# MACHINE LEARNING MODELS FOR CYBER SUPPLY CHAIN THREAT DETECTION

[1] M.Rakesh, , [2] Dr.M.Bheemalingaiah

[1] M.Tech Scholar in Department of CSE J.B. INSTITUTE OF ENGINEERING & TECHNOLOGY

[2] Professor in Department of CSE J.B. INSTITUTE OF ENGINEERING & TECHNOLOGY

rakhirakesh755@gmail.com

**Abstract**

The Cyber Supply Chain (CSC) consists of multiple interconnected subsystems, each performing essential tasks to ensure seamless operations. Due to this complexity, safeguarding the CSC is highly challenging, as vulnerabilities can be exploited at any stage, potentially leading to severe business disruptions. To mitigate these risks, it is critical to understand and forecast possible threats and implement effective protective measures. Cyber Threat Intelligence (CTI) provides valuable insights by analyzing adversary behavior, motivations, tactics, techniques, procedures (TTPs), and Indicators of Compromise (IoCs). In this study, we propose a predictive approach that combines CTI with Machine Learning (ML) models to identify and forecast threats within the CSC environment. We utilize the Microsoft Malware Prediction dataset and apply various ML algorithms—including Logistic Regression, Support Vector Machines, Random Forests, and Decision Trees—to analyze attack patterns and predict vulnerabilities and IoCs.Experimental results highlight that threats such as spyware, ransomware, and spear-phishing are the most prevalent and predictable in cyber supply chains. Based on these predictions, we recommend specific control measures to strengthen security. This study emphasizes the importance of integrating CTI with ML for proactive threat detection and enhancing cybersecurity in supply chain networks.

***Keywords***: *Cyber Supply Chain (CSC), Cyber Threat Intelligence (CTI), Machine Learning (ML), Indicators of Compromise (IoC), Tactics Techniques and Procedures (TTP), Malware Prediction, Cybersecurity, Threat Prediction.*

## I INTRODUCTION

The security of Cyber Supply Chains (CSC) has become a critical concern for ensuring the continuous and reliable operation of smart Cyber-Physical Systems (CPS). Due to the interconnected and distributed nature of CSCs, vulnerabilities can originate from one node and propagate across several other components, thereby threatening the integrity and stability of the entire system. Recent findings from theNational Cyber Security Centre (NCSC) have highlighted numerous cyberattacks that were successful in exploiting such weaknesses within

supply chain infrastructures (NCSC, 2020). The growing reliance of organizations on third-party vendors for outsourcing services and data management has only amplified the attack surface, making these systems increasingly susceptible to targeted intrusions.

Several high-profile incidents illustrate the severity of supply chain attacks. The Dragonfly cyber-espionage group, for instance, is known for its persistent targeting of CSC infrastructures, aiming to compromise operational systems through trusted vendors (Kushner, 2013; Symantec, 2017). Similarly, the cyberattack on Saudi Aramco's power systems disrupted operations on a national scale, demonstrating the devastating potential of CSC vulnerabilities when exploited (NCSC, 2020). Although past studies have examined risks within CSCs, they often lack a comprehensive application of Cyber Threat Intelligence (CTI) to improve overall cybersecurity posture. Moreover, there is an urgent need to anticipate cyberattack trends to enable organizations to take preemptive actions.

Predictive analytics can significantly enhance situational awareness by uncovering patterns related to attacker behavior, intent, and methods. Integrating CTI into this process offers valuable, evidence-based insights into both known and emerging threats. It supports early detection and reduces the time required to respond to incidents, thereby mitigating damage. CTI captures critical elements such as attacker motivation, skill, Indicators of Compromise (IoCs), and Tactics, Techniques, and Procedures (TTPs), which are essential for understanding threat landscapes and designing effective countermeasures.

In this context, the present study aims to strengthen cybersecurity within CSC environments by combining CTI with Machine Learning (ML) models to predict potential attack behaviors. By applying classification algorithms such as Logistic Regression, Support Vector Machines, Random Forests, and Decision Trees, we map threat intelligence attributes—including IoCs and TTPs—into predictive frameworks. This integrated approach enables organizations to better anticipate and defend against evolving cyber threats.

## II LITERATURE SURVEY

In recent years, the intersection of Cyber Threat Intelligence (CTI) and Machine Learning (ML) has become increasingly relevant in cybersecurity research, especially for enhancing threat prediction capabilities in Cyber Supply Chain (CSC) environments. This section reviews the key contributions related to CSC security, CTI frameworks, and the role of ML in cyberattack prediction.

Cyber Supply Chain (CSC) security focuses on securing the exchange of goods, services, and information across connected third-party entities, including suppliers, service providers, and distributors. As business operations increasingly rely on outsourced services, the potential attack surface within the supply chain expands

significantly. Researchers have observed that attacks in these ecosystems often exploit operational and information technologies in cyber-physical infrastructures, resulting in data tampering, delivery redirection, and service disruptions [1], [2]. The National Institute of Standards and Technology (NIST) addressed this issue through the SP800 framework, proposing a four-tiered risk management model that evaluates organizational strategies, threat exposure in inbound/outbound logistics, impact assessments, and real-time monitoring. However, the framework does not incorporate predictive analytics using ML techniques [3]. In addition, researchers proposed structured models for identifying and classifying supply chain attack patterns across the acquisition lifecycle, though the focus remained largely on classification rather than forecasting future threats [4].

CTI has emerged as a crucial capability for identifying, analyzing, and mitigating both known and unknown cyber threats. The European Union Agency for Cybersecurity (ENISA) has identified multiple strategic, tactical, and operational benefits of CTI, including informing executive decision-making, identifying intelligence gaps, and understanding attacker behaviors, motivations, and techniques [5]. However, most of these initiatives fall short in incorporating machine learning as part of the intelligence process. For example, some works have outlined comprehensive CTI lifecycles—spanning direction, collection, processing, analysis, dissemination, and feedback—but rely mostly on internal logs, vulnerability databases, and human-sourced content from the dark web and social media [6]. Others developed intelligence metrics for risk prioritization, asset analysis, and stakeholder engagement but omitted predictive modeling based on historical and real-time threat data [7]. Operational CTI models that track adversary behavior throughout an organizational lifecycle have emphasized intent analysis but lack automated learning capabilities needed for proactive defense [8].

Machine learning, on the other hand, has demonstrated significant promise across various cybersecurity applications, including spam filtering, intrusion detection, malware classification, and anomaly detection [9], [10], [11]. Some studies applied decision tree models to classify HTTP requests and identify malicious web traffic, showing improved accuracy and recall [12]. Others tested ML classifiers like Logistic Regression, Support Vector Machines (SVM), Naïve Bayes, and Decision Trees in cloud environments, achieving high accuracy in packet anomaly detection [13]. Despite their effectiveness, these models were not tailored for CSC-specific threats and lacked integration with CTI.

In a related study, various ML algorithms—such as Artificial Neural Networks, Fuzzy Rule-Based Systems, and Bayesian Networks—were evaluated for intrusion detection, but the focus remained on generic network threats rather than

supply chain-specific vulnerabilities [14]. Another review on cybersecurity datasets used for ML models highlighted deficiencies in feature representation and relevancy for modern intrusion detection systems, particularly in relation to CSC environments [15]. A separate study employed decision tree models to analyze and correlate system logs, achieving reasonable accuracy but did not explore model comparisons or incorporate CTI indicators such as IoCs and TTPs [16].

Further exploration into machine learning for cyber-physical and SCADA systems revealed promising detection capabilities through techniques like K-Nearest Neighbor (KNN), Random Subspace Trees, and deep learning-based semi-supervised models [17], [18], [19]. However, these approaches still lacked a focus on the broader CSC ecosystem involving suppliers, vendors, and logistics nodes. Similarly, research on predictive analytics for cybersecurity incidents using text mining and ML techniques like SVM and Naïve Bayes showed good performance but failed to integrate CTI-driven threat classification [20].

Other initiatives have explored predictive models for malware infection risks using machine learning, such as random forest classifiers, achieving high precision in associating risk profiles with machine behavior patterns [21]. Some authors also used large-scale datasets like the Verizon data breach reports to train random forest classifiers to predict the likelihood of future incidents in enterprise networks, achieving strong predictive performance but without mapping predictions to specific supply chain attack patterns [22].

In summary, although the reviewed literature showcases the growing role of ML in cybersecurity and the evolving application of CTI for threat awareness, there is a clear lack of integrated approaches that combine both CTI and ML for predictive analytics in CSC environments. Existing work has rarely emphasized threat prediction from the perspective of the CSC's inbound and outbound network nodes. Given the cascading nature of cyberattacks in such systems, predicting and mitigating threats early becomes essential. CTI provides the necessary threat context and intelligence, while ML offers automated capabilities to detect patterns and forecast attacks. Therefore, our study bridges this gap by integrating CTI-based data sources with machine learning models to predict potential attacks and support informed decision-making for CSC cybersecurity.

## III EXISTING SYSTEM

In the existing cyber supply chain (CSC) security landscape, several organizations rely on traditional cybersecurity measures and static threat detection tools. While Cyber Threat Intelligence (CTI) has gained traction for its ability to provide insights into known attacks and threat actors, its full potential remains underutilized—especially in predictive security. Most existing approaches focus on reactive

strategies, addressing threats only after they have occurred. Although some frameworks have adopted machine learning (ML) models for broader cybersecurity tasks like intrusion detection and anomaly detection, these models are rarely tailored specifically for CSC environments. Furthermore, they do not typically integrate CTI properties such as Tactics, Techniques, and Procedures (TTP) or Indicators of Compromise (IoC), which are crucial for understanding and forecasting sophisticated cyber threats in supply chains. As a result, these systems fall short in proactively identifying emerging threats and delivering actionable insights for CSC-specific vulnerabilities.

## IV PROBLEM STATEMENT

In today's interconnected digital ecosystem, Cyber Supply Chains (CSC) play a crucial role in business operations. However, their complexity and dependence on third-party vendors expose them to significant cybersecurity threats. These threats are often difficult to detect and can severely disrupt business continuity. Traditional security approaches fall short when it comes to identifying sophisticated, evolving cyberattacks. While Cyber Threat Intelligence (CTI) provides useful information about threat actors and attack patterns, it is rarely used effectively in real-time threat prediction. By combining CTI with Machine Learning (ML), there is an opportunity to proactively predict potential threats and recommend timely security measures. This research addresses the need for an intelligent and predictive system that improves CSC security through the integration of CTI and ML techniques.

### Objectives

**To build an integrated framework that combines CTI and ML for predicting cyber threats**, enabling early detection of both known and emerging attacks within the cyber supply chain.

**To implement and compare various ML models**—such as Logistic Regression, Support Vector Machines, Random Forest, and Decision Trees—based on their accuracy and effectiveness in identifying threats like ransomware, spyware, and phishing.

**To suggest practical security controls and preventive strategies** based on model outcomes, helping organizations reduce vulnerabilities and strengthen their overall supply chain cybersecurity.

## V PROPOSED SYSTEM

The proposed system aims to address the growing challenges in securing Cyber Supply Chains (CSC) by developing a comprehensive, intelligent framework that integrates Cyber Threat Intelligence (CTI) with Machine Learning (ML) techniques. Unlike traditional approaches that react to threats after the fact, this system takes a proactive stance—anticipating potential

attacks before they can compromise systems. At its core, the framework harnesses the power of CTI to gather valuable information on past and current cyber threats. This includes details such as threat actor profiles, their motivation and capabilities, Tactics, Techniques, and Procedures (TTPs), Indicators of Compromise (IoCs), attack vectors, and incident records. This intelligence data forms the foundation for building robust predictive models using machine learning. To achieve high accuracy and adaptability, the system employs several well-established ML algorithms, including Logistic Regression, Support Vector Machines (SVM), Random Forest, and Decision Trees. These models are trained on real-world cybersecurity datasets—such as the Microsoft Malware Prediction Dataset—to learn patterns and relationships between attack indicators and system vulnerabilities. Once trained, these models can classify new data inputs and predict the likelihood of various types of cyberattacks, including advanced persistent threats (APT), spyware, ransomware, and spear-phishing campaigns. One of the most significant strengths of this system is its ability to map CTI properties directly into ML-compatible features. This mapping allows the models to make informed, context-aware predictions rather than relying solely on generic network behavior. By considering both inbound and outbound nodes in the supply chain, the system offers a more holistic view of potential vulnerabilities across the entire CSC ecosystem.In addition to detection, the proposed system also emphasizes response. Based on the nature and type of the predicted threat, it can recommend appropriate control strategies. These include directive controls (policies and procedures), preventive measures (firewalls, access restrictions), detective actions (intrusion detection systems), corrective responses (patching and removal of malware), and recovery strategies (backups and business continuity planning). This layered approach ensures that organizations are not just made aware of threats but are also equipped with actionable strategies to mitigate them.

## VI METHODOLOGY

The proposed system follows a structured and modular methodology to integrate Cyber Threat Intelligence (CTI) with Machine Learning (ML) for effective threat prediction in cyber supply chains (CSC). The first phase involves **data collection**, where datasets related to malware, attacks, and CTI are gathered. The Microsoft Malware Prediction dataset is used as the primary source of structured attack data, while CTI inputs include details such as threat actor capabilities, Tactics, Techniques, and Procedures (TTP), and Indicators of Compromise (IoC). These datasets form the foundation for the ML model's learning and prediction capability.

The next phase is **data preprocessing**, which is essential to ensure the accuracy and performance of ML models. This includes cleaning the dataset to remove duplicates or irrelevant records, handling missing values, encoding symbolic data into numeric format, and normalizing the values to a uniform scale. Additionally, unnecessary features that do not contribute meaningfully to the prediction are removed to reduce complexity and computation time.

After preprocessing, the system proceeds with **feature engineering**, where CTI properties are carefully mapped to ML-compatible features. This mapping includes integrating IoCs, attack vectors, tools used by threat actors, and threat patterns. The idea is to transform high-level intelligence data into structured input features that ML models can use to detect patterns in past and present threats.

In the **modeling phase**, multiple ML algorithms are trained and tested. These include Logistic Regression (LR), Support Vector Machines (SVM), Random Forest (RF), and Decision Trees (DT). These models are chosen based on their proven ability to handle classification problems in cybersecurity applications. The models are trained using the preprocessed dataset and validated through cross-validation techniques to ensure generalizability and to avoid overfitting. Once trained, the models are subjected to **evaluation metrics** such as accuracy, precision, recall, F1-score, and Receiver Operating Characteristic (ROC) curves. These metrics help determine the model that provides the best performance in predicting threats based on CTI inputs. The final phase involves applying the selected model to real-time or batch data for **threat prediction**, followed by recommending **appropriate control mechanisms**. These controls can be preventive detective corrective or recovery-focused

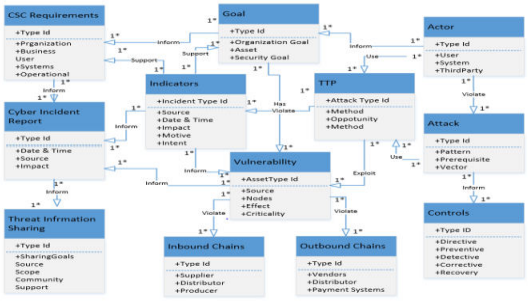



FIGURE 1. Meta-model for the proposed conceptual view of CSC system security.

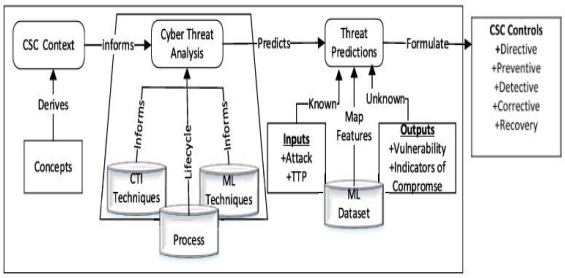



FIGURE 2. Applying CTI and ML for threat intelligence and predictive analytics.

## VII IMPLEMENTATION

The system is implemented using the Python programming language due to its versatility and availability of powerful data science libraries. The development environment includes **Jupyter Notebook**, which provides an interactive workspace for data preprocessing, modeling, and visualization. The primary libraries used include **Pandas** for data manipulation, **NumPy** for numerical computation, **Matplotlib** and **Seaborn**

for data visualization, and **Scikit-learn** for implementing machine learning algorithms.

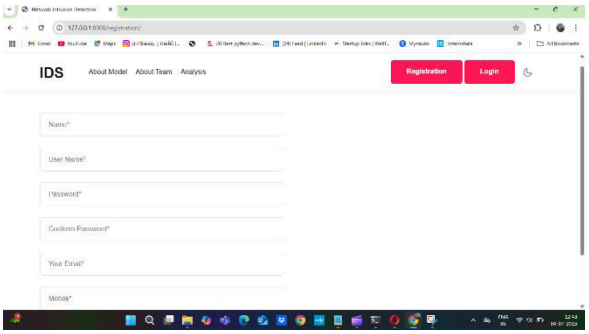
The implementation begins with loading the CTI and malware datasets into Pandas Data Frames. After loading, the data undergoes a comprehensive **preprocessing stage**, which involves cleaning, encoding, normalization, and handling of missing values. The data is then transformed into a format suitable for ML models. Important CTI attributes such as threat actor roles, TTP patterns, and IoCs are embedded as features during this stage.

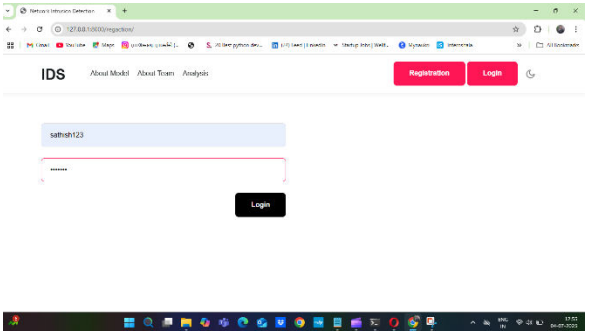
The **model training phase** involves using Scikit-learn to implement and compare different classification algorithms. Each model is trained on a portion of the dataset and evaluated using a separate test set. Techniques such as **Research** are employed for hyperparameter tuning to optimize the model's performance. The system records the accuracy, confusion matrix, and ROC-AUC score for each algorithm to identify the best-performing model.

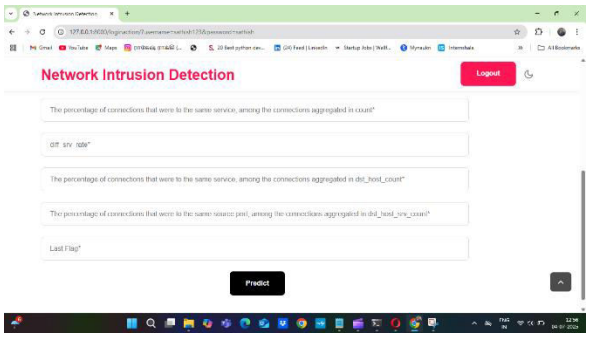
Following model selection, the **threat prediction engine** uses the trained model to classify new instances as safe or potentially malicious based on input features. This classification process is automated, and once a threat is identified, it is passed to the **recommendation module**, which suggests a set of control actions depending on the predicted threat type. For example, a ransomware prediction may trigger recommendations for isolation, backup validation, and patching vulnerable endpoints.

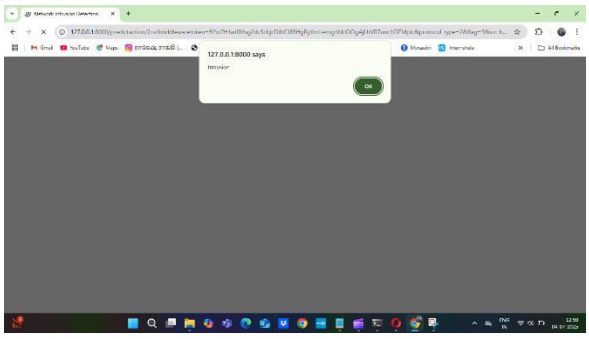
From a hardware perspective, the system is designed to run on a basic configuration—an Intel i3 or above processor with at least 4 GB of RAM and 500 GB of hard disk space. It is lightweight and suitable for academic or enterprise settings. The final implementation can also be extended using a web-based interface or REST API for real-time deployment in a security operations environment.

## VIII RESULSTS



## IX CONCLUSION

The integration of cyber-physical systems (CPS) within Cyber Supply Chain (CSC) environments has significantly influenced various sectors such as transportation, energy, healthcare, manufacturing, and communications. While these advancements have contributed positively to economic and societal progress, they have also introduced complex security challenges. Even a minor vulnerability in one component can trigger serious risks across the entire supply chain network.

To address these concerns, this study proposed a novel approach that combines Cyber Threat Intelligence (CTI) with Machine Learning (ML) techniques for threat analysis and prediction within CSC frameworks. By leveraging essential concepts from both domains, we designed a structured methodology to identify and forecast potential cyber threats. Through experimentation, we evaluated the performance of multiple classification algorithms—Logistic Regression, Decision Tree, Support Vector Machine, and Random Forest—using a majority voting ensemble. The results demonstrated promising prediction accuracy and revealed various potential threat patterns relevant to CSC environments.

Our findings also confirmed the effectiveness of CTI in extracting actionable threat data, which, when integrated with ML models, enhances the accuracy and relevance of threat predictions. This enables CSC organizations to reassess their current security measures and implement additional controls to strengthen their overall cybersecurity posture.

## 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 sup ply 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-OforiandF.Katsriku, Cybercrime and risks for cyber physical systems, Int. J. Cyber-Secur. Digit. Forensics, vol. 8, no. 1, pp. 4357, 2019.

[8] CAPEC-437, Supply Chain. (Oct. 2018). Common Attack Pattern Enu meration and Classi cation: Domain of Attack. [Online]. Available: https://capec.mitre.org/data/de nitions/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. 15, 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 orga nizations, NIST Comput. Sec., vol. 800, no. 161, p. 32, 2015, doi: 10.6028/NIST.SP.800-161. 1.1,

[13] Framework for Improving Critical Infrastructure Cybersecurity, Version 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/les/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, De nition guide to cyber threat intelli gence. 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 Oper ating 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. 6673, doi: 10.1109/ICSIoT47925.2019.00019.

[19] B. Gallagher and T. Eliassi-Rad, Classi cation of HTTP attacks: A study ontheECML/PKDD2007discoverychallenge, LawrenceLiverpoolNat. 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 machinelearning for cloudsecurity, inProc.Int. Conf. Inf. Sci. Secur. (ICISS), Dec. 2016, pp. 15, 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. 11531176, 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. 21862193, doi: 10.1109/BigData.2017.8258167.

[23] E. G. V. Villano, Classi cation 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 Con trol Syst. (ISRCS), Denver, CO, USA, Aug. 2014, pp. 18, 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. 61546162, 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. 525538, 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. 28602870, Apr. 2021, doi: 10.1109/TII.2020.3015026.

[30] M. M. Hassan, M. R. Hassan, S. Huda, and V. H. C. de Albuquerque, Arobust deep-learning-enabled trust-boundary protection for adversarial industrial IoT environment, IEEE Internet Things J., vol. 8, no. 12, pp. 96119621, Jun. 2021, doi: 10.1109/JIOT.2020.3019225.

[31] A. Mohasseb, B. Aziz, J. Jung, and J. Lee, Predicting cybersecu rity incidents using machine learning algorithms: A case study of Korean SMEs, in Proc. INSTICC, 2019, pp. 230237, 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. 12991311, 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. 10091024.

[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