Ai-Based Solutions for Improving Cybersecurity and Its Significance in Defending Evolving Cyber Threats in Enterprises

Authors: ***Sakthiswaran Rangaraju* & Rajesh Dharmalingam*****

**Product Security Leader, Pure Storage, Santa Clara, California, USA*

***Security Architect, Delphix, Redwood City, California, USA*

Abstract

Artificial Intelligence and its sub-domain Machine learning contribute to the system development by learning from previous data, making logical judgements, spotting patterns with little to no human intervention. Cybersecurity approaches offer modern solutions to provide security against the attacks and threats. Consequent to the ability of attackers to evade conventional security solutions, the previous and traditional security measures are not strong enough to tackle the current time's security issues. Protecting the data and software products from the attacks present on servers, computers, smart devices and networks is the practice of cybersecurity. There are two main factors to combine cybersecurity with Artificial intelligence (AI); one is considering cybersecurity for situations where AI is implemented and using AI to improve the cybersecurity measures. It has benefited from various aspects like these models that provide better security and improve the cybersecurity approaches and their effectiveness, thus making proficient identification of cyber threats with no human intervention. In this research article, these two techniques (AI and cybersecurity) have been integrated to provide AI based solutions for improving the cybersecurity of data and systems.

Keywords: artificial intelligence, cybersecurity, data and software security, spam, malicious attack.

1 Introduction

Cybersecurity is known as the set of procedures, systems, and human behavior that assists in protecting electronic resources. In more common terms, it is the domain of employing methods and techniques of safeguarding the networks, data, and devices from unauthorized access and protecting the confidentiality, availability, and integrity (CIA) of the digital data (information)[1].

The primary objective of the cyber-defense system is to make sure that data presented in the system is not compromised and is secured. Vulnerabilities and internal loopholes within the computer networking setup and systems expose these devices and networks to the risk of cyber threats and attacks. Weaknesses and susceptibilities in the design of Network systems include lack of adequate protocols, improper design, and unskilled staff. All of these shortcomings ultimately give rise to the risk of cyber threats on the network system not only from intruders but the attackers from the outside as well. (Pillai, 2022)

Cyber attacks globally increased by 125% in 2021 compared to 2020, and increasing volumes of cyber attacks continued to threaten businesses and individuals in 2022. A concerning statistic is that 67% of SMBs feel that they do not have the in-house skills to deal with data breaches. However, this issue is mitigated as increasing numbers of SMBs are working with Managed Service Providers for cyber security; 89% as of 2022, up from 74% in 2020. In 2022, investment fraud was the most costly form of cyber crime, with an average of $70,811 lost per victim. In 2022, data breaches cost businesses an average of $4.35 million – up from $4.24 million in 2021[2].

Cybersecurity is striving to defend against the threats to secure and protect the data, algorithms, and networks. There has been strong competition between defense and cybercriminals since the time when the first computer virus was developed in 1970. It is becoming difficult and more complex day by day to defend against these threats and make the network system sophisticated enough to stay up to the cybercriminal’s pace. In order to tackle this situation, since the last decade, researchers from the field of cybersecurity have begun to explore and research Artificial Intelligence (AI) methods and techniques to enhance the cybersecurity of systems and networks. In the same way, cyber-criminals have also started to use AI to instill highly sophisticated cyberattacks while being covert regarding their identity and the tracks they follow. Nevertheless, in this research work, the aim is to emphasize how AI techniques can be used to improve the cybersecurity of software systems while offending the attackers better, and preventing system and data breaches[3].

Advancements in AI have taken several beneficial research outcomes and systems with its development since the 1950s. Further advancements in technology gave rise to machine learning (ML) and deep learning (DL) techniques. In current times, AI has been implemented and used in a number of domains and applications such as agriculture, law, space, healthcare, business, as well as manufacturing. The consistent performance progression in the computer software as well as hardware that has also been taken to decrease costs, along with innovative approaches like cloud computing as well as big data, have led to the deployment of an extensive range of AI systems with unpredictable abilities. At present, several AI systems have the ability to perform a wide range of the most difficult and complex tasks involving planning, learning, problem solving, speech and face recognition, and even decision-making. Starting from the 1980s till today, a significant development has emerged in the domain of AI in the form of machine learning (ML) technology. This technique assists the systems to learn as well as adapt to the different conditions by making use of their past patterns, experiences, and knowledge[4]. In the past few years, a subdomain of ML which is also named deep learning (DL) has emerged enabling machines to determine the converted connection and links in input data, thus giving more accurate and precise outcomes for predicting, planning, and decision making. Currently, a significant increase in the interest to employ AI and ML approaches has been witnessed for addressing the issue of cyber-attacks. A strong drive to use such algorithms and approaches arises from the significantly high amount of data that is being generated in the digital world, requiring a number of resources as well as time to evaluate and detect the anomalies, patterns, and intrusions within the traffic data.

By making use of these techniques, it has become possible to identify possible modern times spam, detect cyber fraud, phishing, and malware along with dark websites, and uncover breaches. It is possible to eliminate and eradicate the human deficiencies in the detection methods of these cybercrimes by making use of AI and ML techniques[5]. In addition to this, for detecting, identifying, and responding to the sophisticated cyberattacks of the new generation, there comes the need to implement the proactive approach.

AI/ML algorithms have the potential to quickly show resistance to cyberattacks based on the ability to grasp and learn from previous training and experiences, in such a way these react to the future in a timely manner. Some of the most common cybersecurity technologies of current times are firewalls, intrusion prevention systems (IPS), antivirus software, and unified threat management (UTM). Conventional solutions significantly depend on static device management as per the predetermined rules of network security and lack of automation (or lack of use of AI techniques). In context to the performance, reaction to the cyberattacks, and error rate, AI-based systems can perform much better in comparison to the conventional attack detection methods. These techniques have a much lesser error rate in detecting and defending attacks than any other traditional defense systems[6]. The AI/ML models have played a significant role in enhancing performance and also providing intelligent and robust approaches to identifying and detecting the attacks before and mitigating the damage that these cyberattacks cause. It makes the algorithms more accurate and capable of performing cyberattack categorization rapidly and early.

The organization of this research article is as follows: In section 2, an overview of the landscape of the cybersecurity threats and attacks is presented along with their traditional solutions which are deployed for the protection of various software systems. In section 3, Fundamentals of AI/ML techniques are elaborated that are used for enhancing the cybersecurity of the software systems. Section 4 highlights some techniques to detect cyberattacks and threats using AI/ML. Section 5 summarizes the research article with a conclusion along with some challenges of the cybersecurity community that must be addressed in the future[7].

2 Cybersecurity Fundamentals and Threats

In the past few decades, a significant surge has been observed in cyber threats and attack types. The potential dangers and the risks of all security data breaches are known as threats, and making an attempt to commit the breach is called an attack. There are several ways to elaborate on the term "cybersecurity" which also includes its definition as the most dangerous mugging or assault, for instance, malware or phishing. Phishing is usually referred to as "brand cloning" which is the practice of gaining unauthentic access to "personally identifiable information" to abuse or manipulate it by pretending to be the legal and authentic user.

Phishing is a kind of scamming that uses an authentic or actual website to get and acquire personal data. Trojan horses, Worms, and viruses are a few of the basic types of malware. A virus is known as a small chunk of software that degrades the performance of the system or computer without making the user aware of such damage[8]. This can be harmful to the operating system as well as files saved in the computer devices. On the contrary to worms and viruses, Trojan horses pretend to be the genuine software that is launched by a particular procedure rather than increasing in number. Similarly, unwanted emails can also cause damage to the cybersecurity of a system. Spams on the other hand come up as text, calls, or video communication on the system network or mobile devices. Twitter and YouTube are some of the examples where spammers send messages and videos. Firewalls, intrusion detection systems (IDS), and antivirus software are considered to be some components of the network security system. IDS helps in detecting as well as identifying malicious and unauthorized intrusion and access to the system[9].

Apart from the ones mentioned above, there are a number of cyberattacks that occur today more frequently, A few of them have been discussed below:

2.1 Denial of Service (DoS) Attack

In this attack, an attempt is made to corrupt the user's computing system resources by sending a large amount of requests for it to process in a short duration. These attack types can be done in various ways, for example, one attacker machine can perform a DoS attack on the other (victim) machine by sending an infinite amount of network traffic packets that somehow seem to be authentic and legitimate, for bypassing the security controls as well. Furthermore, multiple machines can perform the distributed DoS attack which results in a similar outcome in the victim machine[10]. In current times, DoS attacks have become more sophisticated and more complex to detect, and the reason behind this is the readily accessibility of the attacker tools and the proliferation of the "CyberCrime as a Service (CCaaS) market".

2.2 Eavesdropping Attack

The attacking process of this malicious attack involves making the network communication line sniff out and then misuse the unethically gained data. There are two possible ways for the attacker to get to the data, either by sniffing the line passively or actively attacking the communication line, and then replacing the messages with fabricated messages, and pretending to be the authentic user.

2.3 Man-in-the-Middle Attack (MiTM)

MiTM is known as the legacy cyberattack which is done by a process where the transmitted data gets interrupted over the communication line between the two authentic and legitimate users who are communicating with each other[11]. In all this setup, the attacker keeps itself either in virtual form or in physical form between both communicating users, in such a way if A and B are two users, an attacker would act as A while communicating to the user B and it is done through interception among both users messages and eventually by replacing the messages with the tempered or malicious messages[12]. The same process is repeated when user B communicates with user A through messages. Abnormal and irregular implementation of such attacks involves IP address spoofing, whereas the malware or harmful actor persuades the authentic system to be an authentic and trustworthy entity so that the attacker can gain access to the system. A message replay attack includes the transmission of the already stored (previous) and stale messages over the communication line, which are already affected by the malicious attacker.

2.4 Phishing Attack

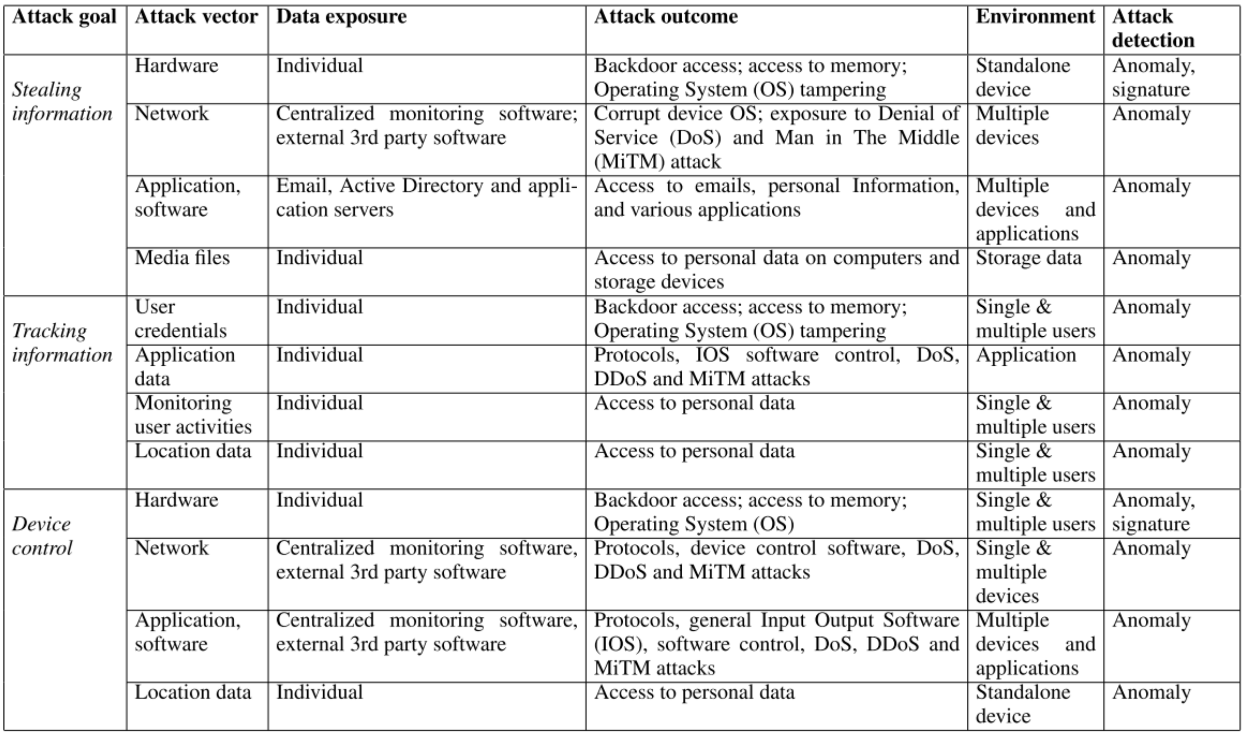
These attacks are done by creating fake emails that actually appear to be real and legitimate and then are transferred to the authentic system[13]. The intention behind doing so is to make the naïve user click on the malicious link and gain access to its personal or crucial data. Such type of attacks uses the principles of social engineering attacks where emails are sent to the user to appear as authentic emails so that the user can trust those emails and click them to open them.

2.5 Password Attack

This type of attack is done by "shoulder surfing user keyboard activity", injecting brute force attack within the system making use of the common passwords, and then creating more sophisticated passwords via AI techniques and applications.

All these attacks are injected within the system to disrupt its overall environment and services and also to gain the confidential data of an individual or corporate organization. These malicious attackers pick up and exploit the OS's “operating system” weakness to gain access to the OS to accomplish harmful and destructive objectives. Table 1 shows the list of a few attacks along with their targeted devices and environment for attack along with the approaches to identify and detect these attacks[14].

Table 1. Several attacks types, their impact, and methods to identify them



Attack goal	Attack vector	Data exposure	Attack outcome	Environment	Attack detection
Stealing information	Hardware	Individual	Backdoor access; access to memory; Operating System (OS) tampering	Standalone device	Anomaly, signature
	Network	Centralized monitoring software; external 3rd party software	Corrupt device OS; exposure to Denial of Service (DoS) and Man in The Middle (MiTM) attack	Multiple devices	Anomaly
	Application, software	Email, Active Directory and application servers	Access to emails, personal Information, and various applications	Multiple devices and applications	Anomaly
	Media files	Individual	Access to personal data on computers and storage devices	Storage data	Anomaly
Tracking information	User credentials	Individual	Backdoor access; access to memory; Operating System (OS) tampering	Single & multiple users	Anomaly
	Application data	Individual	Protocols, IOS software control, DoS, DDoS and MiTM attacks	Application	Anomaly
	Monitoring user activities	Individual	Access to personal data	Single & multiple users	Anomaly
	Location data	Individual	Access to personal data	Single & multiple users	Anomaly
Device control	Hardware	Individual	Backdoor access; access to memory; Operating System (OS)	Single & multiple users	Anomaly, signature
	Network	Centralized monitoring software, external 3rd party software	Protocols, device control software, DoS, DDoS and MiTM attacks	Single & multiple devices	Anomaly
	Application, software	Centralized monitoring software, external 3rd party software	Protocols, general Input Output Software (IOS), software control, DoS, DDoS and MiTM attacks	Multiple devices and applications	Anomaly
	Location data	Individual	Access to personal data	Standalone device	Anomaly

3 Fundamentals of Artificial Intelligence (AI)

AI is considered to be more concerned about how machines can act or think correctly, provided what type of information they have[15]. This universal definition involves how thoroughly and carefully machines get adapted to act or think in a way similar to the human being, as shown in Fig. 1. On one side of the spectrum, machines are taken as the most intelligent equipment when they appear to be performing well and providing optimized results at every phase of the process, while on the other end of the spectrum, a number of questions and queries arise on their intelligence as we Turing Test.

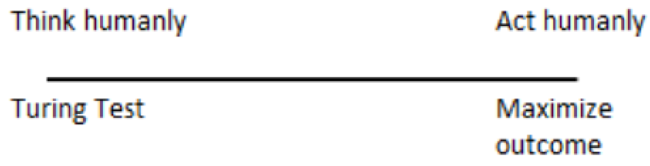


Figure 1. Spectrum span from simulating human thought in processes like the Turing Test to perform human actions for ideal results

Under this test, human-computer communication is considered to be intelligent if the response given by the computer is not recognizable by the human whether it is original or computer generated[16]. On both ends of the spectrum, AI symbolizes and presents computing domains like natural language processing (NLP), logic, knowledge representation, machine learning, automated reasoning, game theory, and mathematics[17].

After the emergence and spread of the internet at the end of the 1990s, software that acts as a human being acquired a lot of popularity in the context of the agent-based AI, also known as bots. Ethical bots were used to keep a check on the internet to improve the search engines, recommendations lists, and yellow pages. However, malicious bots were used to dismay the cyber services to work and operate properly, making the service providers discourage visitors online[18]. As a consequence of this, few of the cybersecurity research explored the solutions to identify, detect, and safeguard cyber systems and software from malicious bots.

Cybersecurity solutions usually do the internet traffic analysis, and classify the upcoming traffic as authentic or malicious. With the emergence of the internet, rule-based systems were used to identify cyberattacks, where attacks were identified using signatures. For the past few years, due to the increased number of internet-linked applications and devices, and the high volume of network traffic in real-time, the rule-based systems take more time to analyze this traffic and eventually make the system protection behave in a defensive manner rather than a proactive manner. Therefore, it is high time to implement and deploy advanced tools and technologies to identify attackers and avoid cyberattacks. AI is capable of analyzing and classifying internet traffic intelligently and automatically. In current times, cybersecurity solutions on the basis of ML technologies are being deployed and implemented to automate the identification and detection of cyberattacks and improve the systems and software's abilities with the passage of time[19]. ML solutions are used in IDS because of their ability to tackle large data volumes and extensive data attributes such as huge table columns, for classification purposes. It is worth noting that because of the extensiveness of ML in handling cybersecurity issues, embracing ML terminology has turned out to be interchangeable with AI in the domain of cybersecurity.

3.1 Machine Learning (ML)

To improve cybersecurity, detect phishing websites, and categorize a number of automated new attacks before time, ML techniques and methods are implemented. In the context of the method, ML is categorized into three main classes: supervised, semi-supervised, and unsupervised learning[20]. In supervised learning, the machine knows about the data classes and targeted labeling, which are then used to train the computer. In unsupervised learning, no intended value is provided by ML. The main objective of this learning type is to determine the association of the data. It searches for data patterns. In semi-supervised learning, some of the data is labeled. At the time of the lettering process, problem solving and improvement in model accuracy are done by taking assistance from human specialists.

Naïve Bayes is an ML approach that is used for classifying the data on the basis of the Bayesian theorem. In this technique, features are expected to emerge from events that are independent. This approach makes use of the computed probability of every class over each of the instances as a basis to determine the probability of new data samples of the class[21]. Some of the sub-techniques of ML are discussed below:

3.2 Various Machine-learning Technologies

3.2.1 Decision Tree (DT)

A DT is the ML approach that is used to make a set of rules using the training data samples. This ML algorithm determines the feature that is considered to be a best-classified sample of data. The iterative segmentation makes the sequence of rules for each categorization side, which results in a tree-like structure until data samples having only one class are identified after segmentation. Fig. 2 illustrates the example of DT classifying the network traffic making use of the rules leading to the classification of normal or attack (malicious) traffic[22].

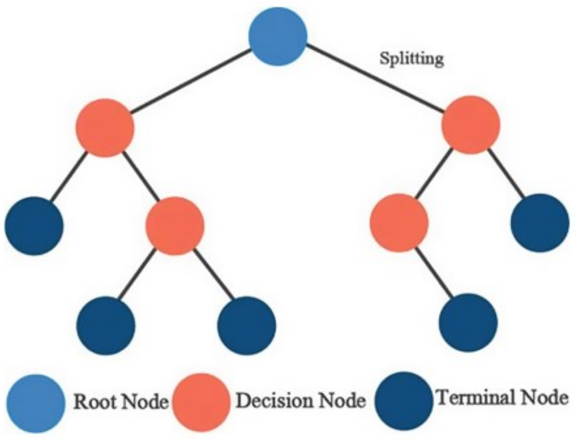


Figure 2. Structure of a decision tree algorithm

3.2.2 Support Vector Machine (SVM)

In intrusion detection systems (IDS), SVMs are considered to be the most likely and most suitable ML methods. On the basis of the labeling of different margins of each side of the hyperplane, SVM categorizes and segments the two data classes. Fig. 3. Illustrates the visual representation of the SVM approach. The gap among the different margins as well as hyperplanes is possible to increase to enhance the classification outcome[23]. Here, the vector points are considered to be the data points which are located at the boundary of the hyperplane. The SVM approach is the classification technique. This binary categorization method predicts the hyperplane in n-dimensional space by making use of the training set.

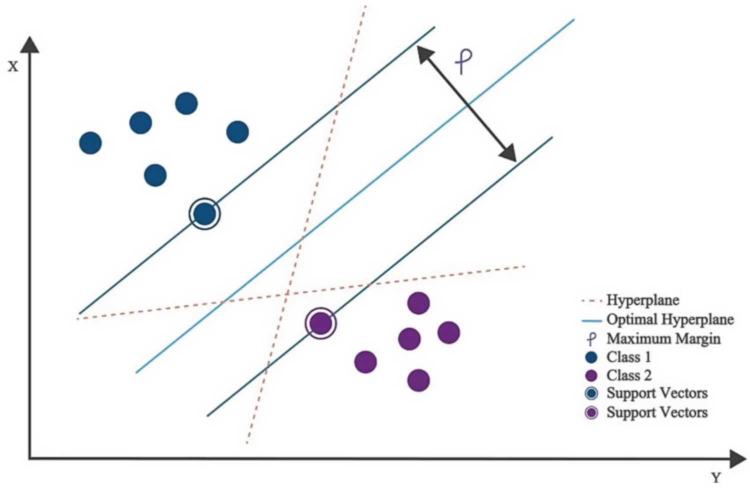


Figure 3. Structure of a support vector machine algorithm

3.2.3 ***Random Forest (RF)***

RF is considered to be ensemble learning that makes use of different classification approaches to create a scientific consensus regarding the issue to make the typical outcome. RF is taken as the more developed version of CART. It generally contains several predicting outcomes that are derived from different DTs[24]. In literature, RF is used for problems like “intruder identification” and also to evaluate the spam quantity.

3.2.4 ***Convolutional Neural Network (CNN)***

CNN is considered to be a multi-layer neural network. It is composed of 3 kinds of layers, as illustrated in Fig. 4. It forms the convolutional layers, more than one interconnected layer, and also a pooling layer. CNN structures like GoogleNet, as well as ResNet, are significantly implemented. The algorithm takes out complicated features in high resolution and changes them to detailed fine features[25].

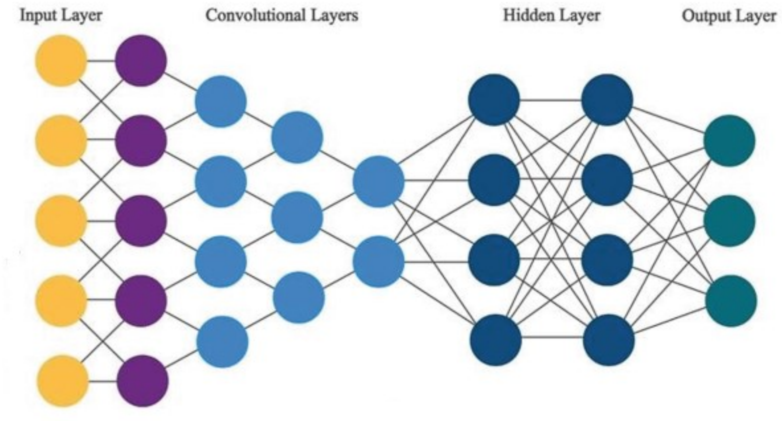


Figure 4. Structure of a convolutional neural network algorithm

3.2.5 ***Reinforcement Learning (RL)***

RL is another sub-domain of ML algorithm, which is defined as the acquiring knowledge with reviewers as algorithms gain feedback for inaccurate or wrong predictions and forecasts[26]. Nevertheless, the RF algorithm is still not trained or informed on how to fix the issue. Rather, the algorithm searches for and tests different alternatives until it finds out the most appropriate solution. This technique works on the basis of rewards and punishment system.

4 Cybersecurity and Use of AI/ML Techniques

Cybersecurity ensures the systems and applications against cybercrimes and dangers. Cybersecurity contains a number of dimensions, for instance, malicious URL identification, detection and then categorization, spam classification, fraudulent transactions, harmful node creation, IDS, probing, and cyber-extortion. In addition to this, with the development of computer systems and networks, smart networks and devices have also developed, however, they have been rendered as the more strong target of cyber attackers and criminals[27]. Cybersecurity links with different other elements and components of cyberspace such as internet security and safety, ICT, and network security. In this section, the three most prominent and significant concerns of cybersecurity (Spam, IDS, and malware identification and recognition) have been addressed in the context of AI/ML algorithms playing a major part in identifying and detecting them.

The subsections below discuss the cyberattacks on computer systems and software technologies while explaining how AI/ML approaches to combat and handle these cyber issues[28].

4.1 Using AI/ML for Spam Detection

Electronic mail is considered to be the technique to send data among various individuals using digital gadgets through the internet. It is the most commonly used tool and its popularity has grown exponentially. Spam messages are unwanted, unnecessary, emails which is usually used for advertisement and also to irritate the user. Such spam emails also take up a lot of email storage space and thus decrease the duration as well as time which is spent online and also network and software system functionality. In current times, more than 90% of the emails that a user gets are spam. The main target of the spammers are considered to be online search engines and emails[29]. It is not just email that is targeted while spamming, but other mediums are also used through which spams are done such as smart phones, online communication channels, newsletters, blogging and streaming sites. Social media platforms like Twitter (X), Facebook and also YouTube enable the scammers to upload and share their material easily so that scammers get benefit from these platforms. Several computer researchers are searching to find solution to this. Spam filtration is one of the process through which emails as spam can be identified and then screened out the unauthentic or unwanted emails. In literature, various strategies have been discussed and suggested about spam filtering, however, it is not efficient as spammers have now become sophisticated enough to vary the spam terms. Anti-spam, usually named as the "anti-spam technology" is a group of few procedures that are deployed to combat different spam attacks while reducing its effect on effectiveness of anticipated medium[30].

A number of ML techniques have been discussed and explained in detail in literature for spam filtration, categorization, and detection. ML algorithms are implemented in various spam detection fields including picture emails, Twitter, and blogging. Each of the domain has its own classification approaches. Meanwhile various research suggest that SVM method has high success rate than the other classification techniques. Some of the researchers have mentioned feature selection method along with classifier to be more accurate. Decision Trees, SVM and Naive Bayes and also Random forest are some of the most popular ML methods. Approaches like content-based ML are implemented to segregate the spam emails through filtering feature. It includes several spam filtering strategies and tools[31].

4.2 Using AI/ML for Intrusion Detection

There exist three significant cyber analysis types for IDS. These detections are anomaly-based, exploit-based, or hybrid-based. Exploit-based detection detects the attacks that are known. Anomaly detection observes the normal network as well as system activity and gets familiar with the irregular behavior of networks and systems.

It is a crucial and difficult phenomenon to comprehend the behavior and patterns of attacks and invaders. To tackle this, ML techniques play a significant role to predict and identify future intrusions and attacking them in real-time[32]. Usually, intruders are detected through ML techniques and some of the most commonly used methods include fuzzy association, decision trees (DT), SVM, and statistical models. Several ML approaches are employed to identify and detect the DoS attacks, for which DT could achieve 97.24% accuracy, while neural network showed 97% accuracy, and the accuracy of Naïve Bayes was 96.65% and that of SVM, it was achieved to be 98.7%.

4.3 Using AI/ML for Malware Detection

Malicious activities are considered “malware” which is software that is installed secretly in a device with the intention of compromising the activities of users. This malware attacks the confidentiality, availability, and integrity of data that is stored on software and hardware by the perpetrator. The term ‘malware’ has been derived from the words “malicious” and “ware”. Worms, Viruses, Trojan Horses, spyware, and adware are a few examples of these malicious activities. This malicious software disrupts and damages the whole system and also expands to other networks and devices[33].

ML techniques and algorithms are considered to be most effective in this concern to detect zero-day threats and attacks and also in identifying complex malicious attacks[34]. SVM is known to be the most researched ML approach for the detection of malware with 29% utilization which is seconded by DT with 17% usage. In addition to this, merging different ML techniques together with semi-supervised learning increases the accuracy and prediction rates.

Cyberattacks and threats to mobile gadgets have increased significantly with the increased usage of mobile banking, e-commerce, and transactions. As a consequence to this, these devices have turned out to be more prone to such attacks in comparison to personal computers.

K-Nearest Neighbor (K-NN), SVM, decision tree, and random forest are considered to be few ML approaches that are better in terms of accuracy to detect malicious attacks and threats in mobile devices as well as network. This accuracy of the ML classifier can also be improved by integrating feature selection with that of the classification method[35]. There are three types of antimalware methods (detection techniques) for mobile gadgets such as, hybrid, static and dynamic. Static detection evaluates the program for the malicious patterns without implementing it or deploying it. On the opposite, dynamic detection is done by executing the actual original program and monitoring the behavior in real-time scenario. The hybrid techniques of detection identifies the malware by integrating dynamic as well as static analysis.

In, a model has been explained and discussed named as “opcode-sequence frequency”, KNN, decision tree and SVM were implemented to acquire the 90% accuracy. In, for identification of malware, SVM, decision tree, RF, and Naïve Bayes were used. The accuracy of detection was found to be more in SVM technique[36].

5 Conclusion

As a consequence of their inaccuracy and inefficiency in determining the cyber threats and attacks within the system devices and networks, the conventional solutions of security are not considered to be appropriate anymore. In this research article, two techniques (AI and cybersecurity) have been explored and discussed, to provide AI-based solutions for improving the cybersecurity of data and systems. The overview of AI/ML algorithms and techniques has been presented in the context of detecting malicious attacks including malware attacks, intrusion detection, and spam detection on the computer systems and networks. For handling and addressing cybercrimes, different AI/ML approaches have been discussed which are considered to provide better accuracy in comparison to the traditional methods and techniques.

With an aim to improve and enhance the security measures in the cyber world and digital systems and software, it has become a global concern to increase the cyber security. In current software applications and systems, AI/ML is used significantly and in a number of ways. For all types of attacks, it is not accurate to recommend only one of the AI/ML techniques and classifiers. For each of the attacks, different approaches provide better results in terms of accuracy. The research article also covers the fundamentals of cyber security including the categorization of intrusions on digital devices and systems.

Recently proposed AI-based solutions for cybersecurity highly emphasize ML approaches involving the integration of intelligent and smart agents to differentiate between legitimate and attack traffic. In such a scenario, intelligent agents work as humans with the task of determining the most appropriate and efficient rule of classification. Nevertheless, the current cyberattack scenario has evolved beyond merely disrupting computers to instigating chaos in society and jeopardizing human welfare. Concerning this, the article also discussed the matter in the context of how developments in technologies are changing the sophistication level of cyberattacks along with their detection and mitigation. With such development, the role of AI in cybersecurity with keep on increasing with the passage of time. New and innovative AI approaches and algorithms need to be developed immediately to rapidly detect as well as alleviate the attacks and threats that threaten social well-being. Most probably, cybersecurity solutions will progress from intelligent agents imitating human actions to replicating human thought processes.

6 References

[1] T. Thomas, A. P. Vijayaraghavan, and S. Emmanuel, "Machine learning and cybersecurity," Machine Learning Approaches in Cyber Security Analytics, pp. 37-47, 2020.

[2] K. Chaudhary and S. Singh, "Different Machine Learning Algorithms used for Secure Software Advance using Software Repositories," 2023.

[3] S. Rangaraju and S. Ness, "Incorporating AI-Driven Strategies in DevSecOps for Robust Cloud Security."

[4] S. Zeadally, E. Adi, Z. Baig, and I. A. Khan, "Harnessing artificial intelligence capabilities to improve cybersecurity," Ieee Access, vol. 8, pp. 23817-23837, 2020.

[5] S. Morgan, "Global cybersecurity spending predicted to exceed $1 trillion from 2017-2021," Cybercrime Magazine, vol. 10, 2019.

[6] S. Rangaraju and S. Ness, "Multifaceted Cybersecurity Strategy for Addressing Complex Challenges in Cloud Environments," International Journal of Innovative Science and Research Technology, vol. 8, pp. 2426-2437, 2023.

[7] H.-S. Ham, H.-H. Kim, M.-S. Kim, and M.-J. Choi, "Linear SVM-based android malware detection for reliable IoT services," Journal of Applied Mathematics, vol. 2014, 2014.

[8] S. Rangaraju, "Secure by Intelligence: Enhancing Products with AI-Driven Security Measures," EPH-International Journal of Science And Engineering, vol. 9, no. 3, pp. 36-41, 2023.

[9] I. Santos, F. Brezo, X. Ugarte-Pedrero, and P. G. Bringas, "Opcode sequences as representation of executables for data-mining-based unknown malware detection," information Sciences, vol. 231, pp. 64-82, 2013.

[10] M. A. Manjramkar and K. C. Jondhale, "Cyber Security Using Machine Learning Techniques," in International Conference on Applications of Machine Intelligence and Data Analytics (ICAMIDA 2022), 2023: Atlantis Press, pp. 680-701.

[11] J. Senanayake, H. Kalutarage, and M. O. Al-Kadri, "Android mobile malware detection using machine learning: A systematic review," Electronics, vol. 10, no. 13, p. 1606, 2021.

[12] R. M. Mohammad, F. Thabtah, and L. McCluskey, "Tutorial and critical analysis of phishing websites methods," Computer Science Review, vol. 17, pp. 1-24, 2015.

[13] S. Rangaraju, "AI Sentry: Reinventing Cybersecurity Through Intelligent Threat Detection," EPH-International Journal of Science And Engineering, vol. 9, no. 3, pp. 30-35, 2023.

[14] A. S. Shatnawi, A. Jaradat, T. B. Yaseen, E. Taqieddin, M. Al-Ayyoub, and D. Mustafa, "An Android malware detection leveraging machine learning," Wireless Communications and Mobile Computing, vol. 2022, 2022.

[15] S. Purkait, "Phishing counter measures and their effectiveness–literature review," Information Management & Computer Security, vol. 20, no. 5, pp. 382-420, 2012.

[16] S. Rangaraju, "A Comprehensive Analysis of GPT Applications in Third-Party Vendor Security Enhancement," Asian Journal of Multidisciplinary Research & Review, vol. 4, no. 6, pp. 105-115, 2023.

[17] P. Wang and Y.-S. Wang, "Malware behavioural detection and vaccine development by using a support vector model classifier," Journal of Computer and System Sciences, vol. 81, no. 6, pp. 1012-1026, 2015.

[18] M. A. Abid, S. Ullah, M. A. Siddique, M. F. Mushtaq, W. Aljedaani, and F. Rustam, "Spam SMS filtering based on text features and supervised machine learning techniques," Multimedia Tools and Applications, vol. 81, no. 28, pp. 39853-39871, 2022.

[19] I. Alsmadi and I. Alhami, "Clustering and classification of email contents," Journal of King Saud University-Computer and Information Sciences, vol. 27, no. 1, pp. 46-57, 2015.

[20] A. D. Kulkarni and L. L. Brown III, "Phishing websites detection using machine learning," 2019.

[21] S. Angra and S. Ahuja, "Machine learning and its applications: A review," in 2017 International Conference on Big Data Analytics and Computational Intelligence (ICBDAC), 2017: IEEE, pp. 57-60.

[22] J. M. Gómez Hidalgo, G. C. Bringas, E. P. Sánz, and F. C. García, "Content based SMS spam filtering," in Proceedings of the 2006 ACM symposium on Document engineering, 2006, pp. 107-114.

[23] T. S. Hyslip and T. J. Holt, "Assessing the capacity of DRDoS-for-hire services in cybercrime markets," Deviant Behavior, vol. 40, no. 12, pp. 1609-1625, 2019.

[24] K. Trieu and Y. Yang, "Artificial intelligence-based password brute force attacks," 2018.

[25] P. M. Churchland and P. S. Churchland, "Could a machine think?," Scientific American, vol. 262, no. 1, pp. 32-39, 1990.

[26] M. Islam and N. K. Chowdhury, "Phishing websites detection using machine learning based classification techniques," in International Conference on Advanced Information and Communication Technology, Chittagong, Bangladesh, 2016.

[27] B. Gonçalves, "Can machines think? The controversy that led to the Turing test," AI & SOCIETY, vol. 38, no. 6, pp. 2499-2509, 2023.

[28] N. F. Shah and P. Kumar, "A comparative analysis of various spam classifications," in Progress in Intelligent Computing Techniques: Theory, Practice, and Applications: Proceedings of ICACNI 2016, Volume 2, 2018: Springer, pp. 265-271.

[29] 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, pp. 1153-1176, 2015.

[30] A. Javaid, Q. Niyaz, W. Sun, and M. Alam, "A deep learning approach for network intrusion detection system," in Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies (formerly BIONETICS), 2016, pp. 21-26.

[31] M. Feng and H. Xu, "Deep reinforecement learning based optimal defense for cyber-physical system in presence of unknown cyber-attack," in 2017 IEEE Symposium Series on Computational Intelligence (SSCI), 2017: IEEE, pp. 1-8.

[32] C.-F. Tsai, Y.-F. Hsu, C.-Y. Lin, and W.-Y. Lin, "Intrusion detection by machine learning: A review," expert systems with applications, vol. 36, no. 10, pp. 11994-12000, 2009.

[33] L. F. Maimó, Á. L. P. Gómez, F. J. G. Clemente, M. G. Pérez, and G. M. Pérez, "A self-adaptive deep learning-based system for anomaly detection in 5G networks," Ieee Access, vol. 6, pp. 7700-7712, 2018.

[34] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," in Proceedings of the IEEE conference on computer vision and pattern recognition, 2016, pp. 770-778.

[35] M. D. Zeiler and R. Fergus, "Visualizing and understanding convolutional networks," in Computer Vision–ECCV 2014: 13th European Conference, Zurich, Switzerland, September 6-12, 2014, Proceedings, Part I 13, 2014: Springer, pp. 818-833.

[36] T. Bayes, "LII. An essay towards solving a problem in the doctrine of chances. By the late Rev. Mr. Bayes, FRS communicated by Mr. Price, in a letter to John Canton, AMFR S," Philosophical transactions of the Royal Society of London, no. 53, pp. 370-418, 1763.

[37] A. S. Pillai, "Cardiac disease prediction with tabular neural network." 2022. doi: 10.5281/zenodo.7750620

[38] Singh, A., Singh, V., Aggarwal, A., & Aggarwal, S. (2022, August). Event Driven Architecture for Message Streaming data driven Microservices systems residing in distributed version control system. In 2022 International Conference on Innovations in Science and Technology for Sustainable Development (ICISTSD) (pp. 308-312). IEEE.

[39] Singh, A., Singh, V., Aggarwal, A., & Aggarwal, S. (2022, November). Improving Business deliveries using Continuous Integration and Continuous Delivery using Jenkins and an Advanced Version control system for Microservices-based system. In 2022 5th International Conference on Multimedia, Signal Processing and Communication Technologies (IMPACT) (pp. 1-4). IEEE.

[40] Singh, Amarjeet, et al. "Event Driven Architecture for Message Streaming data driven Microservices systems residing in distributed version control system." 2022 International Conference on Innovations in Science and Technology for Sustainable Development (ICISTSD). IEEE, 2022.

[41] Singh, Amarjeet, et al. "Improving Business deliveries using Continuous Integration and Continuous Delivery using Jenkins and an Advanced Version control system for Microservices-based system." 2022 5th International Conference on Multimedia, Signal Processing and Communication Technologies (IMPACT). IEEE, 2022.

[42] Palle, Ranadeep Reddy, Haritha Yennapusa, and Krishna Chaitanya Rao Kathala. "Enhancing Cloud-Based Smart Contract Security: A Hybrid AI and Optimization Approach for Vulnerability Prediction in FinTech."

[43] Palle, Ranadeep, and A. Punitha. "Privacy-Preserving Homomorphic Encryption Schemes for Machine Learning in the Cloud."

[44] Palle, Ranadeep Reddy. "Explore the Application of Predictive Analytics and Machine Learning Algorithms in Identifying and Preventing Cyber Threats and Vulnerabilities within Computer Systems."

[45] Palle, R. R., Yennapusa, H., & Kathala, K. C. R. Enhancing Cloud-Based Smart Contract Security: A Hybrid AI and Optimization Approach for Vulnerability Prediction in FinTech.

[46] Palle, R., & Punitha, A. Privacy-Preserving Homomorphic Encryption Schemes for Machine Learning in the Cloud.

[47] Palle, R. R. Explore the Application of Predictive Analytics and Machine Learning Algorithms in Identifying and Preventing Cyber Threats and Vulnerabilities within Computer Systems.