Prevention and Detection of Network Attacks: A Comprehensive Study

1st Ryan Freas
Dept of Math and Computer Science
Augustana College
Rock Island, Illinois
ryanfreas19@augustana.edu

2st Elnatan Mesfin Tesfa
Dept of Math and Computer Science
Augustana College
Rock Island, Illinois
elnatanmesfintesfa20@augustana.edu

3st Max Sellers
Dept of Math and Computer Science
Augustana College
Rock Island, Illinois
maxsellers20@augustana.edu

4st Paul Addai
Dept of Math and Computer Science
Augustana College
Rock Island, Illinois
pauladdai19@augustana.edu

***Abstract*—Cybersecurity is currently a topic of utmost significance in tech sectors. The ever evolving landscape of this field makes it particularly difficult to navigate. This paper aims to help the reader understand the complexity of network attacks and also show how we may never 'solve' the problem of cyber attacks. Our paper may be accessible to the layman, but a basic understanding of networking fundamentals would be desirable. The words computer security, cybersecurity, or information technology security may all be used interchangeably throughout the paper. An 'attack' will refer to a breach in security to an online system that may cause (but is not limited to) the following: unauthorized information disclosure, theft of technology, or disruption of services.**

***Index Terms*—cybersecurity, network, system, attack, security**

I. Introduction

The field of cybersecurity has become more and more important in recent years due to our increasing dependence on modern technology; having a deep understanding of the prevention and detection of cyber attacks is crucial due to how data is being used in this modern era. Network connects and controls almost everything around us, including the internet of things (IoT), self-driving cars, social media, payments, etc. Ensuring data privacy, system integrity, and protecting large networks that can host millions of people are all things that fall under the branch of cybersecurity. From shutting down a power grid to disrupting air trafficking systems, one small breach in a network can have worldwide repercussions. This is why network security is so heavily studied. This field is changing so rapidly that it is no longer sufficient for a consumer to pay for software to protect their computer. Rather, it is necessary to start buying subscriptions that constantly update to protect against any new threats that may emerge. Preventing and detecting network attacks can be costly but very important since a breach in a network system can allow hackers to take over the systems which can cause harm to both the company and the customers. The data and scientific literature available about the topic of cybersecurity is continuously being updated and expanded upon. Previous research in the field of cybersecurity offers a comprehensive view of the many different types of attacks that may occur, as well as a detailed analysis of the different prevention techniques at our disposal. The research also discusses what makes a computer susceptible to attacks.

II. Related Work

A research conducted by Yih-Chun Hu; A. Perrig; D.B. Johnson on network attacks focus on an attack called, "wormhole" which is challenging to safe guard. In the paper, they explained that even if the attacker has not compromised any hosts and even if every communication is valid and secret, the wormhole attack is still feasible. The wormhole attack involves the attacker capturing packets (or bits) at one point in the network, tunneling them (perhaps selectively) to another, then retransmitting them into the network from that point. In wireless networks, the wormhole attack poses a severe risk, particularly to several ad hoc network routing as shown in **??**, methods and location-based wireless security solutions. Without a technique to protect against the wormhole attack, for instance, the majority of current ad hoc network routing systems would be unable to identify routes longer than one or two hops, drastically impairing communication.

For identifying and countering wormhole assaults, they provided a generic technique termed "packet leashes" which can be implemented using the TIK protocol. [1]

Detecting and preventing network attacks can be tedious and would require some form of automation. A research paper by Tanwir Ahmad; Dragos Truscan; Jüri Vain; Ivan Porres focuses on the use of artificial intelligence. They focus on deep learning models in particular, for the purpose of detecting network attacks [2]. In their research, they provided an end-to-end early intrusion detection system to guard against network attacks before these attacks might further harm the system

that is already under attack and to avoid unplanned downtime and disruption. For assault detection, they used a deep neural network-based classifier. Instead of depending on a manual feature selection procedure like other previous systems, the neural network is trained in a supervised manner to extract pertinent characteristics from raw network traffic data. Additionally, they provided a brand-new statistic termed "earliness" to measure how quickly their suggested technique picks up on attacks. They empirically tested their strategy on the CICIDS2017 data-set (Intrusion Detection Evaluation Dataset). The outcomes demonstrated that their method worked effectively and got an overall balanced accuracy of 0.803. When put into context, this is an impressive accuracy rating.

III. Research and Findings

One of the most common forms of cyber attacks is called Distributed denial of Service attack, or a DDOS attack. A DDoS (distributed denial-of-service) attack aims to shut down a machine or a network, rendering it unavailable to its intended clients. With these attacks it is important to act quickly as the level of these attacks can increase. When these attacks spread it is hard to handle and it sometimes needs to be analyzed in order to detect. With DDoS attacks they are attacked by intruders that are either a part of the network or outside the network which creates the conflict of false "traffic," or the amount of data packets in the network.

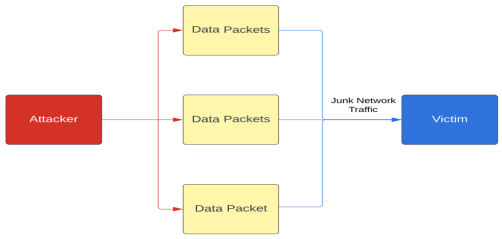

Fig. 1. Example of how DDos attack works

A. DDoS Attacks

This false traffic can be quite hard to detect and there are many different approaches to try to detect them. There are a few approaches that looked like a very interesting way to approach. Osanaiye et al. (2018) created a algorithm based on the immune system when talking about a network. Interesting parameters in the study were the speed of the detection, false alarms, and the time of detection. Another interesting algorithm was a school bus routing system which included the parameters data packet loss ratio and data packet delivery ratio. These algorithms proved to be suitable, but a different approach was found that proved to be a more optimized approach in both detection and in energy. This model was created by Suryaprabha et al (2019) and enhances security. The parameters for this algorithm include sensor devices that examines the environment of the network, a control center that collects the data, DDoS Attacker nodes that attack the improper data, nodes to capture valid data as well to make traffic easier to read, a energy monitoring unit, a unit that measures bandwidth, and a unit that detects an attacker's behavior.

This model was created by Suryaprabha et al (2019) and enhances security. The parameters for this algorithm include sensor devices that examines the environment of the network, a control center that collects the data, DDoS Attacker nodes that attack the improper data, nodes to capture valid data as well to make traffic easier to read, a energy monitoring unit, a unit that measures bandwidth, and a unit that detects an attacker's behavior.

B. Brute Force Attack

A brute force assault involves the use of trial-and-error techniques by attackers to access a target account. Depending on the circumstance, this can entail getting information like a password or personal identification number. The majority of brute force attacks are automatic, therefore there is a considerable diversity of targets, or categories of victims. Attackers can gain unauthorized access to websites that contain vital information thanks to brute force techniques. They can use this technique to entirely shut down the website or access user accounts. The Kali Linux operating system uses Patator, an application approach with a modular design and flexible structure, for brute force attacks. Attacks using the Secure Shell (SSH) and File Transfer Protocol (FTP) can be carried out using this technique. [3]

C. Cross Site Scripting

An attack known as cross-site scripting (XSS) or cross-code execution (CCE) involves an attacker putting malicious code into a victim's online application that would damage the browser of another user. XSS flaws typically give an attacker access to the user's data and the ability to perform any action the target user could perform. The attacker can manage the control of the application as a target and have complete control over the data if the target user has access within the program. [4] There are numerous XSS attack techniques. A malicious script that is executed by the target user can perform XSS. The target may be seeing a false page or a form page that contains a link and asks for the user's credentials. An XSS attack may be launched against websites that contain adverts that the target displays or against users or communities that receive malicious emails.

D. Man-in-the-middle attacks

Man-in-the-middle (MITM) attacks are a type of denial-of-service attack that target networks by monitoring communication between two connections, collecting data, or monitoring communication while enacting a variety of changes. MITM allows for the interruption of two-way communication or the creation of deceptive communication. This attack can be summed up as network packet manipulation and capture. The target and network elements' communication can be overheard

by the attacker (server, switch, router, or modem). They can intercept data packets that are freely moving via the communication network, local network, or remote network in this assault. This assault has become riskier as IoT devices become increasingly prevalent. Different strategies have been devised for the attack's detection and prediction.Intrusion detection methods based on machine learning are starting to achieve increasingly successful outcomes. [5]

E. Injection attack

By forcing a web application to execute particular commands, an attacker who uses an injection attack can affect the execution of the application. A web server may get totally compromised or have data exposed or damaged as a result of an injection attack. Such attacks are conducted by taking advantage of flaws in an application's code that permits unauthenticated user input. [6] Cross-site scripting and SQL injection are the most frequent types of injection attacks.

F. Other Network Attacks

Other network attacks was also focus on mobile ad hoc applications. The collection of mobile devices that connect to one another wirelessly, such as computers, smartphones, sensors, etc., with out a central access point creates a mobile ad-hoc network. This type of network connection is very vulnerable to a lot of different attacks [7]. These attacks includes; Black-Hole, Gray-Hole, Jellyfish, Cooperative Black-Hole, Worm-Hole, HELLO Flood, Man in Middle, etc. These indicates that there is a high probability that this type of connection is part of the top 5 most vulnerable network connections.

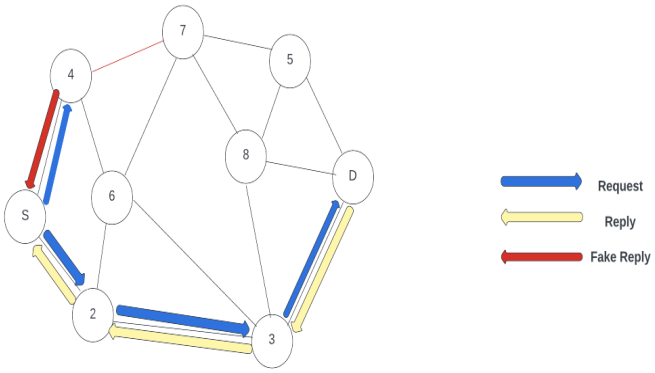

Fig. 2. Example of how Black Hole Attack works. [8]

1) Black Hole Attacks: Black Hole Attacks are one of the major attacks in the Mobile Ad Hoc Network (MANET). These attacks happen when a node consumes all of the routes in the MANET. Attackers do this by responding to request and update messages with fake replies. These attackers might add errors followed by updates to it. Tiruvakadu et al(2018) suggests a honeypot system. They created a Black Hole attack confirmation system which finds and confirms the attacks in MANET with honeypot. This honeypot system finds the type of black hole attack using a Black Hole tree and then confirms it using their Attack History Database. The Black Hole attack tree had used common symptoms for specific attacks and had observations of what they should fix given the symptoms.

2) Jellyfish Attacks: Jellyfish attacks are very similar to Black Hole attacks but instead of taking data packets it delays the packets. These attack have three subcategories: recorder attacks, period dropping attacks, and delay variance attacks. Reorder attacks are caused by using a multi-path routing method. Period Dropping sometimes happen when some nodes drop some packets at a given time. Delay Variance occurs when bad nodes create a random delay in packet transmission because they did not change the data packets order. Satheeshkumar et al (2017)

IV. AI Use in Cyber Attack Defense

Artificial intelligence seems like the most efficient defense against network breaches. This is especially due to the rapid evolution of cyber-attacks; machine learning and artificial intelligence can aid us in keeping up with all of the threats that exist today. Due to how large and complex a network can become, as well as the enormous volume of data they can contain, it is simply impossible for humans to secure and detect every single breach. Even software automation is insufficient to prevent network attacks. There are far too many viruses generated each week by many cyber-criminals around the world trying to find the next hole in a network [9]. The field of AI is also projected to increase dramatically within the next 5 years, so the effectiveness of AI in handling and preventing network breaches will increase. AI can not only help with prevention and detection of attacks, but also prediction. A network attack that would normally be invisible to human cyber-technicians can be spotted by AI instantly. This is because AI can examine behavioral patterns with ease, and therefore is able to evaluate the appearance of website traffic as either routine or hazardous and malicious. AI systems can also predict which parts of a network are the most vulnerable before they are breached [10].

V. How AI is used to Create Cyber Attacks

Although AI can be utilized in the prevention of cyber attacks, it can also be used in cyber attacks. Malicious software has only ever been produced by humans up until this point. Malicious software that can morph on its own, hide on its own, replicate on its own, and think on its own has, however, proved harder to predict. Humans may now create programs that "think" independently and may be able to assault hundreds of targets simultaneously. Future software must be capable of understanding how to evaluate all potential attack vectors, choose the most advantageous course of action, carry it out successfully, and avoid detection. Additionally, these initiatives may be directed at your company. A continuous, round-the-clock, evolutionary, algorithm-driven cyber attack program will be running, "thinking" critically about how to attack.

Most crucially, it can change in order to evade detection. These tools, for instance, could be able to identify every single employee who currently works for or has ever worked for your business by searching through Linked In data. After that, it might attack each of their home networks before waiting for one of them to log on to the company network. Since the majority of AI practitioners are excellent at interpreting the information at hand, they are rarely security professionals who can safeguard their systems and data. Adversary AI was created as a result of cybercriminals' ability to infiltrate these systems. The ability of data and AI systems to provide the promised benefit to the business is put at risk by this kind of cyberattack. Cybercriminals can modify the data or add significantly different data sets that are given to the learning model along with the original data once they have gained unauthorized access to the storage network.

Machine learning data poisoning targets only the training data provided to the model, as opposed to the traditional adversarial AI cyberattack, which depends on stealing a pre-trained model. It is easier for hackers to alter the learning of the model itself because fewer highly skewed samples of the input data are required. In order to detect potential problems once an ML model has been trained on the contaminated data, deep AI knowledge will probably be needed, especially in the case of unsupervised learning models.

The hijacking or reverse engineering of AI models is known as AI model theft. Additionally, private AI models are put into use on open networks that may be accessed via API requests. The data being consumed and output from deployed models can also be used to recreate algorithms.

In general, AI-driven hacks will get worse before becoming nearly difficult to find using conventional cybersecurity techniques. It essentially comes down to weighing human effort vs. machine efficiency. Teams working on cybersecurity are being overwhelmed by the complexity and size of this trend. In contrast, it is becoming more expensive and challenging to obtain the sophisticated and skilled cybersecurity personnel that are required to adequately address this danger. These new AI-driven attack methodologies could have fatal and extremely devastating effects. These subtle attacks threaten data security and integrity, which could lead to systemic failures, weakening trust in companies. [11]

VI. Real world Consequences and Recovery

Network breaches and cyber-crime are becoming more and more of a problem every year. After all, research has show that the average cost of a data breach in 2021 worked out to be around 4.24 million dollars per incident. This was the highest average cost in the history according to the current data. The latest reports also establish that cyber attacks are likely to cost a total of 6 trillion dollars annually by the end of 2022. Part of the reason for this rising cost can be attributed to the COVID-19 pandemic, where cyber attacks rose in severity and frequency. This is due to the fact that dependence on the internet and technology grew as people were confined the their home. [12]

One simple way to counter-act cyber attacks is to back up your data. The only way to restore your data without paying a ransom after a malware infection is to have a copy of your valuable data stored elsewhere. With that said, you still must be careful; if you configure your device or computer to back up your data and most valuable files to the cloud and your computer gets attacked by ransomware, it is possible for that ransomware to also spread to your cloud and become infected by the attack as well. It is also a possibility that even if you pay a ransom for your data, you still will never be able to recover it. This is all the more reason to have a back up of your files. Regardless, the best way to deal with an attack is to prevent it from ever happening.

One famous example of a large data breach was against the company Yahoo!. Two hackers named Alexey Belan and Karim Baratov were hired by Russia's secret service to steal information on several high-profile government officials. Belan and Baratov sent Yahoo! employees emails that contained a link to download malware. They only needed one employee to click the download link to gain access to the entire company's server and database. After they successfully tricked an employee, they established a back door to the main Yahoo! server. A backdoor is a hidden entry point in your website or application that offers unrestricted access to it. These can be very hard to detect and can either be set up on purpose or set up maliciously as in the case of the Yahoo! breach. They implemented this to make sure they had easy access to the server in the future. Names, phone numbers, emails, and other sensitive data was leaked in this breach. The company ended up having to setup a settlement fund worth 117,500,000 to pay for the damages it caused to its users. As we can see, even the biggest companies can be brought down with a single click. Due to the costs and dangers of cyber attacks, it is vital to a company's success to have and incident response plan, or IRP. An IRP is a set of instructions designed to mitigate and control the damage of a data breach or network attack [13]. Every single company should have one, as a single attack can destroy a company's reputation and hurt them financially.

VII. Results

A. IRP Prevention

Even with all of the prevention techniques at our disposal, we can never make our networks completely secure. One thing that is just as important as preventing the network attacks is how we can recover from them. Like we mentioned previously, one way to recover from a data breach is to have an IRP ready. Since the frequency of these breaches is so high, responding fast and efficiently to these attacks is a must. An IRP typically has four steps. The first step is preparation. Before any incident ever happens, you should prepare and perform a risk assessment analysis and identify where the vulnerable parts in your network are. The next step is identification. In this step, you will detect deviations from typical operations in your system and evaluate the severity of the incident. Next is containment. Once your team finds the breach, their first priority is to contain it and prevent more

damage from occurring. After that, there is the eradication of the threat. You must identify the root cause of the attack and remove any other malware and patch the vulnerability, so it cannot be exploited again in the future. The final step is recovery, where you bring the affected systems back to normal operation after you have dealt with all the threats [13].

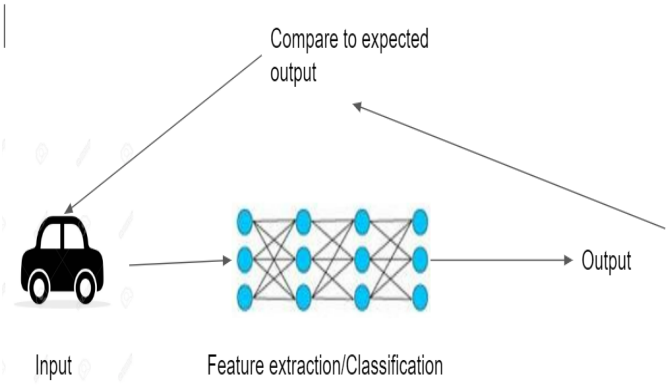

Fig. 3. Deep learning training scheme.

B. Machine learning methods to detect cyber attacks

Machine learning approaches in attack detection are used for three main purposes: detection, attack classification, and analysis. Training data goes through a series of preprocesses before being used in model training.

1) Support Vector Machine: A decision boundary between two classes is found using the Support Vector Machine (SVM), a vector space-based machine learning technique, which is farthest from any point in the training data. When an attack has been identified once, SVM can be used with the classification model to perform a secure packet transfer between various sensor nodes. [14]

2) Naive Bayes: A supervised learning technique known as the Naive Bayes (NB) classifier is based on the Bayes theorem and a number of conditional independence assumptions about the attributes. To determine explicit probabilities for the hypothesis, it integrates prior knowledge and observable data.

3) Extreme Gradient Boosting: A machine learning approach called Extreme Gradient Boosting (XGBoost) is based on gradient-boosted decision trees. By avoiding the issue of overfitting during algorithm training, XGBoost, one of the new generation community learning algorithms, improves the model's overall accuracy. This method's primary success factor is the purpose function it employs during the learning process. [15]

4) Autoencoders: Autoencoders (AE) are uncontrolled neural networks that attempt to match the output to the same vector by taking a vector as input. An input can be used to represent data in a higher or lower dimension by taking the input, altering its size, and then rebuilding the input. These adaptable neural networks can unsupervisedly train to encrypt compressed data. A suitable model can be created with fewer computer resources by training one layer per iteration. When hidden layers have smaller dimensions than input and output layers, the network is utilized to encrypt data.

5) k- Means clustering: Among unsupervised learning techniques, k- Means clustering is one of the most popular machine learning algorithms. Data samples are sorted into K groups based on how similar they are. Similar characteristics of objects from other groups are shared within each group. K is the user-specified number of clusters. The center of gravity for each cluster is then randomly selected after the number of clusters has been established. The distance between the center of gravity and data points is calculated using the Euclidean equation. The data points that are clustered are those closest to the gravitational center. It is determined that the value obtained serves as the new weight center by calculating the average separation between these data points. Up until no more data points are transferred between them, the process is repeated.The performance of the intrusion detection system can be enhanced by using a variation of the K-means algorithm to generate new, tiny training datasets that accurately replicate the training dataset, minimize the classifiers' training time, and build new, smaller training datasets. [16]

6) Recurrent neural network: A directed loop is formed by connections between units in a recurrent neural network (RNN). RNN can display dynamic temporal behavior. It has the ability to process inputs using its own input memory, unlike forward propagation neural networks. RNNs are a good technique for voice and handwriting recognition because of this property. Unlike other deep learning models, RNN features hidden states and a structure that enables prior outputs to be used as input.

VIII. Conclusion

Security in cyber-physical contexts is increasingly important as our reliance on network devices grows. Machine learning approaches and intrusion detection systems, such as rule- and signature-based intrusion detection systems, have improved cyber security. The classification abilities of deep learning-based detection systems were also improved according to the current data. [17] The success of deep learning techniques is quite impressive. Research on unique attack-type applications has increased as a result of more attack diversity. The only area where early intervention tactics may be improved is the detection of attacks. Multivariate statistical metrics for attack detection and gauging the effectiveness of traditional models for AI based machine learning applications in cyber security can both be investigated further. The categorisation of attacks is crucial in this regard. For each kind of attack, there should now be enough information available. As we have discussed, the threat of network attacks is real and the cost is high. It would not be a stretch to say our future is completely reliant on how we are able to defend against the network attacks we have discussed. Those in the past fought with swords and defended with shields, while today we fight with computer viruses and protect ourselves with firewalls.

REFERENCES

[1] Y.-C. Hu, A. Perrig, and D. Johnson, "Wormhole attacks in wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 370–380, 2006.

[2] T. Ahmad, D. Truscan, J. Vain, and I. Porres, "Early detection of network attacks using deep learning," in *2022 IEEE International Conference on Software Testing, Verification and Validation Workshops (ICSTW)*, pp. 30–39, 2022.

[3] M. Maliha, "A supervised learning approach: Detection of cyber attacks," in *2021 IEEE International Conference on Telecommunications and Photonics (ICTP)*, pp. 1–5, IEEE, 2021.

[4] K. Kuppa, A. Dayal, S. Gupta, A. Dua, P. Chaudhary, and S. Rathore, "Convxss: A deep learning-based smart ict framework against code injection attacks for html5 web applications in sustainable smart city infrastructure," *Sustainable Cities and Society*, vol. 80, p. 103765, 2022.

[5] N. Sivasankari and S. Kamalakkannan, "Detection and prevention of man-in-the-middle attack in iot network using regression modeling," *Advances in Engineering Software*, vol. 169, p. 103126, 2022.

[6] R. Yan, X. Xiao, G. Hu, S. Peng, and Y. Jiang, "New deep learning method to detect code injection attacks on hybrid applications," *Journal of Systems and Software*, vol. 137, pp. 67–77, 2018.

[7] T. Baba and S. Matsuda, "Tracing network attacks to their sources," *IEEE Internet Computing*, vol. 6, no. 2, pp. 20–26, 2002.

[8] K. Kumar and S. Arora, "Review of vehicular ad hoc network security," *International Journal of Grid and Distributed Computing*, vol. 9, pp. 17–34, 11 2016.

[9] O. Osanaiye, A. S. Alfa, and G. P. Hancke, "A statistical approach to detect jamming attacks in wireless sensor networks," *Sensors*, vol. 18, no. 6, 2018.

[10] T. Ahmad, D. Truscan, J. Vain, and I. Porres, "Early detection of network attacks using deep learning," in *2022 IEEE International Conference on Software Testing, Verification and Validation Workshops (ICSTW)*, pp. 30–39, 2022.

[11] B. Guembe, A. Azeta, S. Misra, V. C. Osamor, L. Fernandez-Sanz, and V. Pospelova, "The emerging threat of ai-driven cyber attacks: A review," *Applied Artificial Intelligence*, pp. 1–34, 2022.

[12] E. A. Morse, "Market price effects of data security breaches," *Information Security Journal*, vol. 6, p. 273, 2011.

[13] K. Levchenko, R. Paturi, and G. Varghese, "On the difficulty of scalably detecting network attacks," in *Proceedings of the 11th ACM Conference on Computer and Communications Security*, CCS '04, (New York, NY, USA), p. 12–20, Association for Computing Machinery, 2004.

[14] G. M. Borkar, L. H. Patil, D. Dalgade, and A. Hutke, "A novel clustering approach and adaptive svm classifier for intrusion detection in wsn: A data mining concept," *Sustainable Computing: Informatics and Systems*, vol. 23, pp. 120–135, 2019.

[15] T. Chen and C. Guestrin, "Xgboost: A scalable tree boosting system," in *Proceedings of the 22nd acm sigkdd international conference on knowledge discovery and data mining*, pp. 785–794, 2016.

[16] W. L. Al-Yaseen, Z. A. Othman, and M. Z. A. Nazri, "Multi-level hybrid support vector machine and extreme learning machine based on modified k-means for intrusion detection system," *Expert Systems with Applications*, vol. 67, pp. 296–303, 2017.

[17] H. Hanif, M. H. N. M. Nasir, M. F. Ab Razak, A. Firdaus, and N. B. Anuar, "The rise of software vulnerability: Taxonomy of software vulnerabilities detection and machine learning approaches," *Journal of Network and Computer Applications*, vol. 179, p. 103009, 2021.