A SURVEY ON MACHINE LEARNING TECHNIQUES FOR DETECTION OF CYBER-ATTACK AND PERPETRATOR PREDICTION

[1]Dr. M. Shanmugapriya, [2] Dr. N. P. Revathy , [3] Mr. V.Suresh Kumar

Associate professor,Department of Computer Science,Kongu Arts and Science College (Autonomous) Erode

Associate Professor,Department of Computer Applications ,Gobi Arts and Science College (Autonomous) Gobichettipalayam

Head of the Department,Department of Computer Applications,Shree Venkateshwara Arts and Science College, Gobi

Abstract

Cyberspace has grown as a result of the widespread usage of mobile apps and the Internet. Cyberspace is seeing an increase in long-term, automated cyberattacks. Cybersecurity strategies improve security systems to identify and thwart attacks. Because hackers are now skilled enough to circumvent conventional security measures, the security mechanisms that were previously in place are no longer adequate. Unknown and polymorphic security attacks are difficult for traditional security methods to identify. In many applications related to cyber security, machine learning (ML) techniques are essential. Even But there are still a lot of obstacles to overcome before ML systems can be considered reliable. Numerous malevolent adversaries with financial motives are prepared to take advantage of these ML vulnerabilities in cyberspace. By reviewing the literature on machine learning (ML) techniques for cyber security, including intrusion detection, spam detection, and malware detection on computer networks and mobile networks over the past ten years, this paper seeks to provide a thorough overview of the difficulties that ML techniques face in defending cyberspace against attacks. Along with regularly used security datasets, critical machine learning tools, assessment measures for assessing a classification model, and concise explanations of all machine learning techniques, it offers more. Lastly, the difficulties in implementing machine learning methods for cyber security are examined. The most recent comprehensive bibliography and the most recent developments in machine learning for cyber security are presented in this paper.

Keywords--- Cyber security, intrusion detection, malware, machine learning, spam.

I. INTRODUCTION

More and more people are using the Internet to access online information and services. The number of people utilising the Internet is increasing quickly; 48% of people worldwide utilised the Internet to obtain information in 2017 [1]. In developed nations, this percentage rose to 81% [2]. Transferring data across a network between nodes is the main function of the Internet. The Internet is a global network of millions of different computers, networks, and other devices. The use of the Internet has increased dramatically as a result of developments in computer systems, networks, and mobile devices. Cybercriminals and adversaries have therefore turned their attention to the Internet [3].

Data confidentiality, availability, and integrity must all be guaranteed via a reliable and secure computer system. When an unauthorised person or piece of software gains access to a computer or network with the purpose to destroy it or interfere with regular operations, the system's security and integrity are jeopardised [4]. The collection of security measures that can be put in place to guard user assets and cyberspace against invasions and unauthorised access is known as cybersecurity. A cyber defence system's primary goal is to ensure that data is private, necessary, and accessible [5].

A nation's national defence determines its integrity. Security features that restrict data access to authorised users are built into (or ought to be built into) computer networks. In January 2008,

the Bush Administration launched the Comprehensive National Cyber Security Initiative (CNCSI) [6].

The initiative sought to increase awareness of a number of concerns, such as identifying and addressing vulnerabilities, detecting new and emerging cyber security risks, and catching criminals attempting to access secured federal information systems. President Obama went on to say that "America's economic prosperity in the 21st century will depend on cyber security" and that "the cyber threat is one of the most serious economic and national security challenges we face as a nation." [7].

It is imperative to bring attention to the Estonian cyberattack of 2007. For three weeks, several journalistic, educational, and financial websites in Estonia were affected [8]. The NATO Bucharest Summit Declaration focused on the first cyberwar. 2008 saw the announcement of NATO's cyber defence strategy [9].

Computer systems and networks are vulnerable to threats and cyberattacks due to inherent and internal weaknesses in their configuration and functioning. Inadequate protocols, staff with little education or expertise, and improper configuration are some of the vulnerabilities that might arise when constructing a computer network system. Threats and attacks from both inside and outside a network are more likely to occur when certain defects are present. People in a wide range of professions are finding that cyber networks are increasingly crucial. An agent is deemed a threat using a certain penetration technique if it has unfavourable and undesired impacts on a computer or network's behaviour and functioning [10].

The goal of cyber security is to defend programs, networks, and data integrity against online attacks[11]. Cybercriminals and defenders have been engaged in a race since the first computer virus appeared in 1970 [12]. Keeping up with the speed of these cyberattacks and defending against them is becoming increasingly difficult. To solve these security issues, researchers are currently concentrating on the pressing need to develop new automated security techniques. Automated machine learning algorithms are among the best and most effective ways to identify new and unknown cyberthreats [13].

Both the cyber security and the attacker sides are using machine learning techniques. On the criminal side, fraudsters are employing machine learning algorithms to identify system vulnerabilities and advanced attack strategies to breach the defence wall. Machine learning models are playing a crucial role on the defence side in reducing the impact and harm that occurred by offering more potent and intelligent techniques to enhance performance and early attack detection [14]. Combining machine learning methods improves the accuracy of early and accurate assault classification [15]. However, an insufficient dataset is used in the great majority of the investigations. A thorough and integrated analysis of cyberthreats and attacks on computer networks and mobile devices was absent from any of the surveys that were analysed.

II. CYBER THREATS

A potential weakness that could have a detrimental effect on computer systems or applications is the threat in the field of computer security. It could be the consequence of intentional or unintentional behaviour. The intentional events could be classified as either individual assailants or criminal organisations. On the other hand, unintentional occurrences fall into one of two categories: computer errors or natural calamities like earthquakes, fires, or tornadoes. The National Information Assurance Glossary (NIAG) defines a threat as any event or situation that has the potential to significantly affect the system or infrastructure by revealing confidential data, allowing unauthorised access, changing data, or generating a denial of service (DoS).

The CIA triad—availability, integrity, and confidentiality—is the primary security component. The definition of security is based on these three principles. There is a significant risk that the system or application in issue could

be compromised if any one of these pillars is compromised

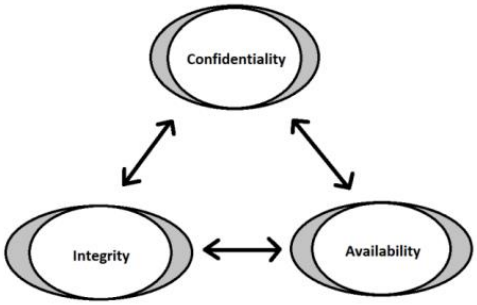

Figure 1: CIA Triad

1.1. Types of cyber threats

There are mainly 9 types of cyber threats as follows:

A) Malware

Malware refers to malicious software which is generally a file or code which is spread over the network and infects, steals any sensitive information or conducts any behaviour that the attacker wants virtually or physically. There are various types of malware shown in the figure 2.

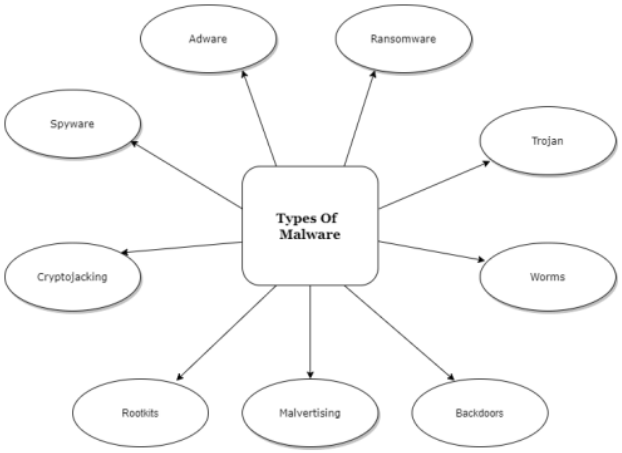

Figure 2: Types of Malware

B) Phishing

This type of social engineering assault is commonly used to acquire user data, login passwords, or credit card information. Examples of phishing techniques include voice phishing, SMS phishing, cloning, spear phishing, and email phishing.

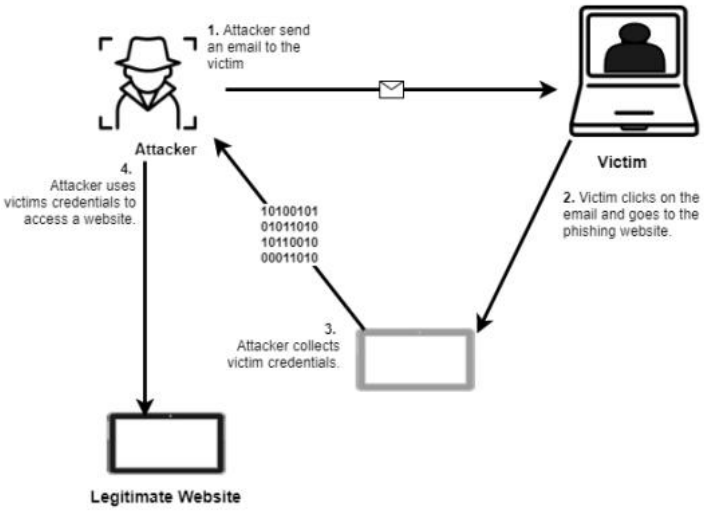

Figure 3: Phishing

C) Man in the Middle Attack

It is sometimes referred to as "monkey-in-the-middle," "person-in-the-middle," "machine-in-the-middle," and "monster-in-the-middle." As so, the attacker can control the messages that are exchanged between two individuals who believe they are chatting to each other directly. If the transmission is not encrypted, an attacker can change the message or get credentials by utilising HTTP instead of HTTPS.

.

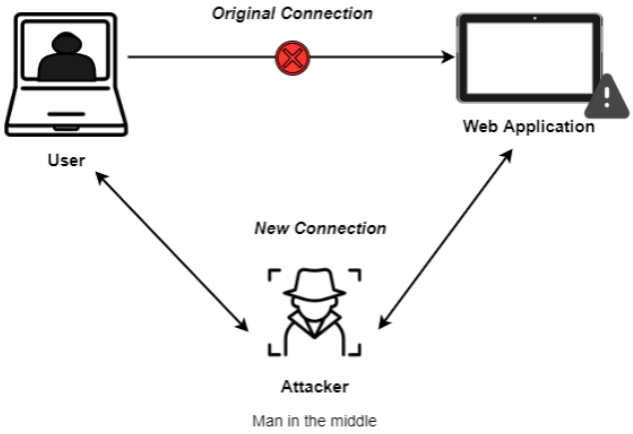

Figure 4: MITM (Man-in-the-middle)

D) Denial of Service Attack

E) It prevents authorised users from accessing the network or computer. In this case, the attacker overloads the server with requests, causing it to crash, preventing the legitimate user from accessing it.

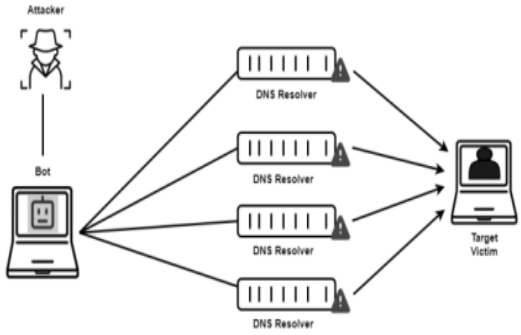

Figure 5: DOS (Denial of Service)

F) SQL injection

This web security vulnerability allows the attacker to alter the SQL queries that different applications send to the database. This risk allows the attacker to read or obtain data from the database.

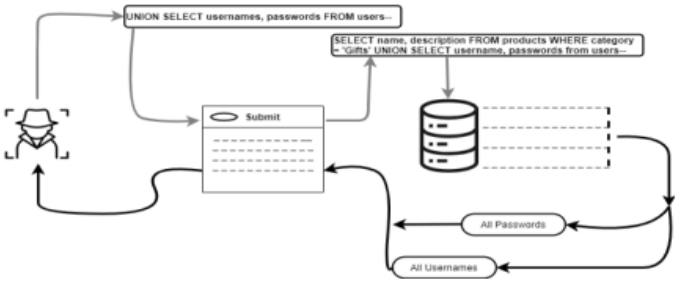

Figure 6: SQL Injection

G) Zero-day Exploit

This is the threat that is unknown and the patch against it is not developed yet. Until the mitigation is developed hackers can exploit it and can take the advantage of this threat.

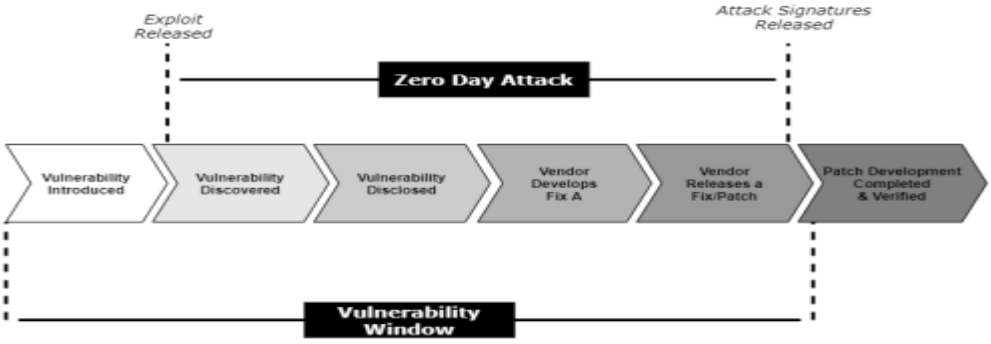

Figure 7: Zero-day Exploit Cycle

H) Advanced Persistent Threat

This is done by groups such as nation-state or state sponsored for gaining unauthorised access to networks or systems. Also, they remain undetected for an extended period.

I) Ransomware

Ransomware is a type of malware that encrypts a user's personal data. It blocks the access until the ransom is not paid. The attacker asks for the money for the decryption of the data.

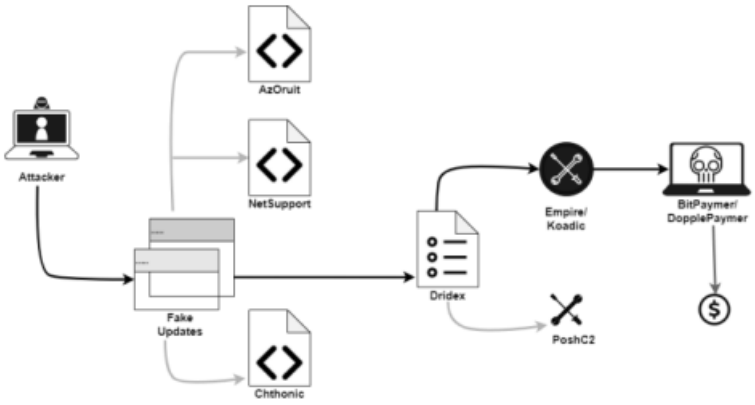

Figure 8: Ransomware

J) DNS Attack

DNS means Domain Name System which resolves domain names into the specific IP address which is associated with it. In this threat, the attacker takes advantage of a vulnerable domain name system (DNS). There are various types of DNS threats such as domain hijacking, DNS flood attack, DNS tunnelling etc.

III. LITERATURE SURVEY

Cyberattack detection is a widely used technique for attack mitigation. It involves responding to an anomalous connection in order to report the presence of an attack pattern or profile in a network. One of the most important methods for detecting cyberattacks is intrusion detection. The method of identifying an attack or intrusion signature in a continuous network flow is known as intrusion detection [16]. To find invasions, intrusion detection systems are employed. Intrusion detection systems come in three different varieties. These consist of misuse-based (signature-based), hybrid, and anomaly-based detection methods, in that order. While abuse detection considers the signatures of known attacks to help with intrusion detection, anomaly detection examines profiles of normal network activity to identify intrusions where a deviation from the regular profile is observed. Combining the two approaches results in a hybrid strategy [17].

Numerous works on cyberattack detection are in the public domain. However, most of these techniques have not been able to detect attacks, and some have resulted in the overuse of computer resources. Similarly, most of the approaches presented in the corpus of current research are merely theoretical marvels and not computationally practical. Later sections will discuss more accessible cyberattack detection methods and analyse the methodology, benefits, and drawbacks of each tactic.
Machine learning techniques for detecting cyberattacks have become more and more common in recent years. The main tasks of machine learning algorithms are to classify and predict whether or not a taught instance would exist using training data, and machine learning is

excellent at evaluating data and predicting the outcomes of particular events based on the sample inputs that are available [18]. In the present cyberattack detection scenario, the accuracy of the detection process has significantly risen with the use of machine learning.

A. Cyber-attack Prevention Approaches

Cyber-attack detection and cyber-physical system prevention are recommended by Nutjahan et al. [19]. The fuzzy logic-based attack classifier (FLAC) and the Chi-square detector were used to identify fraudulent data injection and distributed denial of service attacks. Examples of fuzzy features used to choose the attacks on the list include activity profiling, average packet rate, change point detection algorithm, cusum algorithm, user sessions that haven't expired, injected incomplete information, and session key reuse. An example scenario has been created using OpNET Simulator. Simulation tests show that FLAC and the Chi-square detector are capable of accurately identifying the previously described cyber-physical hazards. When compared to the existing fuzzy logic-based attack detector, the proposed model performs better than the traditional distributed denial of service and false data detectors.
A reinforcement learning-based solution called RLXSS is provided by Fang et al. [20] to enhance the XSS detection model and offer protection against hostile attacks. The detection model's adversarial samples are mined first by the reinforcement learning-based adversarial attack model. Next, alternating training is applied to the adversarial model and the detection model. After every iteration, the newly identified adversarial examples—which are classified as malicious samples—are used to train the detection model. Experimental results show that the proposed RLXSS model can effectively mine adversarial samples that avoid black-box and white-box detection while retaining aggressive features. Additionally, by training the confronting assault and detection models alternatively, the detecting model's escape rate is continuously reduced. This implies that the detection model has the potential to improve its defences against intruders.

According to Ganesh et al. [21], phishing attacks are the most straightforward way to gather personal information from unintended victims. Phishers aim to get private information, including bank account details, usernames, and passwords. Cyber security experts are currently searching for dependable and consistent ways to identify phishing websites. This article describes how to use machine learning algorithms to differentiate between real and fraudulent URLs. It extracts and examines a number of features of both kinds of URLs. Phishing websites are identified using algorithms such as Random Forests, Decision Trees, and Support Vector Machines. The goal of the paper is to detect phishing URLs and determine the optimal machine learning technique by assessing the accuracy, false positive, and false negative rates of each algorithm.

According to Jhons and colleagues, one of the most prevalent types of attacks on online applications is cross-site scripting (XSS), which information security must consider. [22]. The attacker must insert the malicious code inside the web application for it to run on the user's browser. This code is typically JavaScript. The ability of a web application to identify dangerous scripts is a crucial part of its protection. This study investigates the development of classifiers for JavaScript code that use Random Forests, SVM, and k-NN to identify and prevent certain attacks, whether or not they are known. When engaging feature sets that combine linguistic and behavioural information are utilised, it has been shown that classifiers can achieve high accuracy and precision on large real-world data sets without concentrating only on obfuscation.

Manjeet Rege et al. [23] assert that by facilitating information acquisition, heuristic learning, choice trees, and numerical models for choosing, machine learning techniques offer the benefits of solidity, controllability, and discernibleness. In a clinical setting, updating is typically as simple as downloading the new patient's data.
Bharati et al. [24] claim that by offering initial phase indications, ML models can help clinical specialists detect human illness. According to Marsland et al. [25], machine learning (ML) may be a branch of artificial intelligence that advances the notion that machines can learn by applying themselves the optimal method to tackle a specific problem by providing them with access to reliable data. By providing sophisticated numerical and factual models, machine learning (ML) enables machines to carry out academic tasks and develop opinions on their own without relying on the traditional methods that people usually use. The field of system administration has benefited greatly from the use of machine learning to automate complicated procedures, such as projecting the plans and operations of communication networks onto computers. System management domains have effectively adopted machine learning techniques including interruption discovery, as suggested by Buczak et al. [26], and intellectual radios, as suggested by Bkassiny et al. [27]. The investigation concentrated on machine learning for optical system management in the midst of many other system administration domains.

Due to their many successful attributes, such as decreased cost, high limit, and unquestionably more, Mukherjee et al. [28] recommended that optical firms navigate the fundamental physical infrastructure for all major organisation providers worldwide. DeCusatis [29] and Song et al. [30] suggested that it would also appear as datacom in the big telecom shows in the not-too-distant future, making it the entry component that has the best potential of being replaced by another optional innovation.
A learning model based on the correlation between the aim worth and the ratings of the indicator traits was proposed by Silva et al. [31]. It's crucial to consider how the course may make use of previously published academic content. Grouping difficulties like administered learning are mentioned by ML. As a result, it is essential to provide a test informational index from which the classification should be selected, together with an information collection that includes examples of known classes.

According to Gao et al. [32], the success of characterisation is greatly influenced by the calibre of the data utilised for learning in connection to the kind of machine learning method employed. As is the case with many other contemporary applications, it is typical to expect dishonest clients seeking loans or those who categorise mangoes as lucky or unlucky when grouping approaches are employed. The most obvious type of characterisation challenge is the paired arrangement, where the objective has two acceptable estimates—yes or no, positive or negative, etc. Several methods, including the lift bend, the disarray framework, and collector administrator qualities, are used to estimate the exhibition of arrangement.
Based on their boundary values, Osisanwo et al. [33] came to the conclusion that each ML computation requires a unique learning strategy. The grouping precision for each scenario changes drastically when the order problem is varied by a computation and changing border layouts. Getting reliable boundary estimates for the calculations is the main goal of machine learning (ML), which aids in identifying the optimal solution to the design problem, including the exhibition measurements. Therefore, the boundaries of the calculation must be balanced and consistent with the problem that needs to be resolved. Among the methods to improve are

PSO and search tactics. The primary objective of the analysis is to modify the calculation bounds by using the format of the inquiry technique.

In order to investigate a user's multiple identities and determine whether synthetic identity theft has taken place, Veena and Meena [34] used three different forms of data: input dataset (X), normal dataset (Y), and target dataset (Z).

The practice of predicting the possibility of an attack on a dynamic, regulated network environment is known as cyber-attack prediction. Enhancing the security capabilities of defence systems in cyberspace is the primary objective of cyberattack (intrusion) prediction, according to [35]. GhasemiGol and Ghaemi-Bafghi introduced the E-correlator, an entropy-based alert correlation system, in [36] to make it easier to analyse a big set of warnings without losing any information between the correlated and original raw alerts. Raw alerts are sent to the E-correlator system, which generates a hyper-alerts graph. The density-based spatial clustering of applications with noise (DBSCAN) technique is used to accomplish this. There are several advantages to grouping related alerts into certain clusters using the DBSCAN technique. These include detecting noise or outliers in the data set, successfully locating clusters that are produced at random, and avoiding predetermining the number of clusters in the data. With a log linear processing cost of O(n log n), the suggested model is likewise incredibly quick for a dataset this size. The E-correlator system's effectiveness is probably limited by its failure to account for other intrusion sources, such as flaws in the host's applications, services, or protocols. As a result, the warning correlation and clustering method is not applicable to the prediction of multistage attacks. However, the DBSCAN approach is sensitive to input parameter values and vulnerable to weak cluster descriptors, despite its resistance to noise and outliers.

The approach of [37] builds an attack tree from important episodes that span an episode window in order to simulate attack prediction. They achieved a 95% accuracy rate in both scenarios by modelling assault scenarios, which included the detection and prediction of multistage attacks, and by constructing an attack tree. The attack tree architecture can yield a definite result and is easy to use and comprehend. The decision-making process of the attacker can be modelled using attack trees. This is accomplished by building a tree, where the root node represents the attacker's objective and the leaf nodes represent the different routes that can be taken to get there [38]. Rebuilding attack plans with an attack tree provides a coherent, well-structured view of the events that preceded the attack. Attack trees are helpful for determining the purpose of an attack or specific security issue since they link undesirable events to their most likely causes.
One of the main issues with this strategy is the amount of time needed to build assault trees. However, because only the modelled attack plans in the library may be utilised, the method is less scalable for large networks when attack trees are used. In [24], a hybrid method for anomaly intrusion detection using a prediction module is examined. The frequency of network anomalies, which can overwhelm the network server to the point of depleting its available computational resources, including memory, processors, data structures, and storage, is a crucial element of multistage attacks. The suggested method combines data mining methods like the radial basis kernel function (RBF) of the support vector machine (SVM) with the k-means clustering algorithm. By reducing the number of attributes linked to each data point, the RBF kernel function is utilised for classification on the KDDCup'99 dataset in an effort to improve accuracy and detection rate. Feature selection creates a subset of training data from the original feature space. In this case, feature selection's primary goal is to reduce the

computational burden of using the dataset's whole feature space. To accurately forecast events in the simulated attack space, distinct attributes were chosen for every kind of attack. The results demonstrated that the hybrid strategy outperformed the support vector machine (SVM) and k-means clustering technique when all 41 features of the KDDCup'99 dataset were used. The accuracy of the hybrid technique was 80.28.89% for all attack classes, while the accuracy of the k-means and SVM approaches was 73.24% and 49.3%, respectively. Furthermore, the accuracy for DoS attacks was high, up to 93.33%, in contrast to the k-means and SVM techniques, which had accuracy rates of 86.67% and 40%, respectively. With a substantially lower false alarm rate, the hybrid approach demonstrated an accuracy of 87.01% for all attack classes and 100% for DoS for a chosen feature space. The outcomes show how successful the hybrid strategy suggested in [38]

B. Cyber-attack Prevention Approaches

Attack prevention is a proactive procedure that quickly identifies and resolves potential network threats. Preventing cyberattacks is essential to the procedure. Most detection methods are reactive, which means they are only applied after the impact zone has been severely damaged. To improve cyberspace security, a variety of intrusion prevention systems (IPSs) have been introduced.
Patil and Meshram [39] addressed DoS attack variants such flooding, flooding with IP spoofing, and ping of death attacks in their discussion of a technique for preventing network invasions. The method is modelled as platform neutral using the Java virtual machine (JVM). The Linux iptables command is used to prevent malicious traffic from entering the internal network, and the packet sniffer is created using the Jpcap package. Before utilising the Jpcap library, you must install the winpcap (for Windows) and libpcap (for Unix or Linux) libraries. By examining incoming packets that were captured using Jpcap in promiscuous mode, assaults are prevented in this case. When packets are inspected, the SYN flag is set, and the packet refers to the same destination address over a continuous network traffic flow, the system assumes a SYN flood assault. The specifics of the detected assault are contained in the log file. The packet is then dropped using the net-filter (Windows) or iptables (Linux) commands. All flag attacks, XMAS attacks, SYN-FIN attacks, fraggle attacks (UDP packets), and smurf attacks (ICMP packets) can also be prevented using the recommended technique. The technique offered a quick attack prevention solution, even if it was highly dependent on iptables rules. Furthermore, if a rule-match method does not detect such an assault in a timely manner, it might still penetrate the network and cause significant damage to internal network resources. Numerous assault types and their variations, as well as strategies for neutralising them, have been covered in this book. Nonetheless, one of the most elusive attack types in cyberspace is Distributed Denial of Service (DDoS) flooding, which employs botnets, sometimes referred to as an attack army, to disrupt services provided to authorised users of a system or network. Botnets are commonly used to distribute malicious packets across the Internet to a large number of machines, sometimes on a global scale, by exploiting security defects, also called vulnerabilities, in computers [40].

These botnets are made up of masters, handlers, and bots, which are the agents that spread the distorted packets required for a successful DDoS attack. Attackers that utilise handlers to communicate with agents or bots are known as masters. The attackers use zombies to provide command and control. Zombies are previously compromised PCs that occasionally compromise other vulnerable computers along the assault path as part of the attack army. This

allows the attack to intensify until all computing resources are completely disabled, at which point significant and irreversible damage can be done.

It has been a difficult task to defend against DDoS attacks. Ideally, hundreds of thousands of computers connected to Internet-enabled networks, together with additional devices like cellphones and personal digital assistants (PDAs), should have all susceptible services and ports disabled. However, these vulnerable ports and services come from unpatched systems, for which most security updates sent to devices through proxy servers are not applied when they ought to be. Because of this, there are a lot of unpatched and unprotected machines that botnets with command and control (C & C) skills can employ to initiate a DDoS flooding attack.
Consequently, [40] claims that the use of techniques such source address authentication, capabilities, and filtering methods is essential for thwarting DDoS flooding attacks. In a similar vein, Internet service providers could collaborate to prevent and shorten such attacks by leveraging technologies like cloud computing and the Internet of Things. In this regard, the close proximity of the Internet is a major benefit. Additionally, although the classification has considered a wide range of DDoS attack sources and results, little attention has been paid to the correlation of alerts, which could be used to determine the origin of the assault given a large number of examples that represent the attack. When flooding attacks are quantified in terms of the amount of traffic generated without utilising the unofficial links between such traffic instances, it can be difficult to pinpoint the attack source in real time.
There have been suggestions for cloud-based solutions in connection with defences against cyberattacks. In [41], one such technique, SnortFlow, was proposed. It provides an intrusion prevention system for cloud environments based on OpenFlow. One of the key benefits of this technology is its ability to immediately alter the cloud networking system as a defence when an assault is detected.

To implement the IPS, the authors modelled the system to include the controller, the cloud cluster, and OpenFlow switches. In the proposed system, cloud resources are hosted by the cloud cluster, which is based on the parallel virtualisation technology XenServer. The resources at different cloud servers are then connected by OpenFlow switches (OFS), and different physical cloud servers provide layer-2 connectivity and other cutting-edge technologies. The controller stays in the centre of the architecture in order to further exert control or view over the OpenFlow-enabled infrastructure.

Instead of reacting immediately to suspicious traffic, the entire cloud environment is redesigned to prevent intrusions in order to improve the efficacy of the strategy. This is done using the network programmability feature of the OpenFlow switch (OFS) and Open vSwitch (OVS). Some countermeasures that can be used to protect the network include port blocking, quarantine, media access control (MAC) and Internet protocol (IP) address changes, traffic redirection and isolation, and deep packet inspection.

The data evaluation indicates that SnortFlow performs better since it inherits both Snort's intrusion detection capability and OpenFlow's highly network reconfigurable nature. Because testing have shown a maximum performance barrier of 2500 packets and a tendency to delete packets when performance surpasses this threshold, it is unknown if SnortFlow would work properly for high-speed packets under different deployment scenarios. For this paradigm to work in real-time environments, it must be enhanced. Using several controller systems to provide commands to numerous OFS and OVS simultaneously is one such enhancement.

[42] recommends a software-defined intrusion prevention system, or SDNIPS, to prevent cloud-based attacks. This detection-based approach combines a Snort-based intrusion detection system with Open vSwitch (OVS). Since the SDNIPS architecture has been greatly simplified, cloud resources are now the source of the traffic that passes via the SDNIPS agent. Any matches are reported as alerts and put to the log file once the traffic is compared to the Snort rules. This alarm data is then captured by the SDNIPS daemon and sent to the JSON server of the controller. During processing, the alert interpreter parses the alert data and extracts the relevant information, including the TCP port, source and destination IP addresses, and attack type. As the alert data is processed further, the OVS updates the flow table using the OpenFlow rules entries from the rules generator. Any suspect traffic that fits the updated flow table entries is then subjected to the proper countermeasures in the data plane. In this way, an attack can be prevented and the cloud's resources can be protected. Even if the approach demonstrates a successful preventive system, using Snort permits total reliance on specialised knowledge for rule definition, which can be time-consuming. However, the approach is likely to result in a higher rate of computational resource consumption because traffic must always pass through the IPS and the host system's resources would be significantly influenced by the delay in matching each traffic pattern against the pre-established criteria.

As businesses' security needs increase, more and more dependable solutions are required to protect the large resource space. One method to have a workable security solution is to have a strategy or product that is scalable, flexible, and reasonably priced. [43] emphasises on this in their proposed real-time approach to detect and prevent assaults. The technique, which was developed based on the software engineering framework, uses requirement analysis, design, implementation, and testing to configure Snort in inline mode to achieve intrusion prevention. The intrusion prevention system (IPS) can use its sensors to identify and reject suspicious packets that might include attack payloads when Snort is set up in inline mode. The dropped packets are eventually logged using Splunk. Nevertheless, a major drawback of this approach is that signature-based intrusion detection and prevention systems, such as Snort, perform poorly during periods of high network traffic and are unable to detect unanticipated attacks.

IV. INFERENCE FROM EXISITNG WORKS

The literature assessment that cyberattacks and crimes are worthy of more research since they seriously hurt both individuals and governments. We employed machine-learning techniques in our investigation to find out which regions used them and how well they performed in making predictions. Significant contributions to the literature were made by the research, especially to the criminal units conducting the investigations. These studies frequently use attacks, cybercrimes, and general crimes as datasets. A machine learning-based model utilising the dataset of our study is advised because the actual dataset based on human qualities is examined to a lesser extent. Because of the significance of the areas being investigated, the cyber-attack and perpetrator estimating approach is addressed.

V. CONCLUSION

Because security technology have advanced to detect and respond to threats, cybersecurity has become a global issue. Due to their inability to identify polymorphic and unidentified threats, the conventional security technologies that were previously in use are no longer adequate. In many applications of cyber security systems, machine learning techniques are essential. According to our research, there has been a notable increase in corporate and scholarly interest in machine learning and cyber security, especially in the past ten years, which has led to an increase in publications. The safe application of machine learning methods in cyberspace to

offer certain high-level correctness assurances rather than focussing on model accuracy and performance is known as trustworthy machine learning.

VI. REFERENCES

1. ICT Fact and Figures 2017. Accessed: Jun. 1, 2020. [Online]. Available: https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ ICTFactsFigures2017.pdf
2. ICT Facts and Figures, International Telecommunication Union. (2017). Telecommunication Development Bureau. [Online]. Available: https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx (accessed Oct. 09, 2019).
3. Naseer, S., Saleem, Y., Khalid, S., Bashir, M.K., Han, J., Iqbal, M.M. and Han, K., 2018. Enhanced network anomaly detection based on deep neural networks. IEEE access, 6, pp.48231-48246.
4. V. Ambalavanan, ‘‘Cyber threats detection and mitigation using machine learning,’’ in Handbook of Research on Machine and Deep Learning Applications for Cyber Security. Hershey, PA, USA: IGI Global, 2020, pp. 132–149.
5. T. Thomas, A. P. Vijayaraghavan, and S. Emmanuel, ‘‘Machine learning and cybersecurity,’’ in Machine Learning Approaches in Cyber Security Analytics. Singapore: Springer, 2020, pp. 37–47. [Online]. Available: https://link.springer.com/chapter/10.1007/978-981-15-1706-8_3
6. The Comprehensive National Cybersecurity Initiative. Accessed: Jun. 1, 2020. [Online]. Available: https://obamawhitehouse. archives.gov/issues/foreign-policy/cybersecurity/national-initiative
7. The White House, Remarks by APHSCT Lisa O. Monaco at the International Conference on Cyber Security. Accessed: Oct. 17, 2019. [Online]. Available: https://obamawhitehouse.archives.gov/thepress-office/2016/07/26/remarks-aphsct-lisa-o-monaco-internationalconference-cyber-security
8. 10 Years After the Landmark Attack on Estonia, Is the World Better Prepared for Cyber Threats? Accessed: Jun. 1, 2020. [Online]. Available: https://foreignpolicy.com/2017/04/27/10-years-after-the-landmarkattack-on-estonia-is-the-world-better-prepared-for-cyber-threats/
9. North Atlantic Treaty Organization. (Apr. 3, 2008). Bucharest Summit Declaration. Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Bucharest. Accessed: Oct. 9, 2019. [Online]. Available: https:// www.nato.int/cps/en/natolive/official_texts_8443.htm
10. Figueira, P.T., Bravo, C.L. and López, J.L.R., 2020. Improving information security risk analysis by including threat-occurrence predictive models. Computers & Security, 88, p.101609.
11. Kosseff, J., 2017. Defining cybersecurity law. Iowa L. Rev., 103, p.985.
12. Li, M.Q., Fung, B.C., Charland, P. and Ding, S.H., 2021. I-MAD: Interpretable malware detector using galaxy transformer. Computers & Security, 108, p.102371.
13. Rhode, M., Burnap, P. and Jones, K., 2018. Early-stage malware prediction using recurrent neural networks. computers & security, 77, pp.578-594.
14. K. Geis, ‘‘Machine learning: Cybersecurity that can meet the demands of today as well as the demands of tomorrow,’’ Ph.D. dissertation, Master Sci. Cybersecur., Utica College, Utica, NY, USA, 2019.
15. M. Thangavel, A. S. TGR, P. Priyadharshini, and T. Saranya, ‘‘Review on machine and deep learning applications for cyber security,’’ in Handbook of Research on Machine and Deep Learning Applications for Cyber Security. Hershey, PA, USA: IGI Global, 2020, pp. 42–63.
16. N. B. Aissa and M. Guerroumi, “Semi-supervised statistical approach for network anomaly detection”, Procedia Computer Science, vol. 83, (2016), pp. 1090-1095.
17. Sarvari, S., Sani, N.F.M., Hanapi, Z.M. and Abdullah, M.T., 2020. An efficient anomaly intrusion detection method with feature selection and evolutionary neural network. IEEE Access, 8, pp.70651-70663.
18. A. L. Buczak and E. Guven, “A survey of data mining and machine learning methods for cyber security intrusion detection”, IEEE Communications Surveys & Tutorials, vol. 18, no. 2, (2016), pp. 1153-1176.
19. Nurjahan, F. Nizam, S. Chaki, S. Al Mamun and M. S. Kaiser, ”Attack detection and prevention in the Cyber-Physical System,” 2016 International Conference on Computer Communication and Informatics (ICCCI), 2016, pp. 1-6, d

20. Fang, Y., Huang, C., Xu, Y., & Li, Y. (2019). RLXSS: Optimizing XSS detection model to defend against adversarial attacks based on reinforcement learning. Future internet, 11(8), 177.
21. Ganesh, V., Shastrakar, K., Sulakhiya, A., Satange, S., Dhurat, J., & Miralwar, N. (2023). Phishing Website Detection Using Machine Learning.
22. Johns, M., Engelmann, B., & Posegga, J. (2008, December). Xssds: Server-side detection of cross-site scripting attacks. In 2008 Annual Computer Security Applications Conference (ACSAC) (pp. 335-344). IEEE.
23. Rege M., Mbah R. B. K. Machine Learning for Cyber Defense and Attack. Proceedings of the Data Analytics: The Seventh International Conference on Data Analytics; November 2018; Athens, Greece. pp. 73–78.
24. Bharati A., Sarvanaguru R. A. Crime prediction and analysis using machine learning. International Research Journal of Engineering and Technology . 2018;**5**(9):1037–1042. [Google Scholar]
25. Marsland S. Machine Learning: An Algorithmic Perspective" . FL, USA: CRC Press; 2015. pp. 1–430.
26. Buczak A. L., Guven E. A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials . 2016;**18**(2):1153–1176. doi: 10.1109/comst.2015.2494502. [CrossRef] [Google Scholar]
27. Mahesh, B., 2020. Machine learning algorithms-a review. International Journal of Science and Research (IJSR).[Internet], 9(1), pp.381-386.
28. Mukherjee. Optical WDM Networks" . Berlin, Grermany: Springer Science & Business Media; 2017. [Google Scholar]
29. DeCusatis C. Optical interconnect networks for data communications. Journal of Lightwave Technology . 2014;**32**(4):544–552. doi: 10.1109/jlt.2013.2279203. [CrossRef] [Google Scholar]
30. Musumeci, F., Rottondi, C., Nag, A., Macaluso, I., Zibar, D., Ruffini, M. and Tornatore, M., 2018. An overview on application of machine learning techniques in optical networks. IEEE Communications Surveys & Tutorials, 21(2), pp.1383-1408.
31. Beretta, L. and Santaniello, A., 2016. Nearest neighbor imputation algorithms: a critical evaluation. BMC medical informatics and decision making, 16(3), pp.197-208.
32. Shah, S.H., Iqbal, M.J., Ahmad, I., Khan, S. and Rodrigues, J.J., 2020. Optimized gene selection and classification of cancer from microarray gene expression data using deep learning. Neural Computing and Applications, pp.1-12.
33. Osisanwo F. Y. Supervised learning algorithms: classification and comparisons. International Journal of Computer Trends and Technology . 2017;48(3):128–132. [Google Scholar]
34. Veena K., Meena K. Determination of performance to verify the synthetic identity theft by training the neural networks; Proceedings of IEEE International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM) ; August 2017; Chennai, India. pp. 246–250.
35. W. Xing-zhu, "Network Intrusion Prediction Model based on RBF Features Classification", International Journal of Security and Its Applications, vol. 10, no. 4, (2016), pp. 241-248.
36. M. Ghasemi Gol and A. Ghaemi-Bafghi, "E-correlator: an entropy-based alert correlation system", Security and Communication Networks, vol. 8, no. 5, (2015), pp. 822-836.
37. A. A. Ramaki, M. Amini and R. E. Atani, "RTECA: Real time episode correlation algorithm for multistep attack scenarios detection", Computers & Security, vol. 49, (2015), pp. 206-219.
38. U. Ravale, N. Marathe and P. Padiya, "Feature selection based hybrid anomaly intrusion detection system using K means and RBF kernel function", Procedia Computer Science, vol. 45, (2015), pp. 428- 435.
39. S. Patil and B. B. Meshram, "Intrusion Prevention System", International Journal of Emerging trends in Engineering and Development, vol. 4, no. 2, (2012), pp. 577-584.
40. Vishwakarma, R. and Jain, A.K., 2020. A survey of DDoS attacking techniques and defence mechanisms in the IoT network. Telecommunication systems, 73(1), pp.3-25.
41. Chi, Y., Jiang, T., Li, X. and Gao, C., 2017, March. Design and implementation of cloud platform intrusion prevention system based on SDN. In 2017 IEEE 2nd international conference on big data analysis (ICBDA) (pp. 847-852). IEEE.
42. Shaghaghi, A., Kaafar, M.A., Buyya, R. and Jha, S., 2020. Software-defined network (SDN) data plane security: issues, solutions, and future directions. Handbook of Computer Networks and Cyber Security: Principles and Paradigms, pp.341-387.
43. Bocu, R. and Iavich, M., 2022. Real-Time Intrusion Detection and Prevention System for 5G and beyond Software-Defined Networks. Symmetry, 15(1), p.110.