iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** IX **Month of publication:** September 2023

DOI: https://doi.org/10.22214/ijraset.2023.55918

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue IX Sep 2023- Available at www.ijraset.com

Detection of Cyber Attacks using Machine Learning

Simran Saini[1], Prof. Dr. Arvind Kalia[2]
Department of Computer Science, Himachal Pradesh University, Shimla, H.P

Abstract: ***In today's world, every aspect of daily life is now dependent on cyberspace. As a result, cybercrimes and threats are becoming more likely. Numerous machine learning methods have been developed to combat cyber threats and prevent them. Machine learning played an important role to detect the cyber-attacks as machine learning algorithms were used for the detection of cyber-attacks. The study aims to compare different machine learning algorithms used for detecting cyber-attacks and provide a comparative analysis based on different metrics. The paper presents a literature review of various detection techniques used for cyber-attacks detection. The comparison table in the paper compares different machine learning algorithms used for detecting cyber-attacks. The algorithms are compared on different metrics such as accuracy, methods used, datasets, and performance. The paper highlights the importance of detection of cyber-attacks and the effectiveness of machine learning algorithms in detecting such attacks.***
Keywords: Cyber-attacks, machine learning, cyber-attack detection, Accuracy, database.

I. INTRODUCTION

In the field of Internet security, cyber-attack is a touchy subject. People are connected to the internet almost every day for business, to keep in touch with their family and friends, for education and so on. Being connected comes with a number of potential risks in addition to concerns about life or career advancement. New forms of malware that target networks are developing daily, making the situation worsening. To better secure our systems, it is crucial to comprehend these attacks both before and after they take place.
The work is focused on the issue of cyber-attacks and the need for effective detection techniques to catch them. It explores various detection techniques for different types of cyber-attacks, using machine learning algorithms. Comparison of different algorithms took place on various metrics such as accuracy, false positive rate, false negative rate, performance, and datasets. Aims to provide a conclusive analysis of the work of various researchers in this field. The paper discusses the existing literature on cyber-attack detection, highlighting the different detection techniques and algorithms proposed by researchers. It aims to identify the strengths and weaknesses of different machine learning algorithms in detecting cyber-attacks, providing insights into their applicability and performance in real-world scenarios. The paper contributes to the understanding of cyber-attack detection by synthesizing and analyzing the findings from previous research and identifying research gaps.

II. TYPES OF CYBER ATTACKS

1) *DDoS:* - DDoS Attack is an abbreviation for "Distributed Denial-of-Service (DDoS) Attack," and it is a type of cybercrime in which an attacker floods a server with internet traffic in order to prohibit people from accessing linked online services and sites.
2) *Malware:* - Any program or code created with the intention of causing harm to a computer, network, or server is considered malware or malicious software.
3) *Denial-of-Service (DoS) Attacks:* - Users are unable to access email, websites, online accounts, or any other resources that are controlled by a compromised computer or network during a DoS attack. While the majority of distributed denial of service attacks do not result in the loss of data.
4) *Phishing Attack:* - Phishing are scams that attempts to steal user's credential or sensitive data, such as passwords or account numbers or it can be a malicious fikle that will leave virus on their systems or phones.
5) *Ransomware:* - Ransomeware is sophisticated malware that uses strong encryption to hold data or system functionality hostage by exploiting system flaws.
6) *Backdoor Trojan:* - Backdoor Trojans open a backdoor on the victim's system, allowing the attacker to take complete and remote control. Attackers can also use the Trojan for other types of cybercrime.
7) *DNS Tunneling:* -DNS Tunneling is a type of cyber-attack that uses queries and responses from the domain name system (DNS) to get around traditional security measures and send data and code inside the network.

©IJRASET: All Rights are Reserved

8) *IoT-Based Attacks:* - Any cyber-attack that targets an Internet of Things (IoT) device or network is an IoT attack. The hacker can take control of the device after it has been compromised, steal data, or join a group of infected devices to form a botnet to launch DoS or DDoS attacks.
9) *Supply Chain Attacks:* - An supply chain attack is a type of cyber-attack that targets a trusted third-party vendor who offers services or software vital to the supply chain.

III. LITERATURE REVIEW

In this section various detection techniques of different cyber-attacks are discussed also using machine learning algorithms. The work of various researchers have been studied which further assists in providing a conclusive analysis. Here, the findings, theoretical and methodological contributions, as well as the published information in a particular subject area that includes the finding, are discussed.

Ying Huang et al. (2007) proposed a scheme to detect early-stage DDoS attacks based on a feature called the non-negative cumulative increment effect of DDoS traffic throughput, effectively distinguishing it from normal flash crowd traffic. The algorithm can even detect potential DDoS attacks when packet attributes lack distinct features, and it works for online and distributed attacks, as confirmed through simulations.

Yu Chen et al. (2007) introduced a DDoS flooding attack detection system at the traffic-flow level, designed for ISP core networks. The system uses cooperative attack-transit routers and CAT servers in ISP domains to aggregate flooding alerts. It employs a secure infrastructure protocol (SIP) to resolve policy conflicts across domains. Simulations on the DETER testbed demonstrate high detection accuracy (98%) with minimal false positives, and the system scales effectively to cover 84 AS domains.

Ying Huang et al. (2008) proposed an algorithm for early DDoS attack detection based on the persistent increase trend of DDoS traffic. Their method detects DDoS attacks even when the attacking packet lacks distinct features, signatures, or conditions. It adapts to various sophisticated attacks and is effective when attack rates are low and gradually increasing. The algorithm can extract attack characteristics like increment trends and persistence features, and it works with various DDoS packet types, including ICMP, UDP, TCP-SYN, and source IP.

Sabaliauskaite and Mathur (2013) propose using Intelligent Checkers (IC) to enhance the security of Cyber-Physical Systems (CPS). ICs, independent of the cyber-component, monitor physical processes and trigger alarms when measurements breach predefined limits. They validate data from CPS sensors through one-way communication, even in cases of communication failure or undetected cyber-attacks. Placing ICs strategically within a CPS aims to enable early attack detection.

Wenji Chen et al. (2013) focused on detecting cyber-attacks through changes in network traffic cardinality. They presented a nonparametric error-bounded solution for cardinality-based change point detection in dispersed attack traffic streams. This method allows data from multiple monitoring locations to identify widespread attacks, making it suitable for space-constrained systems with efficient resource use. Their experiments, using synthetic and real-world data, demonstrated fine-grained and quick change point detection through a sliding window approach. This method can detect attacks close to their onset and is suitable for online detection of cyber-attacks like DDoS and worm spreading.

Chia-mei Chen et al. (2014) focused on early-stage detection of targeted attacks. They proposed a defense system that analyzed multiple network logs to extract reconnaissance attack sequences related to targeted attacks. The study revealed that current detection systems often mistook intruders for regular users and failed to identify joint attacks effectively. Their system, however, effectively detected and identified early-stage targeted attacks by combining and correlating multiple logs. It employed a state-based hidden Markov model (HMM) for detecting joint attacks, and experimental results showed its effectiveness in detection.

Emmanouil Vasilomanolakis et al. (2016) developed a honeypot for detecting multi-stage attacks on Industrial Control System (ICS) networks. This honeypot creates signatures that Intrusion Detection Systems (IDSs) can use to thwart similar future attacks. The paper presents a formal model for detection mechanisms and details the signature generation process. Experiments showed the honeypot and generated signatures offer accurate detection, with the Bro IDS effectively using these signatures for future attack detection.

Bhunia S. S. and Gurusamy M. (2017) introduced "Soft Things," an SDN-based secure IoT framework. It employs machine learning at the SDN controller to monitor and learn from IoT device behavior, enabling early detection of abnormal behaviors and attacks at the network edge. This approach ensures faster identification and mitigation of attacks on IoT devices. Machine learning is used to spot traffic anomalies, and emulation experiments on Mininet showed that the framework effectively mitigated attacks with high precision and recall.

Yaokai Feng et al. (2018) proposed a machine learning approach to detect distributed cyber-attacks early by selecting crucial features from network traffic data. They assessed various feature selection techniques and machine learning algorithms, finding that SVM feature selection with an SVM classifier performed best. The study also emphasized the significance of feature selection in enhancing algorithm performance for early detection of cyber-attacks.

Karan B. V. et al. (2018) proposed a two-stage DDoS attack detection system for SDN. Snort identified signature-based attacks, while machine learning, using SVM and DNN on the KDD Cup dataset, detected anomaly-based attacks. In an SDN environment, DNN showed superior precision and accuracy over SVM, making it more effective at distinguishing between normal and abnormal requests.

D.C. Grant (2018) conducted a test to assess the effectiveness of remote devices in detecting distributed denial of service (DDoS) attacks and enabling rapid response. The experiment showed that combining open-source intrusion detection systems with open-source honeypots was both feasible and reasonably effective. While honeypot logs weren't the most effective DDoS detection method, remote sensors across the Internet can safely transmit valuable information to intrusion detection systems. Additionally, the implemented systems demonstrated sufficient security to prevent impersonation or traffic replay by attackers.

Mehmet Necip Kurt et al. (2018) used model-free reinforcement learning (RL) for POMDPs to create an online cyber-attack detection solution for smart grids. They demonstrated the algorithm's effectiveness in quickly and accurately detecting cyber-attacks in smart grids, presenting the problem as a POMDP with a Precision/Recall/F-score-based solution. Mathematical analyses highlighted the benefits of their approach, showing RL's potential in solving challenging cybersecurity problems.

M. Lopez-Vizcaino et al. (2019) addressed the challenge of early intrusion detection to halt the "Cyber Death Chain." They assessed time-aware metrics for identifying threats in computer networks early and introduced a new metric, NormERDE. Using a real-world dataset, they conducted a time-aware evaluation, emphasizing the importance of time-aware criteria for accurate judgments. They found that NormERDE (o=5) provided better results for assessing time-aware intrusion detection systems, underscoring the significance of rating each chunk of data.

Zakaria El Mrabet et al. (2019) focused on detecting false data injection attacks in home area networks using Artificial Neural Networks (ANN). They used energy data from 200 US households to train and test their ANN model, comparing it to other machine learning techniques. ANN with a Relu activation function and 100 neurons achieved a 99% accuracy in identifying false data, outperforming SVM and RF. However, RF had a lower false alarm rate (0.2%) compared to ANN (0.9%).

Fan Zhang (2019) developed a multi-layer intrusion detection system (IDS) for industrial control systems (ICSs). It uses network traffic, host system data, and process parameters to create a defense-in-depth approach. Real-time ICS testbed data were used to simulate cyber-attacks and build data-driven detection models. The system employs classical classification models to provide a secondary line of defense in case intrusion detection fails. This multi-layer data-driven IDS is promising for enhancing ICS cybersecurity.

IV. COMPARATIVE ANALYSIS

This segment gives examination and correlation of the different detection methods utilized for different types of cyber-attacks. The techniques will be easier to comprehend with the help of this chapter.

Table 1 comparison of cyber-attack detection accuracy of existing machine learning techniques.

Year	Problem Identified	Technique used	Dataset used	Result
2007	Detecting Distributed Denial of Service (DDoS) attacks	a non-negative and cumulative increment algorithm to detect DDoS attacks		a new algorithm that can detect DDoS attacks in their early stages based on a non-negative and cumulative increment effect of DDoS traffic throughput

2007	Detecting DDoS flooding attacks	a distributed change-point detection (DCD) architecture using change aggregation trees (CAT) to detect DDoS flooding attacks		The proposed DCD system can detect DDoS attacks with 98% accuracy and 1% false-positive alarms, and can scale well to cover most ISP core networks
2008	Detecting Distributed Denial of Service (DDoS) attacks	a new algorithm that combines stateful and stateless signatures to detect DDoS attacks in their early stages		The algorithm can accurately detect DDoS attacks in their early stages with online and distributed characteristics
2013	Detecting changes in the cardinality of network/attack traffic to indicate ongoing cyber-attacks	a nonparametric error-bounded scheme for cardinality-based change point detection in distributed streams of attack traffic	authors conducted experiments using both real-world traces and synthetic data to evaluate the proposed scheme	The nonparametric error-bounded scheme can detect changes in the cardinality of network/attack traffic within given time and error bounds, and can be used as a building block in network and security monitoring systems to detect large distributed cyber-attacks.
2013	Need to improve the security of cyber physical systems (CPS).	a novel approach using Intelligent Checkers (ICs)		The proposed approach using Intelligent Checkers (ICs) is expected to improve the security of cyber physical systems (CPS) by detecting process measurement violations and raising alarms, independent of the cyber-portion of the CPS
2014	targeted cyber-attacks and the need for efficient early detection to prevent further damage in the networks	a state-based model using Hidden Markov Model (HMM) algorithm for efficient early detection of targeted cyber attacks	labeled test data	The state-based model using HMM algorithm can efficiently detect early phase targeted cyber-attacks, which can prevent further damage in the networks
2016	Security	A novel honeypot		The result of this work

	challenges in Industrial Control Systems	technique for detecting multi-stage attacks targeting Industrial Control System (ICS) networks		is a novel honeypot capable of detecting multi-stage attacks targeting ICS networks and generating signatures to prevent future attacks of the same type
2017	security threats to IoT devices	use of machine learning algorithms at the SDN controller to monitor and learn the behavior of IoT devices over time		SoftThings framework is capable of detecting attacks on IoT devices with around 98% precision using non-linear Support Vector Machine (SVM) algorithm
2018	Distributed cyber-attacks early detection	a machine learning-based approach using traffic features to detect Command and Control (C&C) communication	CCC datasets including C08, C09, C10 and C13 datasets	After no. of features reach 40, there is no change in the detection performance and top 10 features for detecting C&C traffic were found.
2018	vulnerability of SDN controller to DDoS attacks	signature-based detection using Snort and anomaly-based detection using machine learning algorithms, specifically Support Vector Machine (SVM) classifier and Deep Neural Network (DNN)	KDD Cup dataset	The Deep Neural Network (DNN) algorithm performs better than the Support Vector Machine (SVM) classifier in detecting DDoS attacks in an SDN environment.
2018	Escalation of Distributed Denial of Service (DDoS) attacks	a collaborative system that combines distributed honeypots and intrusion prevention systems (IPS) to detect and actively respond to DDoS attacks.		the testing of operational communication between distributed honeypots and IPS devices to detect and actively respond to DDoS attacks at near machine speed

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

2018	online cyber-attack detection in the smart grid	a model-free reinforcement learning algorithm for partially observable Markov decision processes (POMDPs)		The RL-based algorithm effectively detects cyber-attacks targeting the smart grid in a timely and accurate manner
2019	false data injection attacks in home area networks	Artificial Neural Network (ANN) based approach for detecting false data injection attacks in Home Area Networks	The dataset used in this work contains energy profiles of 200 U.S. households	the ANN model has a high probability of detection (Pd) of false data injection attacks in home area networks, outperforming other machine learning methods such as SVM and Random Forest
2019	Detecting cyber-attacks in IoT networks using machine learning algorithms	evaluates seven machine learning algorithms, including K-Nearest Neighbors, ID3, Random Forest, AdaBoost, Quadratic discriminant analysis, Multilayer perceptron, and Naive Bayes, to detect cyberattacks in IoT networks	DARPA 98, KDD99, UNSW-NB15, ISCX, CICIDS2017, and N-BaIoT	machine learning algorithms can effectively detect cyber-attacks in IoT networks, and the new features extracted from the Bot-IoT dataset outperformed the features used in previous studies
2019	need for time-aware metrics in evaluating Network Intrusion Detection Systems (NIDS)	used time-aware metrics in evaluating Network Intrusion Detection Systems (NIDS)	OS Scan Attack from Kitsune dataset	The proposal of using time-aware metrics in evaluating Network Intrusion Detection Systems (NIDS) to improve early detection of threats.
2019	Cybersecurity of industrial control systems	a multi-layer, data-driven cyber-attack detection system utilizing network	AAKR	The proposed multi-layer data-driven cyber-attack detection system utilizing network, system, and process data is a promising solution for safeguarding an ICS

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

2020	Detecting attacks in cybersecurity.	Wrapped evolutionary algorithm with a special crossover operator that considers feature importance, and random forest as a classification technique.		The incorporation of feature importance information in the wrapped evolutionary algorithm improves the performance of random forest in detecting attacks in cybersecurity.
2020	Inefficiency of conventional signature-based methods in detecting advanced malware programs, specifically in the case of zero-day and polymorphic viruses attacks	a multilayered feed-forwarding approach with Random Forest (RF), Support Vector Machine (SVM), K-Nearest Neighbor (K-NN) classifiers, Ensemble Voting (EV) algorithm, and adaptive frameworks to detect phishing attacks	The paper uses three datasets to train and test the proposed framework: 1. A dataset of static webpages 2. A dataset gathered by the Phish Tank website 3. A phishing dataset of the Center for Machine Learning and Intelligent Systems	The proposed adaptive Machine Learning based active malware detection framework successfully detects phishing attacks with higher accuracy rates compared to conventional signature-based methods
2020	Obtaining fast predictions with less resources while using deeper neural networks for intrusion detection	a neural network with Leaky ReLU activations and dropout to reduce over-fitting	CICIDS2017 and UNSW-NB15	The architecture can achieve comparable accuracies to simple fully connected neural networks without evaluating all layers for the majority of samples, thus saving energy and computational efforts

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

2021	The need for early multistage attack detection	a combination of Machine Learning and the MITRE Adversary Tactic Technique and Common knowledge (ATT&CK) framework for early multistage attack detection in real-time.	labeled dataset	The model achieves 98% accuracy in detecting multistage attacks using a combination of Machine Learning and the MITRE ATT&CK framework.
2021	Early-stage botnet detection problem	feature selection techniques and machine learning classifiers for early-stage botnet detection	Cyber Clean Center (CCC) dataset containing C08, C09, C10, and C13 datasets	The approach efficiently classifies normal and malicious traffic at an early stage with an accuracy of 99%, True Positive Rate (TPR) of 0.99%, and False Positive Rate (FPR) of 0.007%
2021	detecting cyberattacks on computer networks by identifying anomalies in network traffic and determining their impact using statistical methods	the Dickey-Fuller test, rescaled range analysis, detrended fluctuation analysis, moving average, Z-Score, and CUSUM		The proposed technique demonstrated the presence of self-similarity in network traffic and confirmed the high efficiency of the method for detecting cyberattacks in real or near real time

The above table shows the comparison of various cyber-attacks detection techniques used in this study. The problem identified by the researchers, dataset used, techniques which are used for implementation, the features and results produced by the various techniques are discussed in this table.

V. CONCLUSION

One of the most prevalent issues affecting computer networks and the cyber world is cyber-attacks. As a result, we need effective detection algorithms or systems to catch these attacks. Based on the datasets, tools, and algorithms used, this study shows that how various algorithms improve detection performance.

The work focuses on the early detection of cyber-attacks using machine learning algorithms. The study shows that cyber-attacks are a prevalent issue in computer networks and the cyber world, and effective detection algorithms are needed to catch these attacks. The work compares different machine learning algorithms used for detecting cyber-attacks and provides a comparative analysis based on different metrics.

Overall, the paper emphasizes the importance of developing effective detection methods to combat cyber-attacks. The methods currently used to detect cyber-attacks are thoroughly reviewed and compared in this study. The work provides a detailed analysis of the performance of different machine learning algorithms on different datasets and provides valuable insights into the effectiveness of these algorithms for detecting cyber-attacks.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

The SDN-based secure IoT framework was found to be the most suitable method for detecting cyber-attacks with an accuracy of 98%. Overall, the paper highlights the importance of early detection of cyber-attacks and the effectiveness of machine learning algorithms in detecting such attacks.

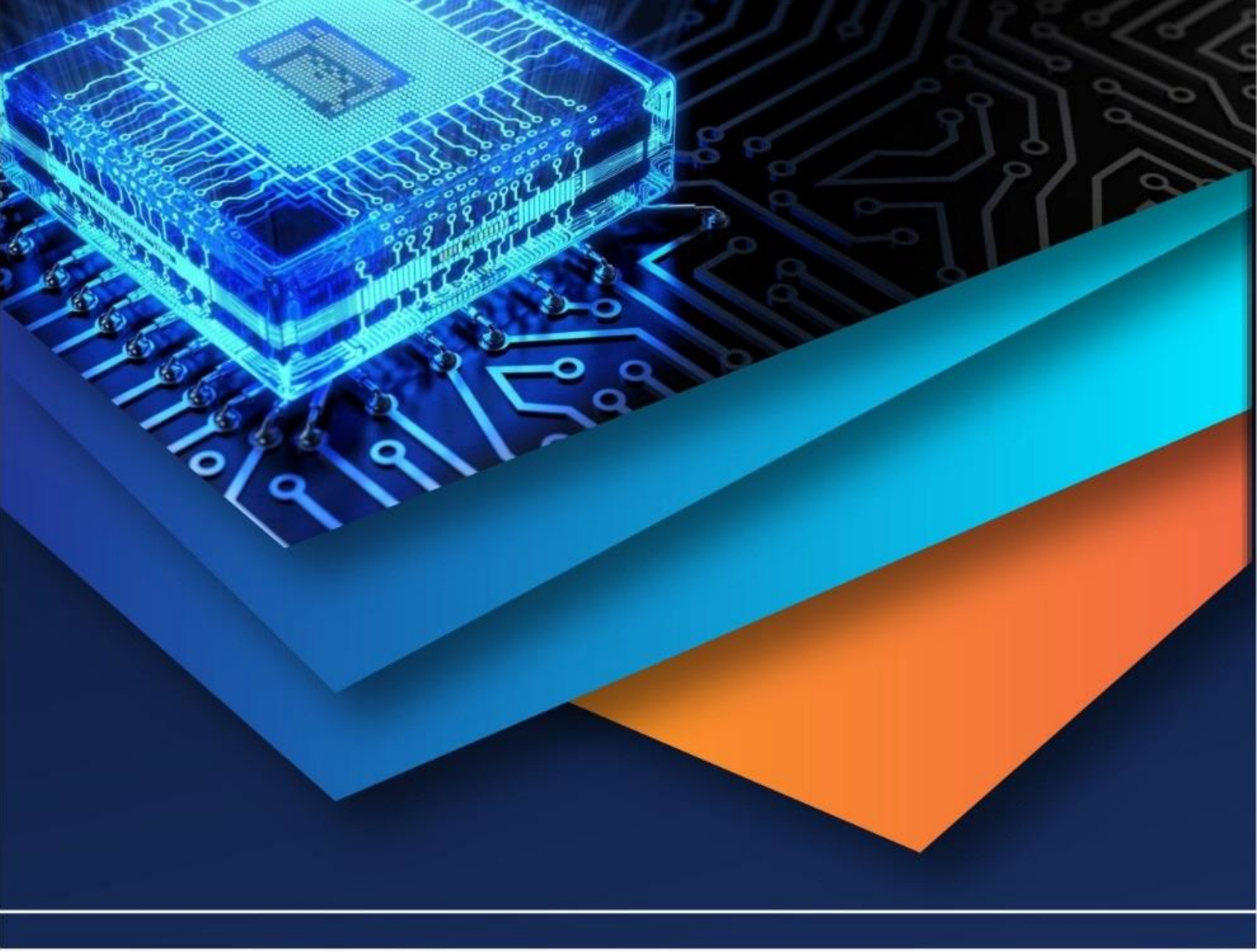
VI. FUTURE SCOPE

The potential future work could include Adaptive Algorithms i.e. Designing machine learning algorithms that can adapt to evolving cyber threats and update their models accordingly which can ensure long-term effectiveness in cyber threat detection without the need for frequent retraining or manual adjustments.

REFERENCES

[1] Ying Huang, H. S. (2007). Non-negative Increment Feature Detection of the Traffic Throughput for Early DDoS Attack. IEEE, 6.
[2] Yu Chen, M. I. (2007). Collaborative Detection of DDoS Attacks over Multiple Network Domains. IEEE, 14.
[3] Ying Huang, X. F. (2008). The Early Detection of DDoS Based on the Persistent Increment Feature of the Traffic Volume . IEEE, 6.
[4] Mathur, G. S. (2013). Intelligent Checkers to Improve Attack Detection in Cyber Physical Systems. IEEE, 4.
[5] Wenji Chen, Y. L. (2013). cardinality change-based early detection of large scale cyber attacks. IEEE, 10.
[6] Chia-Mei Chen, P.-Y. Y.-H.-W. (2014). Targeted Attack Prevention at Early Stage. IEEE, 5.
[7] Guan, W. C. (2013). Cardinality Change-based Early Detection of Large-scale Cyber-Attacks. IEEE, 9.
[8] Emmanouil Vasilomanolakis, S. S. (2016). Multi-stage Attack Detection and Signature Generation with ICS Honeypots. IEEE, 6.
[9] Suman Sankar Bhunia, M. G. (2017). Dynamic attack detection and Mitigation in IoT using SDN. IEEE, 6.
[10] Karan B. V., N. D. (2018). Detection of DDoS Attacks in Software Defined Networks. IEEE, 9.
[11] Mehmet Necip Kurt, O. O. (2018). Online Cyber-Attack Detection in Smart Grid: A Reinforcement Learning Approach. IEEE, 12.
[12] Grant, D. (2018). Distributed Detection and Response for the Mitigation of Distributed Denial of Service Attacks. IEEE, 3.
[13] Yaokai Feng, H. A. (2018). Feature Selection For Machine Learning-Based Early Detection of Distributed Cyber Attacks. IEEE, 8.
[14] Yalda Khosroshahi, E. O. (2019). Detection of sources being used in DDoS attacks. IEEE, 6.
[15] Manuel Lopez-Vizcaino, F. J. (2019). Early Intrusion Detection for OS Scan Attacks. IEEE, 5.
[16] Zakira El Mrabet, P. R. (2019). Data Injection Attack in home Area Networks During ANN. IEEE, 8.
[17] Zhang, F. (2019). Multi-Layer Data-Driven Cyber-Attack Detection System for Industrial Control Systems Based on Network, System, and Process Data. IEEE, 8.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)