High	Attack graph modeling, Smart Grid security	Integration of deep learning into attack graph modeling for power systems
[52]	Real-time stability assessment in smart cyber-physical grids: a deep learning approach	Deep learning for real-time stability assessment	Moderate	Stability assessment in smart grids	Application of deep learning to real-time stability analysis in smart grids
[53]	Blockchain-based deep learning approach for cybersecurity in next-generation industrial cyber-physical systems	Blockchain and deep learning integration	High	Cybersecurity, Blockchain, Industrial CPS	Unique combination of blockchain and deep learning for enhanced cybersecurity
[54]	Deep learning-based DDoS-attack detection for cyber–physical system over 5G network	Deep learning for DDoS attack detection	High	DDoS attack detection, 5G networks	Application of deep learning for DDoS detection in 5G- enabled CPS
Our Paper	CPS security using DL	Systematic analysis	High	Innovative solutions, key challenges, and insights	Emphasis on original insights

C. LONG-TERM DEPENDENCE AND SECURITY INTIMIDATIONS

The Internet of things and cyber-physical systems will endure deviations over time, particularly when imperiled by a long operational period. Following features of the change might cause faults such as changes in the environment, functional changes, and changes in technology.The catagories of attacks implied on different CPS systems are mentioned below:

- **Physical Layer:**At this layer there is material decay and environmental effects issues at this layer and this voilates the environment.
- **Network Layer:**It overloads the information by putting false traffic on the network. Due to this the communication through protocol also voilates.
- **Control Layer:**It disturbs the timing or manipulates the clocks this leads to the aging effects and uncertainity effects.

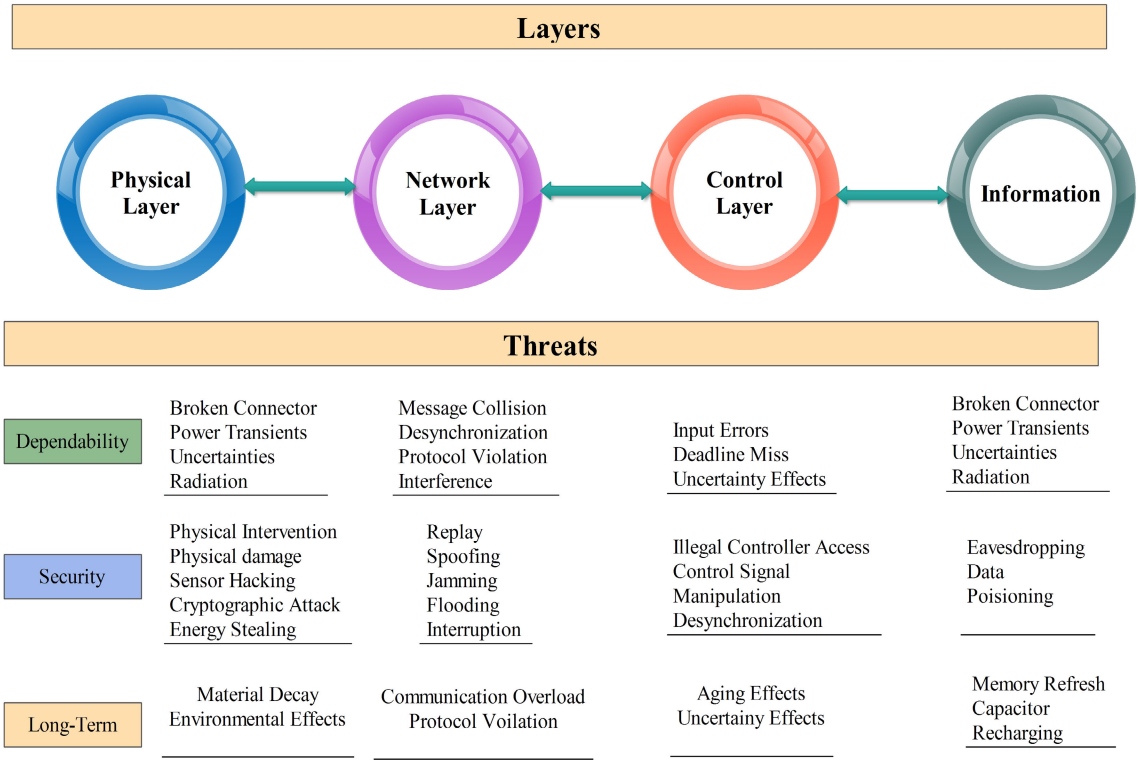


FIGURE 6. Reliability failures and sanctuary intimidations with reference to cyber physical systems layers.

TABLE 3. Threat models for different CPS layers.

Layers	Physical Layer	Sensor/Actuator Layer	Communic-ation Layer	Control Layer	Information Layer	Integration level Layer
Attacks	Manufacturer, Designer, External Attacker	Manufacturer, Designer, External Attacker	Manufacturer, Designer, External Attacker	Manufacturer, Designer, External Attacker	Manufacturer, Designer, External Attacker	Manufacturer, Designer, External Attacker
Methodology	Physical Interference	Hacking, Control Access, Information Influences	Replay, Sybil, Congestion, Implosion, Deceiving	Eavesdropping, Control Access	Eavesdropping	All conceivable control & Communication assaults
Payloads	Denial of Service, Aging Consistency	Energy Stealing, Denial of Service, Data Leakage, Desynchro-nization	Energy Thieving, Denial of Service, Information Leakage, Desynchro-nization	Leakage of Information, Denial of Service, Desynch-ronization	Leakage of Information	Stealing of energy, Denial of Service, Leakage of Information, Desynchron-ization

- **Information Layer:**The biggest itimidation concerned with confidentiality is stealing of information. The refershing of memory, recharging is theissues relaed to this layer.

D. DEEP LEARNING IN CYBER-PHYSICAL SYSTEMS

Here we discuss how deep learning can be applied in CPS. So, the introduction of deep learning is required for how it is used in security-related applications such as CPSs. Nowadays, DL is gaining huge focus in data science to enhance performance in various applications [12]. Deep Learning Algorithms contain hierarchical architectures with many layers in which higher-level features are explained in standings of lower-level features capable for the extraction of features and concepts from underlying data [14]. These architectures can produce outstanding results in applications like cyber-physical systems security [12], [15]. Figure 5 presents various applications of DL for CPS. The deep architectures are formed of various hidden layers [4]. Deep Learning methods can represent additional abstract illustrations of information due to the multi-level architecture.

Deep Learning models have revealed better generalization competence in many practical applications than shallow ANNs.

There are some major fields where deep learning has been effectively applied in cyber-physical systems for security-related determinations such as detection of anomaly, detection of malware and threat hunting, susceptibility recognition, interruption detection, prevention of blackouts, assaults, and destructions in CPSs.

E. CYBER ATTACKS

In current years, there was a hike in the proportion of cyber attacks aiming cyber physical systems with distressing significances. As per recent studies [86], [97], cyber physical systems are susceptible to malicious code injection attacks [66] and code reuse attacks [76]in addition with false data injection attacks [77], zero-control data attacks [83]. These kinds of attacks can lead to black out targeting cyber physical system's industrial devices and systems as shown in Table 4.

V. OPEN ISSUES FOR SECURING CPS

There are several open issues and research directions related to securing Cyber Physical Systems (CPS) using Deep Learning (DL). Some of the key areas of focus include:

- **Data Collection and Preparation:** CPS typically generate vast amounts of data that are relevant to the security of the system [31], [55]. However, collecting and preparing this data for use in DL models can be challenging, particularly when the data is highly heterogeneous and distributed across multiple sources [105].
- **Model Selection and Development:** There is a need to identify the most appropriate DL models for securing CPS and to develop these models so that they can be effectively applied to real-world scenarios [106]. This includes choosing the right type of model, such as CNNs or RNNs, and optimizing the model's architecture and parameters to improve its performance.
- Integration with Other Security Measures: DL models need to be integrated with other sanctuary procedures to ensure that they are effective in detecting and mitigating cyber threats [107], [108]. This may include integrating DL models with intrusion detection systems, firewalls, or access control systems, or incorporating additional data sources such as log data or network traffic data to improve the accuracy of the models.
- **Scalability and Real-Time Processing:** CPS generate huge quantities of data in real-time, which makes it challenging to use DL models to detect and answer to cyber intimidations in real-time [109], [110]. There is a need for DL models that are able to scale to handle large amounts of data and that can be implemented in real-time to detect and reply to cyber intimidations in real-time.
- **Explainability and Trustworthiness:** One of the challenges of using DL models for security purposes is the lack of transparency and interpretability of the models. There is a need to develop DL models that are more transparent and interpretable, so that security experts and decision-makers can understand the basis for the models' predictions and decisions [55], [56].
- **Adversarial Robustness:** CPS are often targeted by sophisticated cyber-attackers who use techniques such as adversarial machine learning to evade detection. There is a need for DL models that are robust to these attacks and that can continue to operate effectively even in the presence of adversarial inputs [111].

These are some of the key areas of focus for securing CPS using DL, and there is a growing body of research aimed at addressing these challenges. By developing DL models that are effective in detecting and mitigating cyber threats, and by integrating these models with other security measures, it is possible to improve the sanctuary of CPS and reduce the risk of cyber-attacks.

A. RESEARCH DIRECTIONS IN SECURING CPS USING DL

There are several open issues and research directions for securing CPS using DL techniques. Some of these include:

- **Development of robust and accurate DL-based intrusion detection systems for CPS:** This involves the usage of DL methods such as CNNs and RNNs to detect and classify various types of cyber-attacks in CPS.
- **Improving the interpretability of DL-based CPS security models:** Currently, one of the main limitations of deep learning models is their absence of interpretability, making it hard to comprehend how they attain at their decisions. Research is needed to make DL models more transparent and interpretable [57].
- **Anomaly detection in CPS using unsupervised DL techniques:** Unsupervised DL techniques such as Autoencoders and Variational Autoencoders (VAEs) could be utilized to detect anomalies in CPS by learning the normal behavior of the system and identifying nonconformities from this normal behavior [112].
- **Adversarial attacks on DL-based CPS security models:** Adversarial attacks are a major concern in DL, and they pose a threat to the security of CPS systems. Research is needed to develop defense mechanisms against these attacks and to enhance the robustness of DL-based security models [113].
- **Integration of DL with other security techniques:** DL-based security models can be combined with other security techniques such as firewall, detection of intrusion and anticipation systems, and encryption to create a more comprehensive and effective security system for CPS [114].
- **Handling large and complex data in CPS using DL:** CPS systems generate large amounts of data, and this data is often complex and unstructured. Research is needed to develop DL models that can handle this data effectively and efficiently [58], [115].

TABLE 4. Different CPS system with different types of anamolies.

CPS System	Existing Work	Type of Anomalies								
		Attacks					Faults			
		DoS	MITM	Packet Injection	Malware	FALSE Control Signals	Sensor Layer	Network Layer	Control System	Manually Created
Industrial Control System	[37]	Yes	Yes	X	No	No	No	No	No	No
	[59]	No	Yes	No	No	Yes	No	No	No	No
	[60]	No	No	No	No	No	No	No	No	X
	[61]	No	No	No	No	No	Yes	No	No	No
	[62]	No	No	No	No	No	Yes	No	No	Yes
	[63]	No	Yes	No	No	Yes	No	No	No	No
	[64]	Yes	No	Yes	No	Yes	No	No	No	No
	[65]	No	Yes	No	No	Yes	No	No	No	No
	[66]	No	No	No	No	No	No	Yes	No	No
	[67]	No	No	No	No	No	Yes	No	No	No
	[68]	No	No	No	No	No	Yes	No	No	No
	[69]	No	No	No	No	No	Yes	No	No	Yes
	[70]	No	No	No	No	No	Yes	No	No	Yes
	[71]	No	No	No	Yes	No	Yes	No	No	Yes
	[72]	Yes	No	Yes	Yes	X	No	No	No	Yes
	[73]	No	No	Yes	No	No	No	No	No	
	[74]	No	Yes	No	No	Yes	No	No	No	No
Smart Grid and ITS	[75]	No	No	No	No	No	No	No	No	Yes
	[76]	Yes	X	Yes	Yes	Yes	No	No	No	Yes
	[77]	No	Yes	No	No	No	No	No	No	Yes
	[78]	No	Yes	No	No	No	No	No	No	Yes
	[79]	No	Yes	No	No	No	No	No	No	Yes
	[80]	No	Yes	No	No	No	No	No	No	Yes
	[81]	No	Yes	No	No	No	No	No	No	Yes
	[82]	No	No	No	No	No	Yes	No	No	No
	[83]	No	Yes	No	No	No	No	No	No	Yes
	[84]	No	No	No	No	No	No	No	No	No
	[85]	No	Yes	No	No	No	Yes	No	No	Yes
	[86]	No	No	Yes	No	Yes	No	No	No	Yes
	[20]	Yes	No	Yes	No	Yes	No	No	No	Yes
	[87]	No	No	Yes	No	No	X	No	No	Yes
	[88]	Yes	Yes	Yes	No	Yes	No	No	No	No
	[89]	No	Yes	Yes	No	No	No	No	No	Yes
Aerial System	[90]	No	No	No	No	Yes	No	No	No	No
	[91]	No	No	No	No	Yes	No	No	No	No
	[92]	No	No	X	Yes	No	No	No	No	No
	[93]	No	No	No	No	No	No	Yes	No	No
	[94]	No	No	No	No	No	No	No	Yes	Yes
	[95]	No	No	No	No	No	No	No	No	Yes
	[96]	No	No	No	No	No	No	No	No	Yes

Note*: X belongs to Not Clear but inferred to be Yes

VI. CHALLENGES AND FUTURE SCOPE

The major potential fields are shown in the figure where the research areas may arise. The seven steps of the research methodology are already shown in the figure. The research literature can be improvised with our research methodology, and with the help of this, the comparative analysis can be done appropriately. The further challenges can be categorized into different directions, which are:

A. THE NEW SCENARIOS OF CYBER-PHYSICAL SYSTEM'S CYBERSECURITY

The various articles analyzed communication networks in the scenarios of cyber-physical systems [25], [103]. Most of the survey papers have examined the methods of cyber-physical systems in the intelligent grids or the water treatments of plants described in the 13/27 survey papers. It is the emergent way to apply deep learning in the current industry. Deep Learning is used for detecting the faults and defects in the industrial sector of complex items [97]. But these were not considered as there were no issues of cyber security covered in this. The cyber-attacks and threats usually exist in the cloud server where design models are stored. We suggest that the blockchain will be analyzed more in a broader way in collaboration with cyber-physical systems, and the variety and development of cyber-physical systems scenarios will lead to intense analysis of cyber security [116], [117], [118].

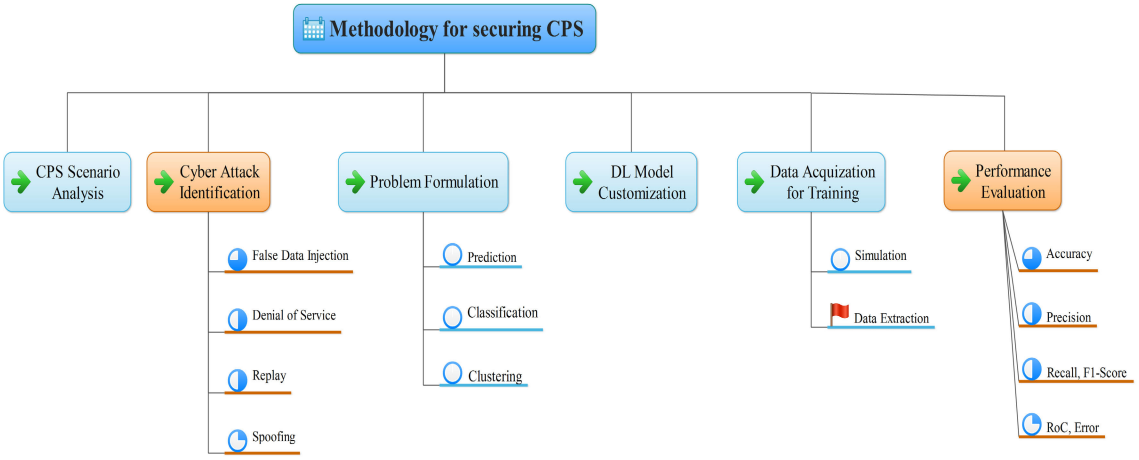


FIGURE 7. The deep learning driven methodology for security of cyber physical systems.

TABLE 5. Real cyber physical systems attacks.

Country	Nature of Attack	Type	Target	Motives	Date
USA	Slammer Worm Sensors Failure	Malware-DoS Accident	Ohio Nuke Plant Network [98] Taum Sauk Hydroelectric Failure of Power Station [99]	Criminal N/A	Jan 25,2003 14 Dec 2005
	Installed Software Update	Undefined Software	Georgia Nuclear Power Shutdown of Plant [100]	Unclear	Mar 7, 2008
	Reconnaissance	Undefined Software Programs	US Electricity Grid [101]	Political	Apr 8, 2009
	Backdoor	Unauthorised Access	Springfield Pumping Station [97]	Criminal	Nov 8, 2011
	Physical Breach	Unauthorised Access	Georgia Water Treatment Plant [102]	Criminal	Apr 26, 2013
Iran	Stuxnet [103]	Worm	Iranian nuclear facilities	Political	Nov,2007
	Stuxnet-2	worm	power plant and another industry	Political	25 Dec 2012
	DDoS	Disruptive	Iranian Infrastructure and communications companies	Political	03 Oct 2012
	Computer Virus	Malware	Iranian key oil facilities	Political	23 Apr 2012
Saudi Arabia	Shamoon-1	Malware	Saudi infrastructure in the energy industry	Religio-Political	15 Aug 2012
	Shamoon-2	Malware	Saudi government computers and targets	Religio-Political	17 Nov 2016
	Shamoon-3	Malware	Tasnee and other petrochemical firms, National Industrialization Company, Sadara Chemical Company	Religio-Political	23 Jan 2017
Qatar	Shamoon	Malware	Qatar's RasGas	Political	30 Aug 2012
United Arab Emirates	Trojan Laziok	Malware	UAE energy sector	Political	Jan-Feb 2015
Australia	Remote Access	Unauthorised Access	Maroochy Water Breach [73]	Criminal	March, 2000
Canada	Security Breach	Exploited Vulnerability	Telvent Company [104]	Criminal	Sept 10, 2012

B. IDENTIFYING CYBER ATTACKS

Most of the survey papers have analyzed the false data injection attacks. Recognizing surreptitious untruthful data injection attacks is challenging as a considerable amount of noise is being formed in the cyber-physical systems, and there is a deficiency in the mechanisms of cyber security for authenticating the devices and messages which are transmitted over the network. Some categories of false injection attacks depend on the information of invaders [119], [120]. As no such advanced information is needed to initiate a denial of services attacks, individually logged packets are required for replay attacks, scanned tools for penetrating attacks, and automated tools for fuzzy attacks. However, the cyber security of cyber-physical systems is a vast area compared to cyber-attacks in contradiction to cyber-physical systems. Detection of cyber-attacks that are initiated in cyberspace and infiltrate the physical domain is a challenging task [22], [121]. We assume that emergent cyber-attacks will head the defense devices, but the risk could be moderated via the data-driven approach.

C. ACCEPTING NEW PARADIGMS OF MACHINE LEARNING/DEEP LEARNING

Usually, all analyzed papers follow conventional machine learning standards, includes supervised and unsupervised learning. Around 4 papers inspected problems of regression, 3 papers are related to problems of clustering, and others are based on problems of classification. The directing usage of supervised learning reflects the value of using well-labeled data [21], [122], [123]. Particularly, network packets were labeled as usual or attack traffic, and the kinds of attacks were distinguished. This dependence on labeled data is limited to the broader acceptance of machine learning or deep learning methods. We suggest that the researchers and authors use new machine learning/deep learning paradigms [124]. It includes reinforcement and self-supervised learning to improve the explainability of the model. We suggest self-supervised learning flourishes in the cyber-physical system's domain as deep learning models suffer from deprived explainability. We are expectant about predicting that the deep learning models will be further reasonable when new tools and techniques are conceived and utilized [125].

D. PROTECTING THE TRAINED DEEP LEARNING MODELS

No survey papers are measured for defending the trained deep learning models, contrary to numerous attacks. In contrast, we highlight the significance of protecting the trained deep learning models due to the computational expenditures for introducing the deep learning models [126], [127]. The attackers can acquire adequate data to imitate a machine learning/deep learning model by generating many inquiries and conglomerating the outcomes. The removed data can be utilized to construct a mirroring model for the assailant to find conceivable avoidance assaults. We emphatically advocate that cyber defense be led quickly because of the ignorance of adversarial assaults in the cyber physical systems situations.

E. ADVANCING DATASETS OF CYBER PHYSICAL SYSTEMS CYBERSECURITY

Between the reviewed papers, datasets gathered in the area ruled the simulation with a proportion of 14:6. Simulated information was explored in the 2 cyber physical systems situations – shrewd matrices and vehicular organizations [128]. Five papers utilizing field information picked the Smack dataset, two reports the CICIDS2017 dataset, and the other diverse datasets [129], [130], [131].

Additionally, new datasets will constantly be essential and appreciated. In a perfect world, the new datasets are publicly released field information gathered from physical testbeds. A few cyber physical system testbeds are proposed to work with recognizing cyber assaults [24].The new pattern of expanding interest in building cyber physical system testbeds may help specialists to gather superior-grade assault and defense information [132], [133]. The new datasets are enormous enough to take advantage of deep learning models' power, and both new and old cyber assaults should be incorporated because cyber assaults advance rapidly. If naming information is tested, sequentially isolating the assaults from the typical traffic is a practical thought. Falsely mixing the information passages addressing assaults into a bunch of ordinary traffic records should be kept away from because the basic information increase strategy doesn't consider practicality, going after groupings, and potential connections changes. To help the headway of exploration and information, we emphatically energize more high-quality datasets increasingly to be made accessible to the local area [134], [135].

F. IMPROVISING THE EVALUATION OF MODELS

Standard execution measurements were utilized in the vast majority of the reviewed papers. Misleading up-sides were examined, precision and fault rate. This is demonstrated by authors [65] that it is fundamentally further hard to distinguish the seldom-happened assaults than the normal ones determined by the Bayesian regulations [136], [137].

Moreover, time is essential in ongoing investigations since each prepared machine learning or deep learning model's presentation will unavoidably corrupt over the long run. When the cyber develops quickly, the models prepared with old information will battle with identifying new assaults. A period rot metric was proposed in to assess a prepared model's presentation misfortune. By concentrating on the time rot, we will want to choose when the model should be retrained. We want to see future work like about cyber physical systems and cyber assaults. When top-to-bottom information is created and acquired, we might hope to relieve the risk of cyber-physical systems' cyber assaults.

VII. CONCLUSION

This review gives an ongoing perspective on recognizing cyber-attacks in the cyber physical systems.In particular, an inclusive perception is obtained through analyzing the cyber-physical systems situations, recognizing cybersecurity issues, interpreting the exploration issue to the machine learning/deep learning space, developing the deep learning model, planning datasets, and lastly, assessing the model. The Cyber attacks endure as a constant and conspicuous danger to the safety and betterment of cyber-physical systems. The work shows extraordinary potential to take advantage of cyber physical system's cyber information through deep learning models as a result of their promising demonstrations. We distinguished favorable examination issues, incorporating blockchain, identifying cutting-edge, steady dangers, taking on new machine learning and deep learning standards, avoiding adversarial and attacks of model extraction, enhancing datasets, and utilizing different execution measurements. We are hopeful and sure that the examination in this field will thrive.

REFERENCES

[1] N. Falliere, L. O. Murchu, and E. Chien, "W32. stuxnet dossier," Secur. Response, Symantec Corp., Cupertino, CA, USA, White Paper, Version 1.4, Feb. 2011, p. 29, vol. 5, no. 6.

[2] A. Humayed and B. Luo, "Cyber-physical security for smart cars: Taxonomy of vulnerabilities, threats, and attacks," in *Proc. ACM/IEEE 6th Int. Conf. Cyber-Phys. Syst.*, Seattle, WA, USA, Apr. 2015, pp. 252–253.

[3] J. Slay and M. Miller, "Lessons learned from the maroochy water breach," in *Proc. Int. Conf. Crit. Infrastruct. Protection*. Boston, MA, USA: Springer, 2007, pp. 73–82.

[4] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Secur. Privacy*, vol. 9, no. 3, pp. 49–51, May 2011.

[5] J. P. Farwell and R. Rohozinski, "Stuxnet and the future of cyber war," *Survival*, vol. 53, no. 1, pp. 23–40, Feb. 2011.

[6] C.-H. Lee, B.-K. Chen, N.-M. Chen, and C.-W. Liu, "Lessons learned from the blackout accident at a nuclear power plant in Taiwan," *IEEE Trans. Power Del.*, vol. 25, no. 4, pp. 2726–2733, Oct. 2010.

[7] J. P. Conti, "The day the samba stopped [power blackouts]," *Eng. Technol.*, vol. 5, no. 4, pp. 46–47, Mar. 2010.

[8] Y. Liu and S. Hu, "Cyberthreat analysis and detection for energy theft in social networking of smart homes," *IEEE Trans. Computat. Social Syst.*, vol. 2, no. 4, pp. 148–158, Dec. 2015.

[9] Y. Liu and S. Hu, "Smart home scheduling and cybersecurity: Fundamentals," in *Smart Cities and Homes*. Amsterdam, The Netherlands: Elsevier, 2016, pp. 191–217.

[10] J. Liang, L. Sankar, and O. Kosut, "Vulnerability analysis and consequences of false data injection attack on power system state estimation," *IEEE Trans. Power Syst.*, vol. 31, no. 5, pp. 3864–3872, Sep. 2016.

[11] S. Li, Y. Yilmaz, and X. Wang, "Quickest detection of false data injection attack in wide-area smart grids," *IEEE Trans. Smart Grid*, vol. 6, no. 6, pp. 2725–2735, Nov. 2015.

[12] D. B. Rawat and C. Bajracharya, "Detection of false data injection attacks in smart grid communication systems," *IEEE Signal Process. Lett.*, vol. 22, no. 10, pp. 1652–1656, Oct. 2015.

[13] R. Deng, G. Xiao, R. Lu, H. Liang, and A. V. Vasilakos, "False data injection on state estimation in power systems—Attacks, impacts, and defense: A survey," *IEEE Trans. Ind. Inform.*, vol. 13, no. 2, pp. 411–423, Sep. 2016.

[14] K. Paridari, N. O'Mahony, A. E.-D. Mady, R. Chabukswar, M. Boubekeur, and H. Sandberg, "A framework for attack-resilient industrial control systems: Attack detection and controller reconfiguration," *Proc. IEEE*, vol. 106, no. 1, pp. 113–128, Jan. 2018.

[15] A.-Y. Lu and G.-H. Yang, "Secure state estimation for cyber-physical systems under sparse sensor attacks via a switched Luenberger observer," *Inf. Sci.*, vol. 417, pp. 454–464, Nov. 2017.

[16] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Trans. Autom. Control*, vol. 58, no. 11, pp. 2715–2729, Nov. 2013.

[17] A. J. Gallo, M. S. Turan, P. Nahata, F. Boem, T. Parisini, and G. Ferrari-Trecate, "Distributed cyber-attack detection in the secondary control of DC microgrids," in *Proc. Eur. Control Conf. (ECC)*, Limassol, Cyprus, Jun. 2018, pp. 344–349.

[18] S. Altaf, A. Al-Anbuky, and H. GholamHosseini, "Fault diagnosis in a distributed motor network using artificial neural network," in *Proc. Int. Symp. Power Electron., Electr. Drives, Autom. Motion*, Ischia, Italy, Jun. 2014, pp. 190–197.

[19] B. M. Sanandaji, E. Bitar, K. Poolla, and T. L. Vincent, "An abrupt change detection heuristic with applications to cyber data attacks on power systems," in *Proc. Amer. Control Conf.*, Portland, OR, USA, Jun. 2014, pp. 5056–5061.

[20] M. Russo, M. Labonne, A. Olivereau, and M. Rmayti, "Anomaly detection in Vehicle-to-Infrastructure communications," in *Proc. IEEE 87th Veh. Technol. Conf. (VTC Spring)*, Porto, Portugal, Jun. 2018, pp. 1–6.

[21] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*. Cambridge, MA, USA: MIT Press, 2016.

[22] D. Xiong, D. Zhang, X. Zhao, and Y. Zhao, "Deep learning for EMG-based human-machine interaction: A review," *IEEE/CAA J. Autom. Sinica*, vol. 8, no. 3, pp. 512–533, Mar. 2021.

[23] L. Kuwatly, M. Sraj, Z. Al Masri, and H. Artail, "A dynamic honeypot design for intrusion detection," in *Proc. IEEE/ACS Int. Conf. Pervasive Services (ICPS)*, Beirut, Lebanon, Jul. 2004, pp. 95–104.

[24] R. Mitchell and I.-R. Chen, "A survey of intrusion detection techniques for cyber-physical systems," *ACM Comput. Surv.*, vol. 46, no. 4, pp. 1–29, Apr. 2014.

[25] C. S. Wickramasinghe, D. L. Marino, K. Amarasinghe, and M. Manic, "Generalization of deep learning for cyber-physical system security: A survey," in *Proc. 44th Annu. Conf. IEEE Ind. Electron. Soc. (IECON)*, Oct. 2018, pp. 745–751.

[26] S. Gaba, H. Khan, K. J. Almalki, A. Jabbari, I. Budhiraja, V. Kumar, A. Singh, K. K. Singh, S. S. Askar, and M. Abouhawwash, "Holochain: An agent-centric distributed hash table security in smart IoT applications," *IEEE Access*, vol. 11, pp. 81205–81223, 2023.

[27] A. Barnawi, S. Gaba, A. Alphy, A. Jabbari, I. Budhiraja, V. Kumar, and N. Kumar, "A systematic analysis of deep learning methods and potential attacks in Internet-of-things surfaces," *Neural Comput. Appl.*, vol. 35, no. 25, pp. 18293–18308, Sep. 2023.

[28] H. Sharma, N. Kumar, I. Budhiraja, and A. Barnawi, "Secrecy rate maximization in THz-aided heterogeneous networks: A deep reinforcement learning approach," *IEEE Trans. Veh. Technol.*, vol. 72, no. 10, pp. 13490–13505, Oct. 2023.

[29] V. Vishnoi, P. Consul, I. Budhiraja, S. Gupta, and N. Kumar, "Deep reinforcement learning based energy consumption minimization for intelligent reflecting surfaces assisted D2D users underlaying UAV network," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, May 2023, pp. 1–6.

[30] V. Vishnoi, I. Budhiraja, S. Ishan, and N. Kumar, "A deep reinforcement learning scheme for sum rate and fairness maximization among D2D pairs underlaying cellular network with NOMA," *IEEE Trans. Veh. Technol.*, vol. 72, no. 10, pp. 13506–13522, 2023, doi: 10.1109/TVT.2023.3276647.

[31] S. Singh, A. Bhardwaj, I. Budhiraja, U. Gupta, and I. Gupta, "Cloud-based architecture for effective surveillance and diagnosis of COVID-19," in *Convergence of Cloud With AI for Big Data Analytics: Foundations and Innovation*. Hoboken, NJ, USA: Wiley, 2023, pp. 69–88.

[32] L. Cheng, K. Tian, and D. Yao, "Orpheus: Enforcing cyber-physical execution semantics to defend against data-oriented attacks," in *Proc. 33rd Annu. Comput. Secur. Appl. Conf.*, Orlando, FL, USA, Dec. 2017, pp. 315–326.

[33] R. Chalapathy and S. Chawla, "Deep learning for anomaly detection: A survey," 2019, *arXiv:1901.03407*.

[34] R. Heartfield, G. Loukas, S. Budimir, A. Bezemskij, J. R. J. Fontaine, A. Filippoupolitis, and E. Roesch, "A taxonomy of cyber-physical threats and impact in the smart home," *Comput. Secur.*, vol. 78, pp. 398–428, Sep. 2018.

[35] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," *ACM Comput. Surv.*, vol. 41, no. 3, pp. 1–58, 2009.

[36] J. Giraldo, D. Urbina, A. Cardenas, J. Valente, M. Faisal, J. Ruths, N. O. Tippenhauer, H. Sandberg, and R. Candell, "A survey of physics-based attack detection in cyber-physical systems," *ACM Comput. Surv.*, vol. 51, no. 4, pp. 1–36, Jul. 2019.

[37] P. Schneider and K. Böttinger, "High-performance unsupervised anomaly detection for cyber-physical system networks," in *Proc. Workshop Cyber-Phys. Syst. Secur. PrivaCy*, Jan. 2018, pp. 1–12.

[38] M. Mohammadi, A. Al-Fuqaha, S. Sorour, and M. Guizani, "Deep learning for IoT big data and streaming analytics: A survey," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 2923–2960, 4th Quart., 2018.

[39] E. M. Veith, L. Fischer, M. Tröschel, and A. Nieße, "Analyzing cyber-physical systems from the perspective of artificial intelligence," in *Proc. Int. Conf. Artif. Intell., Robot. Control*, Dec. 2019, pp. 85–95.

[40] Y. Luo, Y. Xiao, L. Cheng, G. Peng, and D. Yao, "Deep learning-based anomaly detection in cyber-physical systems: Progress and opportunities," *ACM Comput. Surv.*, vol. 54, no. 5, pp. 1–36, Jun. 2022.

[41] R. Mitchell and I.-R. Chen, "A survey of intrusion detection techniques for cyber-physical systems," *ACM Comput. Surveys*, vol. 46, no. 4, pp. 1–29, Apr. 2014.

[42] S. Nazir, S. Patel, and D. Patel, "Assessing and augmenting SCADA cyber security: A survey of techniques," *Comput. Secur.*, vol. 70, pp. 436–454, Sep. 2017.

[43] B. Siciliano, A. G. Scaglione, and L. Galluccio, "A survey of cyber-physical attacks and defenses in the smart grid," *IEEE Trans. Ind. Informat.*, vol. 16, no. 5, pp. 3231–3240, Jun. 2020.

[44] I. Ndiaye, J. G. Nijlla, and I. Balogun, "A survey of intrusion detection in Internet of Things," *IEEE Access*, vol. 9, pp. 73900–73917, 2021.

[45] L. Yu, H. Wu, Z. Liu, Y. Li, and W. Zhao, "A review of machine learning methods in cybersecurity," *IEEE Access*, vol. 8, pp. 135695–135718, 2020.
[46] J. Zhang, L. Pan, Q.-L. Han, C. Chen, S. Wen, and Y. Xiang, "Deep learning based attack detection for cyber-physical system cybersecurity: A survey," *IEEE/CAA J. Autom. Sinica*, vol. 9, no. 3, pp. 377–391, Mar. 2022.
[47] A. A. Jamal, A.-A. M. Majid, A. Konev, T. Kosachenko, and A. Shelupanov, "A review on security analysis of cyber physical systems using machine learning," *Mater. Today*, vol. 80, pp. 2302–2306, Jan. 2023.
[48] F. O. Olowononi, D. B. Rawat, and C. Liu, "Resilient machine learning for networked cyber physical systems: A survey for machine learning security to securing machine learning for CPS," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 1, pp. 524–552, 1st Quart., 2021.
[49] Y. Luo, Y. Xiao, L. Cheng, G. Peng, and D. Yao, "Deep learning-based anomaly detection in cyber-physical systems: Progress and opportunities," *ACM Comput. Surv.*, vol. 54, no. 5, pp. 1–36, Jun. 2022.
[50] B. Li, Y. Wu, J. Song, R. Lu, T. Li, and L. Zhao, "DeepFed: Federated deep learning for intrusion detection in industrial cyber–physical systems," *IEEE Trans. Ind. Informat.*, vol. 17, no. 8, pp. 5615–5624, Aug. 2021.
[51] A. Presekal, A. Ştefanov, V. S. Rajkumar, and P. Palensky, "Attack graph model for cyber-physical power systems using hybrid deep learning," *IEEE Trans. Smart Grid*, vol. 14, no. 5, pp. 4007–4020, 2023, doi: 10.1109/TSG.2023.3237011.
[52] F. Darbandi, A. Jafari, H. Karimipour, A. Dehghantanha, F. Derakhshan, and K. Raymond Choo, "Real-time stability assessment in smart cyber-physical grids: A deep learning approach," *IET Smart Grid*, vol. 3, no. 4, pp. 454–461, Aug. 2020.
[53] S. Rathore and J. H. Park, "A blockchain-based deep learning approach for cyber security in next generation industrial cyber-physical systems," *IEEE Trans. Ind. Informat.*, vol. 17, no. 8, pp. 5522–5532, Aug. 2021.
[54] B. Hussain, Q. Du, B. Sun, and Z. Han, "Deep learning-based DDoS-attack detection for cyber–physical system over 5G network," *IEEE Trans. Ind. Informat.*, vol. 17, no. 2, pp. 860–870, Feb. 2021.
[55] A. M. Aslam, R. Chaudhary, A. Bhardwaj, I. Budhiraja, N. Kumar, and S. Zeadally, "Metaverse for 6G and beyond: The next revolution and deployment challenges," *IEEE Internet Things Mag.*, vol. 6, no. 1, pp. 32–39, Mar. 2023.
[56] M. Gupta, B. Gupta, A. Jabbari, I. Budhiraja, D. Garg, K. Kotecha, and C. Iwendi, "A novel computer assisted genomic test method to detect breast cancer in reduced cost and time using ensemble technique," *Human-Centric Comput. Inf. Sci.*, vol. 13, no. 18, pp. 1–16, Feb. 2023, doi: 10.22967/HCIS.2023.13.008.
[57] A. Bhardwaj, I. Budhiraja, and U. Gupta, *Cloud-Based Architecture for Effective Surveillance and Diagnosis of COVID-19*. Hoboken, NJ, USA: Wiley, 2023.
[58] A. Bhardwaj, U. Gupta, I. Budhiraja, and R. Chaudhary, "Container-based migration technique for fog computing architecture," in *Proc. Int. Conf. Adv. Technol. (ICONAT)*, Jan. 2023, pp. 1–6.
[59] M. Kravchik and A. Shabtai, "Detecting cyber attacks in industrial control systems using convolutional neural networks," in *Proc. Workshop Cyber-Phys. Syst. Secur. PrivaCy*, Jan. 2018, pp. 72–83.
[60] Z. Zohrevand, U. Glässer, M. A. Tayebi, H. Y. Shahir, M. Shirmaleki, and A. Y. Shahir, "Deep learning based forecasting of critical infrastructure data," in *Proc. ACM Conf. Inf. Knowl. Manage.*, Singapore, Nov. 2017, pp. 1129–1138.
[61] Y. Su, Y. Zhao, C. Niu, R. Liu, W. Sun, and D. Pei, "Robust anomaly detection for multivariate time series through stochastic recurrent neural network," in *Proc. 25th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, New York, NY, USA, Jul. 2019, pp. 2828–2837.
[62] B. Eiteneuer, N. Hranisavljevic, and O. Niggemann, "Dimensionality reduction and anomaly detection for CPPS data using autoencoder," in *Proc. IEEE Int. Conf. Ind. Technol. (ICIT)*, Melbourne, VIC, Australia, Feb. 2019, pp. 1286–1292.
[63] J. Goh, S. Adepu, M. Tan, and Z. S. Lee, "Anomaly detection in cyber physical systems using recurrent neural networks," in *Proc. IEEE 18th Int. Symp. High Assurance Syst. Eng. (HASE)*, Singapore, Jan. 2017, pp. 140–145.
[64] C. Feng, T. Li, and D. Chana, "Multi-level anomaly detection in industrial control systems via package signatures and LSTM networks," in *Proc. 47th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw. (DSN)*, Singapore, Jun. 2017, pp. 261–272.
[65] J. Inoue, Y. Yamagata, Y. Chen, C. M. Poskitt, and J. Sun, "Anomaly detection for a water treatment system using unsupervised machine learning," in *Proc. IEEE Int. Conf. Data Mining Workshops (ICDMW)*, New Orleans, LA, USA, Nov. 2017, pp. 1058–1065.
[66] P. Ferrari, S. Rinaldi, E. Sisinni, F. Colombo, F. Ghelfi, D. Maffei, and M. Malara, "Performance evaluation of full-cloud and edge-cloud architectures for industrial IoT anomaly detection based on deep learning," in *Proc. II Workshop Metrol. Ind. IoT (MetroInd&IoT)*, Jun. 2019, pp. 420–425.
[67] A. Legrand, B. Niepceron, A. Cournier, and H. Trannois, "Study of autoencoder neural networks for anomaly detection in connected buildings," in *Proc. IEEE Global Conf. Internet Things (GCIoT)*, Naples, Italy, Dec. 2018, pp. 1–5.
[68] Z. Wu, Y. Guo, W. Lin, S. Yu, and Y. Ji, "A weighted deep representation learning model for imbalanced fault diagnosis in cyber-physical systems," *Sensors*, vol. 18, no. 4, p. 1096, Apr. 2018.
[69] Z. Li, J. Li, Y. Wang, and K. Wang, "A deep learning approach for anomaly detection based on SAE and LSTM in mechanical equipment," *Int. J. Adv. Manuf. Technol.*, vol. 103, nos. 1–4, pp. 499–510, Jul. 2019.
[70] B. Lindemann, F. Fesenmayr, N. Jazdi, and M. Weyrich, "Anomaly detection in discrete manufacturing using self-learning approaches," *Proc. CIRP*, vol. 79, pp. 313–318, Jan. 2019.
[71] M. Canizo, I. Triguero, A. Conde, and E. Onieva, "Multi-head CNN–RNN for multi-time series anomaly detection: An industrial case study," *Neurocomputing*, vol. 363, pp. 246–260, Oct. 2019.
[72] H. A. Khan, N. Sehatbakhsh, L. N. Nguyen, M. Prvulovic, and A. Zajić, "Malware detection in embedded systems using neural network model for electromagnetic side-channel signals," *J. Hardw. Syst. Secur.*, vol. 3, no. 4, pp. 305–318, Dec. 2019.
[73] Y.-J. Xiao, W.-Y. Xu, Z.-H. Jia, Z.-R. Ma, and D.-L. Qi, "NIPAD: A non-invasive power-based anomaly detection scheme for programmable logic controllers," *Frontiers Inf. Technol. Electron. Eng.*, vol. 18, no. 4, pp. 519–534, Apr. 2017.
[74] D. Li, D. Chen, B. Jin, L. Shi, J. Goh, and S.-K. Ng, "Mad-GAN: Multivariate anomaly detection for time series data with generative adversarial networks," in *Proc. Int. Conf. Artif. Neural Netw.*, Springer, 2019, pp. 703–716.
[75] N. L. Tasfi, W. A. Higashino, K. Grolinger, and M. A. M. Capretz, "Deep neural networks with confidence sampling for electrical anomaly detection," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, Jun. 2017, pp. 1038–1045.
[76] Y. Zhang, V. V. G. Krishnan, J. Pi, K. Kaur, A. Srivastava, A. Hahn, and S. Suresh, "Cyber physical security analytics for transactive energy systems," *IEEE Trans. Smart Grid*, vol. 11, no. 2, pp. 931–941, Mar. 2020.
[77] J. Wang, D. Shi, Y. Li, J. Chen, H. Ding, and X. Duan, "Distributed framework for detecting PMU data manipulation attacks with deep autoencoders," *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 4401–4410, Jul. 2019.
[78] Q. Deng and J. Sun, "False data injection attack detection in a power grid using RNN," in *Proc. 44th Annu. Conf. IEEE Ind. Electron. Soc. (IECON)*, Washington, DC, USA, Oct. 2018, pp. 5983–5988.
[79] X. Niu, J. Li, J. Sun, and K. Tomsovic, "Dynamic detection of false data injection attack in smart grid using deep learning," in *Proc. IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. (ISGT)*, Washington, DC, USA, Feb. 2019, pp. 1–6.
[80] H. Wang, J. Ruan, Z. Ma, B. Zhou, X. Fu, and G. Cao, "Deep learning aided interval state prediction for improving cyber security in energy Internet," *Energy*, vol. 174, pp. 1292–1304, May 2019.
[81] S. Basumallik, R. Ma, and S. Eftekharnejad, "Packet-data anomaly detection in PMU-based state estimator using convolutional neural network," *Int. J. Electr. Power Energy Syst.*, vol. 107, pp. 690–702, May 2019.
[82] C. Fan, F. Xiao, Y. Zhao, and J. Wang, "Analytical investigation of autoencoder-based methods for unsupervised anomaly detection in building energy data," *Appl. Energy*, vol. 211, pp. 1123–1135, Feb. 2018.
[83] Y. Wang, D. Chen, C. Zhang, X. Chen, B. Huang, and X. Cheng, "Wide and recurrent neural networks for detection of false data injection in smart grids," in *Proc. 14th Int. Conf., Wireless Algorithms, Syst., Appl. (WASA)*. Honolulu, HI, USA: Springer, 2019, pp. 335–345.

[84] E. Khanapuri, T. Chintalapati, R. Sharma, and R. Gerdes, "Learning-based adversarial agent detection and identification in cyber physical systems applied to autonomous vehicular platoon," in *Proc. IEEE/ACM 5th Int. Workshop Softw. Eng. Smart Cyber-Phys. Syst. (SEsCPS)*, Montreal, QC, Canada, May 2019, pp. 39–45.

[85] F. van Wyk, Y. Wang, A. Khojandi, and N. Masoud, "Real-time sensor anomaly detection and identification in automated vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 21, no. 3, pp. 1264–1276, Mar. 2020.

[86] A. Taylor, S. Leblanc, and N. Japkowicz, "Anomaly detection in automobile control network data with long short-term memory networks," in *Proc. IEEE Int. Conf. Data Sci. Adv. Anal. (DSAA)*, Montreal, QC, Canada, Oct. 2016, pp. 130–139.

[87] T. Kieu, B. Yang, and C. S. Jensen, "Outlier detection for multidimensional time series using deep neural networks," in *Proc. 19th IEEE Int. Conf. Mobile Data Manage. (MDM)*, Aalborg, Denmark, Jun. 2018, pp. 125–134.

[88] K. Zhu, Z. Chen, Y. Peng, and L. Zhang, "Mobile edge assisted literal multi-dimensional anomaly detection of in-vehicle network using LSTM," *IEEE Trans. Veh. Technol.*, vol. 68, no. 5, pp. 4275–4284, May 2019.

[89] C. Jichici, B. Groza, and P.-S. Murvay, "Examining the use of neural networks for intrusion detection in controller area networks," in *Proc. Int. Conf. Secur. Inf. Technol. Commun.*, Springer, 2018, pp. 109–125.

[90] K. Hundman, V. Constantinou, C. Laporte, I. Colwell, and T. Soderstrom, "Detecting spacecraft anomalies using LSTMs and nonparametric dynamic thresholding," in *Proc. 24th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, London, U.K., Jul. 2018, pp. 387–395.

[91] S. Tariq, S. Lee, Y. Shin, M. S. Lee, O. Jung, D. Chung, and S. S. Woo, "Detecting anomalies in space using multivariate convolutional LSTM with mixtures of probabilistic PCA," in *Proc. 25th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, Anchorage, AK, USA, Jul. 2019, pp. 2123–2133.

[92] O. M. Ezeme, Q. H. Mahmoud, and A. Azim, "DReAM: Deep recursive attentive model for anomaly detection in kernel events," *IEEE Access*, vol. 7, pp. 18860–18870, 2019.

[93] L. Gunn, P. Smet, E. Arbon, and M. D. McDonnell, "Anomaly detection in satellite communications systems using LSTM networks," in *Proc. Mil. Commun. Inf. Syst. Conf. (MilCIS)*, Canberra, ACT, Australia, Nov. 2018, pp. 1–6.

[94] A. Nanduri and L. Sherry, "Anomaly detection in aircraft data using recurrent neural networks (RNN)," in *Proc. Integr. Commun. Navigat. Surveill. (ICNS)*, Herndon, VA, USA, Apr. 2016, p. 5C2-1.

[95] E. Habler and A. Shabtai, "Using LSTM encoder-decoder algorithm for detecting anomalous ADS-B messages," *Comput. Secur.*, vol. 78, pp. 155–173, Sep. 2018.

[96] O. M. Ezeme, M. Lescisin, Q. H. Mahmoud, and A. Azim, "DeepAnom: An ensemble deep framework for anomaly detection in system processes," in *Proc. 32nd Can. Conf. Artif. Intell., Adv. Artif. Intell. (Canadian AI)*. Kingston, ON, Canada: Springer, May 2019, pp. 549–555.

[97] V. L. Do, L. Fillatre, I. Nikiforov, and P. Willett, "Security of SCADA systems against cyber–physical attacks," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 32, no. 5, pp. 28–45, May 2017.

[98] K. Poulsen, "Slammer worm crashed Ohio nuke plant network," *Secur. Focus*, vol. 19, 2003.

[99] J. D. Rogers and C. M. Watkins, "Overview of the Taum Sauk pumped storage power plant upper reservoir failure, Reynolds County, MO," in *Proc. 6th Int. Conf. Case Histories Geotechnical Eng.*, Arlington, VA, USA, 2008, pp. 1–13.

[100] T. FoxBrewster, "Ukraine claims hackers caused Christmas power outage," *Forbes Secur.*, 2016.

[101] S. Gorman, "Electricity grid in us penetrated by spies," *Wall Street J.*, vol. 8, no. 8, 2009.

[102] M. J. Credeur, "FBI probes Georgia water plant break-in on terror concern," Bloomberg, 2013.

[103] J. Slay and M. Miller, *Lessons Learned From the Maroochy Water Breach*. Boston, MA, USA: Springer, 2008.

[104] F. Y. Rashid. (2012). *Telvent Hit by Sophisticated Cyber-Attack, SCADA Admin Tool Compromised*. [Online]. Available: http://www.securityweek.com/telvent-hit-sophisticated-cyber-attack-scada-admin-tool-compromised

[105] M. A. Almaiah, F. Hajjej, A. Ali, M. F. Pasha, and O. Almomani, "A novel hybrid trustworthy decentralized authentication and data preservation model for digital healthcare IoT based CPS," *Sensors*, vol. 22, no. 4, p. 1448, Feb. 2022.

[106] R. F. Mansour, "Artificial intelligence based optimization with deep learning model for blockchain enabled intrusion detection in CPS environment," *Sci. Rep.*, vol. 12, no. 1, p. 12937, Jul. 2022.

[107] Z. A. Sheikh, Y. Singh, P. K. Singh, and K. Z. Ghafoor, "Intelligent and secure framework for critical infrastructure (CPS): Current trends, challenges, and future scope," *Comput. Commun.*, vol. 193, pp. 302–331, Sep. 2022.

[108] D. M. Sharma and S. K. Shandilya, "Attack detection based on machine learning techniques to safe and secure for CPS—A review," in *Proc. Int. Conf. IoT, Intell. Comput. Secur., Select (IICS)*, pp. 273–286, Springer, 2023.

[109] A. Albasir, K. Naik, and R. Manzano, "Toward improving the security of IoT and CPS devices: An AI approach," *Digit. Threats: Res. Pract.*, vol. 4, no. 2, pp. 1–30, Jun. 2023.

[110] G. Epiphaniou, M. Hammoudeh, H. Yuan, C. Maple, and U. Ani, "Digital twins in cyber effects modelling of IoT/CPS points of low resilience," *Simul. Model. Pract. Theory*, vol. 125, May 2023, Art. no. 102744.

[111] A. Albasir, K. Naik, and R. Manzano, "Toward improving the security of IoT and CPS devices: An AI approach," *Digit. Threats, Res. Pract.*, vol. 4, no. 2, pp. 1–30, Jun. 2023.

[112] A. Aggarwal, S. Gaba, S. Nagpal, and A. Arya, "A comparative analysis among task scheduling for grouped and ungrouped grid application," in *Proc. CEUR Workshop, Int. Conf. Emerg. Technol., AI, IoT, CPS Sci. Technol. Appl.* Chandigarh, India: NITTTR, Sep. 2021, pp. 1–5.

[113] A. Aggarwal, S. Gaba, S. Nagpal, and B. Vig, "Bio-inspired routing in VANET," in *Cloud and IoT-Based Vehicular Ad Hoc Networks*, 2021, pp. 199–220.

[114] D. Aggarwal and S. Gaba, "A comparative study: Reviewing performance of routing protocols in mobile ad-hoc network," *Vol*, vol. 4, no. 8, pp. 528–532, Jun. 2018.

[115] I. Budhiraja et al., "A comprehensive review on variants of SARS-CoVs-2: Challenges, solutions and open issues," *Comput. Commun.*, vol. 197, pp. 34–51, 2023.

[116] H. Khan, I. Budhiraja, S. A. Wahaj, M. Z. Alam, S. T. Siddiqui, and M. I. Alam, "IoT and blockchain integration challenges," in *Proc. IEEE Int. Conf. Current Develop. Eng. Technol. (CCET)*, Dec. 2022, pp. 1–5.

[117] P. Rani, V. Kumar, I. Budhiraja, A. Rathi, and S. Kukreja, "Deploying electronic voting system use-case on Ethereum public blockchain," in *Proc. IEEE Int. Conf. Adv. Netw. Telecommun. Syst. (ANTS)*, Dec. 2022, pp. 1–6.

[118] P. Consul, I. Budhiraja, R. Chaudhary, and D. Garg, "FLBCPS: Federated learning based secured computation offloading in blockchain-assisted cyber-physical systems," in *Proc. IEEE/ACM 15th Int. Conf. Utility Cloud Comput. (UCC)*, Dec. 2022, pp. 412–417.

[119] R. Nijhawan, M. Juneja, N. Kaur, A. Yadav, and I. Budhiraja, "Automated deep learning based approach for albinism detection," in *Proc. Int. Conf. Recent Trends Image Process. Pattern Recognit.* Kingsvilla, TX, USA: Springer, 2022, pp. 272–281.

[120] A. Aggarwal, S. Gaba, S. Chawla, and A. Arya, "Recognition of alphanumeric patterns using backpropagation algorithm for design and implementation with ANN," *Int. J. Secur. Privacy Pervasive Comput.*, vol. 14, no. 1, pp. 1–11, Feb. 2022.

[121] S. Gaba, A. Aggarwal, and S. Nagpal, "Role of machine learning for ad hoc networks," in *Cloud and IoT-Based Vehicular Ad Hoc Networks*. Hoboken, NJ, USA: Wiley, 2021, pp. 269–291.

[122] A. Aggarwal, S. Gaba, J. Kumar, and S. Nagpal, "Blockchain and autonomous vehicles: Architecture, security and challenges," in *Proc. 5th Int. Conf. Comput. Intell. Commun. Technol. (CCICT)*, Jul. 2022, pp. 332–338.

[123] S. Gaba, S. Nagpal, and A. Aggarwal, "A comparative study of convolutional neural networks for plant phenology recognition," in *Advanced Sensing in Image Processing and IoT*. Boca Raton, FL, USA: CRC Press, 2022, pp. 109–136.

[124] A. Barnawi, I. Budhiraja, K. Kumar, N. Kumar, B. Alzahrani, A. Almansour, and A. Noor, "A comprehensive review on landmine detection using deep learning techniques in 5G environment: Open issues and challenges," *Neural Comput. Appl.*, vol. 34, no. 24, pp. 21657–21676, Dec. 2022.

[125] S. Gaba, D. Kumar, S. Nagpal, and A. Aggarwal, "A quick analysis on cyber physical systems for sustainable development," *Grenze Int. J. Eng. Technol.*, vol. 8, no. 1, pp. 621–627, 2022.

[126] P. Consul, I. Budhiraja, R. Chaudhary, and N. Kumar, "Security reassessing in UAV-assisted cyber-physical systems based on federated learning," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Nov. 2022, pp. 61–65.
[127] A. Verma, P. Bhattacharya, I. Budhiraja, A. K. Gupta, and S. Tanwar, "Fusion of federated learning and 6G in internet-of-medical-things: Architecture, case study and emerging directions," in *Proc. 4th Int. Conf. Futuristic Trends Netw. Comput. Technol.* Ahmedabad, India: Springer, Jul. 2022, pp. 229–242.
[128] P. Arpaia, C. Manna, and G. Montenero, "Ant-search strategy based on likelihood trail intensity modification for multiple-fault diagnosis in sensor networks," *IEEE Sensors J.*, vol. 13, no. 1, pp. 148–158, Jan. 2013.
[129] I. Budhiraja, N. Kumar, H. Sharma, M. Elhoseny, Y. Lakys, and J. J. P. C. Rodrigues, "Latency-energy tradeoff in connected autonomous vehicles: A deep reinforcement learning scheme," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 11, pp. 13296–13308, 2023, doi: 10.1109/TITS.2022.3215523.
[130] A. Barnawi, N. Kumar, I. Budhiraja, K. Kumar, A. Almansour, and B. Alzahrani, "Deep reinforcement learning based trajectory optimization for magnetometer-mounted UAV to landmine detection," *Comput. Commun.*, vol. 195, pp. 441–450, Nov. 2022.
[131] Deepanshi, I. Budhiraja, D. Garg, N. Kumar, and R. Sharma, "A comprehensive review on variants of SARS-CoVs-2: Challenges, solutions and open issues," *Comput. Commun.*, vol. 197, pp. 34–51, Jan. 2023.
[132] S. Gaba, S. Nagpal, A. Aggarwal, S. Kumar, and P. Singh, "A modified approach for accuracy enhancement in intruder detection with optimally certain features," in *Proc. 3rd Mobile Radio Commun. 5G Netw. (MRCN)*. Kurukshetra, India: Springer, 2023, pp. 149–157.
[133] S. Gaba, I. Buddhiraja, V. Kumar, and A. Makkar, "Federated learning based secured computational offloading in cyber-physical IoST systems," in *Proc. Int. Conf. Recent Trends Image Process. Pattern Recognit.* Kingsvilla, TX, USA: Springer, 2022, pp. 344–355.
[134] S. Gaba, S. Nagpal, A. Aggarwal, R. Kumar, and S. Kumar, "An analysis of Internet of Things (IoT) malwares and detection based on static and dynamic techniques," in *Proc. 7th Int. Conf. Parallel, Distrib. Grid Comput. (PDGC)*, Nov. 2022, pp. 24–29.
[135] P. Singh, G. Bathla, D. Panwar, A. Aggarwal, and S. Gaba, "Performance evaluation of genetic algorithm and flower pollination algorithm for scheduling tasks in cloud computing," in *Proc. Int. Conf. Signal Process. Integr. Netw.* Noida, India: Springer, 2022, pp. 139–154.
[136] H. Sharma, I. Budhiraja, P. Consul, N. Kumar, D. Garg, L. Zhao, and L. Liu, "Federated learning based energy efficient scheme for MEC with NOMA underlaying UAV," in *Proc. 5th Int. ACM Mobicom Workshop Drone Assist. Wireless Commun. 5G Beyond*, Oct. 2022, pp. 73–78.
[137] P. Consul, I. Budhiraja, D. Garg, and A. Bindle, "Power allocation scheme based on DRL for CF massive MIMO network with UAV," in *Proc. Innov. Inf. Commun. Technol. (ICIICT)*. Thailand: Springer, 2022, pp. 33–43.

SHIVANI GABA received the B.Tech. and M.Tech. degrees from Kurukshetra University, in 2015 and 2017, respectively. She is currently an Educator, a Researcher, and a Philanthropist. She is also a Microsoft Technology Associate (MTA) and a Microsoft Office Specialist (MOS) Certified. She is also a Research Scholar with the School of Computer Science and Engineering, Bennett University, Greater Noida. She has presented and published abundant papers and chapters in national/international conferences and journals. Her research interests include AI, blockchain, deep learning, and cyber-attacks.

ISHAN BUDHIRAJA (Member, IEEE) received the B.Tech. degree in electronics and communication engineering from Uttar Pradesh Technical University, Lucknow, India, in 2008, the M.Tech. degree in electronics and communication engineering from Maharishi Dayanand University, Rohtak, Haryana, in 2012, and the Ph.D. degree in computer science engineering from the Thapar Institute of Engineering & Technology, Patiala, India, in 2021. He was a Research Associate on the Project Energy Management of Smart Home Using Cloud Infrastructure-A Utility Perspective, funded by CSIR, New Delhi, India. Some of his research findings are published in top-cited journals, such as IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, IEEE TRANSACTIONS ON MOBILE COMPUTING, IEEE INTERNET OF THINGS JOURNAL, *IEEE Wireless Communication Magazine*, and IEEE SYSTEMS JOURNAL, and various international top-tiered conferences, such as IEEE GLOBECOM, IEEE ICC, IEEE WCMC, ACM, and IEEE Infocom. His research interests include device-to-device communications, the Internet of Things, non-orthogonal multiple access, femtocells, deep reinforcement learning, and microstrip patch antenna.

VIMAL KUMAR (Member, IEEE) received the M.Tech. and Ph.D. degrees from MNNIT Allahabad, Prayagraj, Uttar Pradesh, India. He is currently an Assistant Professor in SCSET with Bennett University (Times of India Group), Greater Noida. He has more than 17 years of teaching and research experience. His past research work is more focused on multipath mobile computing in heterogeneous networks for multi-interface enabled smart mobile devices to improve the QoE of end users. He has published 17 research papers in various reputed SCI/Scopus/WoS/ESCI indexed journals and conferences and his papers are awarded best papers in conferences. He is currently passionate about innovations in blockchain use cases and use of IoT devices in various domains. He is also a member of Internet Society.

SHESHIKALA MARTHA (Member, IEEE) received the Ph.D. degree from K. L. University. She has been a Professor and the Head of SR University, since 2012, and having total experience of more than 18 years. She has published more than 50 publications in reputed research journals. Her research interests include data mining, machine learning, deep learning, and cyber-physical systems.

JEBREEL KHURMI received the B.S. degree in Computer Engineering and Networking from Jazan University, Jazan, Kingdom of Saudi Arabia, the M.S. degree in Computer Science Networks and Telecommunications from University of Missouri–Kansas City, MO, USA. Currently, he is a Lecturer with Jazan College of Technology, Saudi Arabia. His research interests are the IoT, Smart Applications, and Sensors Enhancements.

AKANSHA SINGH (Member, IEEE) received the B.Tech. and M.Tech. degrees in computer science and the Ph.D. degree in image processing and machine learning from IIT Roorkee. She is also a Professor with the School of Computer Science and Engineering, Bennett University, Greater Noida, India. She has also undertaken government funded project as a principal investigator. Her research interests include image processing, remote sensing, the IoT, and machine learning. She has served as an associate editor and a guest editor for several journals.

KRISHNA KANT SINGH received the B.Tech., M.Tech., M.S., and Ph.D. degrees in image processing and machine learning from IIT Roorkee. He is currently working as the Director with Delhi Technical Campus, Greater Noida, UP, India. He has wide teaching and research experience. He has authored more than 116 research articles in Scopus and SCIE indexed journals of repute. He has also authored 25 technical books. He is an Associate Editor of *Journal of Intelligent and Fuzzy Systems* (SCIE Indexed) and IEEE Access (SCIE Indexed) and a Guest Editor of *Open Computer Science* and *Wireless Personal Communications*. He is serving as a member of Editorial Board for *Applied Computing and Geoscience* (Elsevier).

S. S. ASKAR received the B.Sc. degree in mathematics and the M.Sc. degree in applied mathematics from Mansoura University, Egypt, in 1998 and 2004, respectively, and the Ph.D. degree in operation research from Cranfield University, U.K., in 2011. He has been an Associate Professor with Mansoura University, since 2016. He has joined King Saud University, in 2012, where he is currently a Professor with the Department of Statistics and Operation Research. His main research interests include game theory and its applications that include mathematical economy, dynamical systems, and network analysis.

MOHAMED ABOUHAWWASH received the B.Sc. and M.Sc. degrees in statistics and computer science from Mansoura University, Mansoura, Egypt, in 2005 and 2011, respectively, and the joint Ph.D. degree in statistics and computer science from Michigan State University, East Lansing, MI, USA, and Mansoura University, Egypt, in 2015. Currently, he holds significant academic positions at Distinguished Institutions, including Computational Mathematics, Science, and Engineering (CMSE), Biomedical Engineering (BME), and Radiology, Institute for Quantitative Health Science and Engineering (IQ), Michigan State University. Additionally, he serves as an Associate Professor at the Department of Mathematics, Faculty of Science, Mansoura University. During 2018, he dedicated to advancing knowledge transcends geographical boundaries, as evidenced by his role as a Visiting Scholar at the Department of Mathematics and Statistics, Faculty of Science, Thompson Rivers University, Kamloops, BC, Canada. He is a Distinguished Researcher and an Academician, widely recognized for his outstanding contributions to the fields of computational intelligence, machine learning, and image reconstruction. With an illustrious career, he has published over 160 papers in esteemed journals, including notable publications like IEEE Transactions on Evolutionary Computation, IEEE Transactions on Medical Imaging, IEEE Transactions on Emerging Topics in Computational Intelligence, Artificial Intelligence Review, Expert Systems with Applications, Swarm and Evolutionary Computation, Knowledge-Based Systems, and Applied Soft Computing. In addition to his prolific research output, he has showcased his expertise by authoring several edited books published by reputable academic publishers such as *Springer, Wiley, Taylor, and Francis*. His impact on the academic community is further amplified through his editorial board service in numerous prestigious journals and conferences. Throughout his illustrious career, he has received recognition for his academic excellence, notably being honoured with the best master's and Ph.D. Thesis Awards from Mansoura University in 2012 and 2018, respectively.