Kandala kalyana Srinivas, et. al. International Journal of Engineering Research and Applications
www.ijera.com
ISSN: 2248-9622, Vol. 12, Issue 6, (Series-V) June 2022, pp. 37-44

RESEARCH ARTICLE OPEN ACCESS

Artificial Intelligence Techniques for Prevention of Cyber Attacks and Detection of Security Threats

Kandala kalyana Srinivas[1], D. Vijay Sai[2], N.Saketh[3], I. Neelima[4], B.Alekhya[5]
Dept. of ECE[1], Dept. of ECE[2], Dept. of ECE[3], Dept. of EEE[4], Dept. of ECE[5]
VNR VJIET, Hyderabad, Telangana.

Abstract— Modern Artificial Intelligence breakthroughs are proving to become the finest alternative for defending against cyber-attacks. Experts are employing artificial intelligence (AI) and its component machine learning as a technique for combating cyber-attacks. Currently, security analysts employ this technology to detect abnormalities, saving time and money for the company. Cyber specialists are facing challenging times in our digital era, especially with the explosion of IoT and connected gadgets. The experts require all available resources to prevent assaults and security flaws, as well as to respond to attacks. Artificial intelligence solutions can improve overall security execution and provide greater security from a rising variety of complex cyber threats, where traditional security systems may be less competent and insufficient. In this study, we look at how human reasoning and AI can be used to improve cyber security. The major goal of this research is to highlight the progress that has been accomplished so far in the field of using AI approaches to combat cyber-attacks.
Keywords— Cyber Security, Security Intelligence, Artificial Intelligence, Machine Learning, Cyber Defense

---

Date of Submission: 13-06-2022 Date of Acceptance: 27-06-2022

I. INTRODUCTION

Artificial intelligence is defined as the ability to think, understand, identify patterns, memorize, make decisions from a variety of options, and learn from experience. Artificial intelligence aims to create a computer that can mimic the capabilities of the human brain, allowing computers to perform all of the tasks that humans do in a fraction of the time. Politics, media, games, and public life have all been impacted by current AI breakthroughs. Artificial Intelligence was used in politics to help make better use of resources, energy, and time during election campaigns to reach the target audience. Today's governments, organizations, and institutions are all vulnerable to cyber-attacks. Around 200 million personal records were exposed as a result of data breaches at the Federal Bureau of Investigation (FBI) and the Department of Homeland Security, including high-profile data releases. At the moment, it's merely a slow and limited attempt to figure out what other people are trying to achieve. According to Forbes, the global market for computer security is expected to reach $170 billion by 2020. Rising technology trends and a flurry of activities that keep security standards updated are the key reasons for the market's rapid growth [21]. Cyber security is a hot topic right now, and it's being used in conjunction with Artificial Intelligence. Cyber security technologies that use artificial intelligence are proven to be more effective at protecting and securing digital data [3].

Fig. 1. AI in cyber security

Artificial Intelligence (AI) has the potential to be extremely useful in combating such dangers as shown in Fig.1.. When it comes to constructing a line of defense against hackers, Artificial Intelligence can be a beneficial ally. Artificial Intelligence can be taught to constantly detect and learn patterns to spot any deviations. Artificial Intelligence relies heavily on machine learning. It constantly improves its operations and develops preventive ways to combat future threats using the data it collects. Its ability to learn and understand human behavior, as well as recognize trends and detect even little deviations from those patterns,

makes it ideal for Cybersecurity. Artificial Intelligence can also make use of this data to construct its plans and functions [4], [30]. Artificial Intelligence's major goal is to develop technology that would allow computer systems to work intelligently. In the context of cybersecurity, AI can be used to quickly and reliably identify new vulnerabilities to prevent future assaults [5], [29].

This technology has the potential to relieve much of the burden now put on human security workers, who are busy, limited in their talents, and prone to error [9].

Machines handle much of the heavy lifting in a cyber-security approach powered by intelligent automation, informing human workers only when action is required [24]. This technology has the potential to relieve much of the burden now put on human security workers, who are busy, limited in their talents, and prone to error [10], [28]. Machines handle much of the heavy lifting in a cyber-security approach powered by intelligent automation, informing human workers only when action is required [20], [27].

II. ARTIFICIAL INTELLIGENCE BASED APPLICATIONS

Artificial intelligence is transforming a variety of industries [22], [26]. According to some estimates, the global market for automation and robotics would be worth $153 million by 2020 [14], [23], [25]. Artificial Intelligence reduces expenses while simultaneously saving time, increasing accuracy, and increasing production [13],[17].

The field of Ai Technology has advanced at a breakneck pace [18]. According to Google, by 2045, robots will have reached human intelligence levels, and one-third of occupations will be done by automation and other intelligent devices [19].

III. ADVANTAGES OF ARTIFICIAL INTELLIGENCE INCYBER SECURITY

Every day, organizations are confronted with millions of risks, making it almost impossible for a cybersecurity firm to define and analyze them. This task can be completed quickly and effectively by utilizing Machine Learning [15].

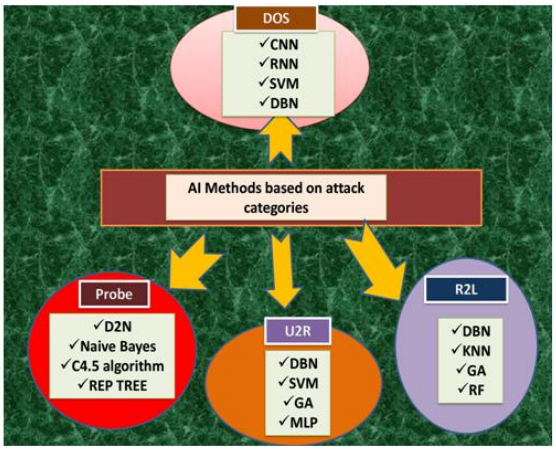

Fig. 2. AI based methods to combat cyber attacks

Organizations will be able to fully leverage the current knowledge of threats and vectors and discover a way to work toward supervised and unsupervised machine learning [16]. When these capabilities are combined with an ability to identify new attacks and find new weaknesses, the systems will be able to safeguard the subjects from dangers in a far more effective and efficient manner with respect to Fig.2.

A. Error reduction

In the vast majority of cases, scientists employ artificial intelligence with the hope and concern of reducing the danger [11]. Additionally, it raises the likelihood of achieving accuracy with a higher degree of precision.

B. Difficult Exploration

Organizations also employ artificial intelligence and robotics science in mining. Other methods of fuel exploration are also available. Furthermore, it uses sophisticated machines to explore the water. As a result, the ocean limitation has been overcome.

C. Daily Application

Computed approaches to learning have become widespread in everyday life. Artificial Intelligence is commonly used by the financial and banking sectors. That is data organization and management. In a smart card-based system, Artificial Intelligence is also utilized to detect fraud users.

D. Digital Assistants

Organizations with superior technology use "avatars." Digital assistants are what they're called. They can also communicate with the users. Hence. They are preserving human resource needs. As a result, it is argued that emotions are linked to mood. They can obscure judgment and reduce human efficiency. Furthermore, machine intelligence is entirely ruled out.

E. No Breaks

Machines do not require frequent breaks and refreshments for humans. As machines are

programmed for long hours. Also, they can continuously perform without getting bored.

F. Increased Work efficiency

AI-powered devices are extremely efficient at specific repetitive tasks. The best part is that they eliminate human mistakes from their tasks to get precise outcomes.

G. Reduced Cost of Training and Operation

Artificial Intelligence methods such as supervised learning and artificial neural are used to learn new information in the same way that people do. Additionally, they avoid the need to develop fresh code each time.

IV. AI AS THE FUTURE OF CYBER SECURITY

Cyber-attacks are one of the most serious challenges facing today's corporations, governments, and institutions. In 2016, data breaches exposed over 200 million personal details, including high-profile thefts at the Department of Homeland Security and the Fbi (FBI).

Ninety-nine percent of exploited vulnerabilities have already been discovered. Unfortunately, we have a reliance on firewalls as a form of protection. Firewalls, on the other hand, will not discourage a determined hacker. For the time being, humans are the only ones who try to predict what the other human will do before they can do it. Therefore with this thought in mind, a few AI-based cyber security techniques are further discussed.

A. AI based Cyber Threat Detection

Cyberattacks are more complicated and unpredictable than they've ever been. As a result, Artificial Intelligence approaches are now being used in Cybersecurity systems. However, no AI model can be said to be 100 percent accurate. As a result, incorrect predictions occur, necessitating human intervention and response. However, keeping up with the continually growing number is becoming increasingly challenging for human analysts. Explainable Artificial Intelligence (XAI) techniques have been developed to address such challenges. There are two aspects to this process. For developing a new model using a training dataset, the first step is to generate the Segment Outlier Score (FOS) information, which is a reliability indicator for AI prediction. The Shapely Additive Explanation (SHAP) model is then used to generate FOS information[1]. It's based on how important each attribute is in AI's training data. The Shapely value extraction formula is as follows:

$$\phi_i = \sum_{s \subseteq F/_j} \frac{|T|!(|F|-|T|-1)!}{|F|!}.(y(T \cup \{j\}) - y(T) \quad (1)$$

Where:

- F corresponds to all the feature sets;
- T is the super set that consists of all the features except j;
- y(x) is a function that denotes contribution corresponding to the subset of x.
- The extraction of relevant features is based on this SHAP plot. They are range processed further by calculating many statistical metrics such as standard deviation.

The computation and assessment of test data based on FOS information for the production of an index related to the AI model's predictability are covered in the second section of the technique. FOS is calculated using the following formula: FOS`=| $F_x(x)$- 0.5|*2

$$= |([\sum_{k=1}^{x}[1-p]^{k-1} - p) - 0.5| * 2] \quad (2)$$

Where:

- p denotes specific label prediction probability.
- X denotes a random variable.

$F_x(x)$ represents the CDF of X. P_x ($X \leq x$) (Here, P_x is the defined probability of x).

The difficulty of requiring a professional analyst to participate and respond to erroneous predictions has been satisfactorily solved by this strategy. The model outperformed other current models on the malware dataset by delivering 114 percent superior efficiency on IDS and 94 percent better performance on harmful code.

B. AI based counter measures for IOT network

The Internet of Things (IoT) is one of the world's fastest-growing technologies. Security worries surrounding IoT networks have grown in popularity in recent years. IoT devices are frequently regarded as weak points and have become easy targets for cyber criminals[2]. Artificial Intelligence-based solutions, in addition to current conventional network protocols, can be used to improve the security of IoT networks. The Table 1. Shows the various attacks in IOT environment.

The IoT network architecture is divided into five tiers, each with its own set of vulnerabilities and solutions, as detailed below and as shown in Fig.3.:

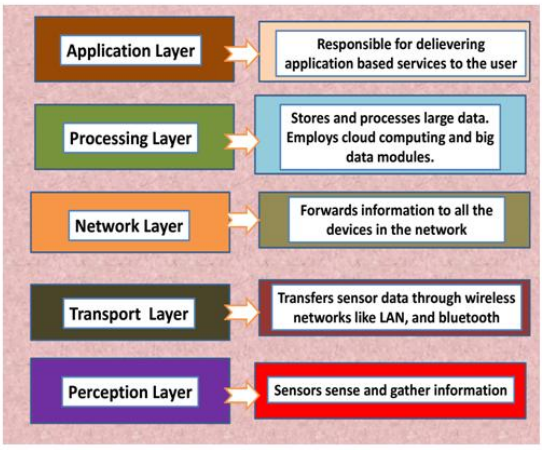

Fig. 3. Layers in an IOT network

Perception Layer: The first layer is the perception layer. It is also known as the sensor layer because it is in charge of collecting data and then sending it to higher levels. Its vulnerability to jamming makes it easier for cybercriminals to gain access. With a confidence level of over 95%, SVM and Controller AI algorithms can be utilized to secure this layer.

Network Layer*:* This layer collects data and sends it to network intermediary devices. This layer is subject to wormhole attacks, rank assaults, reply attacks, and other types of attacks. KN, LVSM, and NN are examples of AI-based detection approaches. Binary classification is 99 percent effective in detecting attacks.

Transport Layer*:* This layer analyses the received data and communicates with the upper layer. Cyber attackers most typically deploy flooding or denial-of-service (DoS) attacks. To detect the attacks, AI approaches such as the Neuro multi fuzzy classification algorithm, RNN, and NN algorithms are used.

TABLE 1. Types of cyber attacks in IOT environment

Attack Category	Attack types
Probe	Mscan, portsweep, satan, nmap
UTR	Httptunnel, sql attack, load module, root kit
R2L	Worm, snmpgeattack, imap, warzemaster
DOS	Processtable, udp storm, Neptune, teardrop

Processing Layer: This layer is in charge of acquiring data and passing it on to the upper layer. In most cases, it's a data server. This layer is vulnerable to fog-based assaults, code injection attacks, and evasion attacks.Artificial intelligence techniques such as soft-max regression and two-class logistic regression are effective against attacks.

Application Layer: This is the topmost abstract layer, which varies by application. The most typical threats on this layer are phishing and malicious code injection. Many anti-phishing methodologies based on SVM, AdaBoost, and RF classifiers are already in use to detect and mitigate attacks with greater than 90% accuracy.

C. Resilient ML for networked cyber-physical systems

Many processes that formerly required human intervention have been automated thanks to Cyber-Physical Systems. In addition to computation and IoT connectivity, CPS has gone a step further by being able to undertake control actions. This has increased the risk of a cyberattack by broadening the attack surface. This necessitates the use of resilient machine learning models.

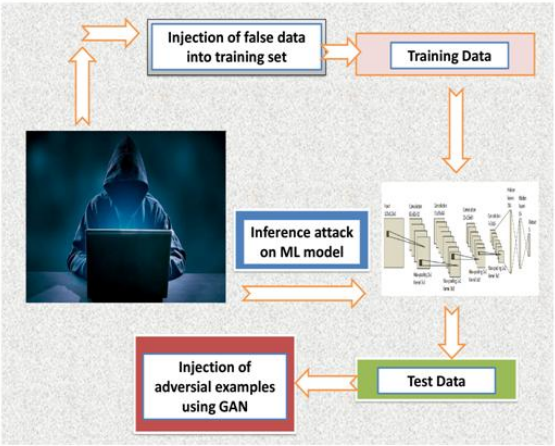

Fig. 4. Cyber attacks on ML models

One of the most pressing concerns in CPS is the early detection of threats. This allows for the mitigation of harm in the event of a cyberattack. The use of machine learning techniques in the detection of assaults in CPS overcomes all of the drawbacks of state-space models like the Kalman filter[6]. Cybercriminals devise several methods to deceive the ML model, including data poisoning, which causes the model to make incorrect classifications as shown in Fig.4..

As a result, it's critical to make the ML models themselves resistant to attacks. This can be accomplished in three ways: adversarial training, defensive distillation, and defense against hostile examples.

A. Adversarial Training: The purpose of this strategy is to reduce the module's worst-case mistake when there is a data anomaly during a cyberattack. This strategy has a high success rate

and makes the machine learning model resistant to attacks.

B. Randomization at Inference Using Random Resizing: The method discusses randomization at inference using random resizing to make the model more resistant to attacks.

C. Defensive Distillation: There are three primary processes in this procedure. The first is to train the network conventionally. Then it must be thoroughly analyzed to obtain soft labels. Then, using the previously created labels, another distillation network is trained. This strategy is particularly good at generating a durable machine learning model.

D. Information theory techniques to detect Cyber attacks

To avoid potential cyber-attacks, it's critical to understand the system and the steps that must be taken to protect it. This procedure requires the processing of a huge number of data sets, all of which are recordings of previous data, in a short amount of time. All of this necessitates a massive storage capacity.

Normalizing the data sets is also a time-consuming process. Due to these issues, the use of artificial intelligence security solutions is extremely limited. To overcome these issues, huge data sets must be shrunk, increasing processing performance. This can be accomplished by generating tiny sample sets[7]. There are certain practical issues when utilizing stochastic models, such as the necessity to assume that the model is time-invariant, which is not true in the real world because physical conditions vary with time.

To address the aforementioned issues, information theory techniques might be incorporated into the earlier methodologies utilized by SROM models. The distributions changes are examined with time but remain constant within a window, say, T, by employing information theory approaches (win).Each sub-data set is treated as a matrix, with rows indicating time instants and columns indicating distinct devices. Later on, a temporal window is considered since the process is stationary within the window and the matrix is processed column by column. After that, the spectral analysis is carried out and the reduced dataset is calculated of 2M items per time window and device column, or per device or time window, or for all devices, all-time windows to generate the reduced data set.

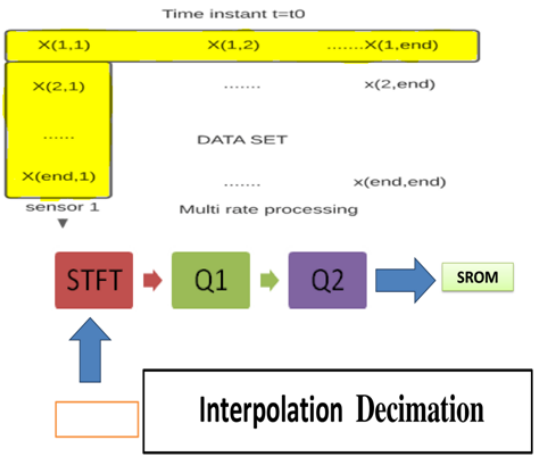

Fig. 5. Process of reducing data sets using information techniques

As illustrated in the Fig.5., the full method can be carried out.

E. Cyber threat detection based on ANN

In most cases, an intrusion prevention system is utilized to detect cyber threats and intrusions in networks.

Any incursion action triggers a signal from this system. SIEM (security information and event management) is the most commonly used tool for managing the warnings generated by an intrusion prevention system (IPS). Because of the large number of false alarms and the large volume of data, identifying intrusions with substantial precision using this method is exceedingly difficult. Models that have been trained using historical threat detection data can be utilized to detect threats using artificial intelligence and machine learning methodologies.

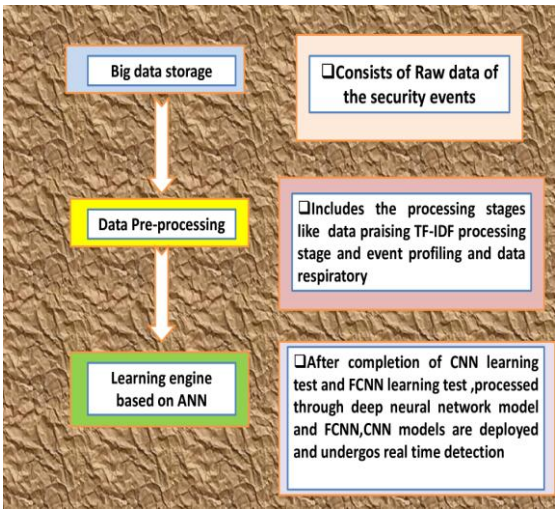

Fig. 6. Process of ANN based threat detection

The fundamental goal of an artificial intelligence-based SIEM is to analyze the network's security and identify actual cyber threat alerts with improved efficiency.

There are three basic steps in this procedure. The raw data is first adjusted using deep neural networks. The TF-IDF method can be used to accomplish this[8]. Each stage's output is used in the subsequent stage. Artificial neural networks are fed to the preprocessed data and are taught to find the most efficient model. The risk raw event is categorized using this model, which improves the efficiency of security alerts. The complete technique is carried out as illustrated in the Fig.6.

F. Cyber security aspect in Smart Airports

Internet of things is one of the booming technologies in today's world. So many sectors started to implement internet of things-based systems. One of the major sectors to implement these automation systems is aviation. This led to the emergence of smart airports which use systems made up of sensors and actuators which are interconnected which results in the automation of the different processes such as e-gates. Generally, Passengers are required to go through a verification process before boarding the flight which includes verifying their passports, etc.

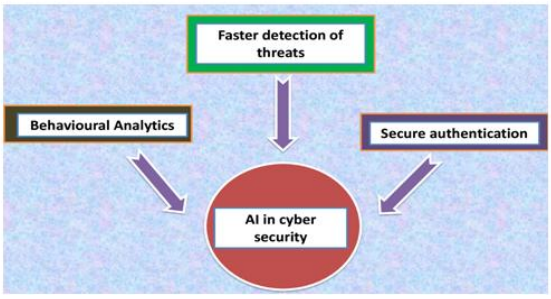

Fig.7. Applications of AI in cyber security

To avoid this time taking and tedious task modern-day airports are implementing e-gates which include acquiring biometric data from the passengers and also immigration servers, etc. Though this method expedites the verification process, it is extremely vulnerable to attackers who could try to tamper with the gates or gain access to the airport's intranet and launch DOS attacks, resulting in serious consequences such as the compromise of sensitive passenger information and, worse, the attackers framing innocent passengers as criminals. There are also systems such as luggage tracking, automated check-in, and so on[12]. Which are likewise subject to cyber-attacks of this nature. To combat these activities, airports have begun to implement AI-based cyber defense tools. Traditionally, anti-malware software relies on rule-based engines, but due to recent advancements, firewalls now rely on ANN and also neural networks such as deep Armor, which protects against malware and zero-day exploits using machine learning models. Networks are studied and their vulnerabilities against various assaults are detected using machine learning and deep learning devices, as shown in the Fig.7.

V. CONCLUSION AND FUTURE SCOPE

Artificial Intelligence is improving the security of organizations and individuals, but it is also putting greater power in the hands of the wrong people. To give Artificial Intelligence more responsibility shortly for security considerations, we must ensure that it remains in the hands of only white hat personnel. Artificial intelligence is without a doubt infinite, brilliant, and faster than humans, yet it needs a human touch to get started. As a result, businesses must concentrate their efforts primarily on finding and educating Artificial intelligence agencies that can collaborate with the machine to ensure product safety.

Combining the human intellect with artificial intelligence would undoubtedly aid in the fight against hackers. To summarise, ai technology is beginning to play an increasingly critical role in how businesses protect their network and sensitive data. It's of little surprise that cybersecurity is a priority for all organizations, more so at a time when the world is moving towards digitalization. AI consultants and top RPA vendors are keenly building advanced solutions to provide a profound and strong defense mechanism. With AI-powered tools here are a few predictions on how AI will change cybersecurity:

- Using artificial intelligence (AI) to track security occurrences
- Machine learning will be integrated into firewalls to detect any anomalies.
- Using natural language processing (NLP) tools, determining the source of cyber attacks
- Robotic process automation (RPA) bots are used to automate rule-based tasks and procedures.
- Cyber risks are monitored and analyzed on mobile endpoints.

REFERENCES

[1]. Kim, Y. Lee, E. Lee and T. Lee, "Cost-Effective Valuable Data Detection Based on the Reliability of Artificial Intelligence," in IEEE Access, vol. 9, pp. 108959-108974, 2021, doi: 10.1109/ACCESS.2021.3101257.

[2]. S. Zaman et al., "Security Threats and Artificial Intelligence Based

Countermeasures for Internet of Things Networks: A Comprehensive Survey," in IEEE Access, vol. 9, pp. 94668-94690, 2021, doi: 10.1109/ACCESS.2021.3089681.

[3]. Li, K. Ota, M. Dong, J. Wu and J. Li, "DeSVig: Decentralized Swift Vigilance Against Adversarial Attacks in Industrial Artificial Intelligence Systems," in IEEE Transactions on Industrial Informatics, vol. 16, no. 5, pp. 3267-3277, May 2020, doi: 10.1109/TII.2019.2951766.

[4]. X. Qiu, Z. Du and X. Sun, "Artificial Intelligence-Based Security Authentication: Applications in Wireless Multimedia Networks," in IEEE Access, vol. 7, pp. 172004- 172011, 2019, doi: 10.1109/ACCESS.2019.2956480.

[5]. F. Farivar, M. S. Haghighi, A. Jolfaei and M. Alazab, "Artificial Intelligence for Detection, Estimation, and Compensation of Malicious Attacks in Nonlinear Cyber-Physical Systems and Industrial IoT," in IEEE Transactions on Industrial Informatics, vol. 16, no. 4, pp. 2716-2725, April 2020, doi: 10.1109/TII.2019.2956474.

[6]. F. O. Olowononi, D. B. Rawat and C. Liu, "Resilient Machine Learning for Networked Cyber Physical Systems: A Survey for Machine Learning Security to Securing Machine Learning for CPS," in IEEE Communications Surveys & Tutorials, vol. 23, no. 1, pp. 524-552, Firstquarter 2021, doi: 10.1109/COMST.2020.3036778.

[7]. B. Bordel, R. Alcarria, T. Robles and Á. Sánchez-Picot, "Stochastic and Information Theory Techniques to Reduce Large Datasets and Detect Cyberattacks in Ambient Intelligence Environments," in IEEE Access, vol. 6, pp. 34896-34910, 2018, doi: 10.1109/ACCESS.2018.2848100.

[8]. Lee, J. Kim, I. Kim and K. Han, "Cyber Threat Detection Based on Artificial Neural Networks Using Event Profiles," in IEEE Access, vol. 7, pp. 165607-165626, 2019, doi: 10.1109/ACCESS.2019.2953095.

[9]. B. Thuraisingham, "Cyber Security and Artificial Intelligence for Cloud-based Internet of Transportation Systems," 2020 7th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2020 6th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), 2020, pp. 8-10, doi: 10.1109/CSCloud-EdgeCom49738.2020.00011.

[10]. B. Thuraisingham, "The Role of Artificial Intelligence and Cyber Security for Social Media," 2020 IEEE International Parallel and Distributed Processing Symposium Workshops (IPDPSW), 2020, pp. 1-3, doi: 10.1109/IPDPSW50202.2020.00184.

[11]. KANIMOZHI AND T. P. JACOB, "ARTIFICIAL INTELLIGENCE BASED NETWORK INTRUSION DETECTION WITH HYPER-PARAMETER OPTIMIZATION TUNING ON THE REALISTIC CYBER DATASET CSE-CIC-IDS2018 USING CLOUD COMPUTING," 2019 INTERNATIONAL CONFERENCE ON COMMUNICATION AND SIGNAL PROCESSING (ICCSP), 2019, PP. 0033-0036, DOI: 10.1109/ICCSP.2019.8698029.

[12]. N. Koroniotis, N. Moustafa, F. Schiliro, P. Gauravaram and H. Janicke, "A Holistic Review of Cybersecurity and Reliability Perspectives in Smart Airports," in IEEE Access, vol. 8, pp. 209802-209834, 2020, doi: 10.1109/ACCESS.2020.3036728.

[13]. N. Parati, L. Malik and A. G. Joshi, "Artificial Intelligence Based Threat Prevention and Sensing Engine: Architecture and Design Issues," 2008 First International Conference on Emerging Trends in Engineering and Technology, 2008, pp. 304-307, doi: 10.1109/ICETET.2008.52.

[14]. Q. Zhao, J. Sun, H. Ren and G. Sun, "Machine-Learning Based TCP Security Action Prediction," 2020 5th International Conference on Mechanical, Control and Computer Engineering (ICMCCE), 2020, pp. 1329-1333, doi: 10.1109/ICMCCE51767.2020.00291.

[15]. Sathya, J. Premalatha and S. Suwathika, "Reinforcing Cyber World Security with Deep Learning Approaches," 2020 International Conference on Communication and Signal Processing (ICCSP), 2020, pp. 0766-0769, doi: 10.1109/ICCSP48568.2020.9182067.

[16]. V. S. Sree, C. S. Koganti, S. K. Kalyana and P. Anudeep, "Artificial Intelligence Based Predictive Threat Hunting In The Field of Cyber Security," 2021 2nd Global Conference for Advancement in Technology (GCAT), 2021, pp. 1-6, doi: 10.1109/GCAT52182.2021.9587507.

[17]. S. Vadupu, K. S. Kandala, A. Peddi, N. S. Yadav, G. V. Kumar and P. A. Harsha Vardhini, "Skin Pathology Detection Using

Artificial Intelligence," 2021 6th International Conference on Signal Processing, Computing and Control (ISPCC), 2021, pp. 373-376, doi: 10.1109/ISPCC53510.2021.9609516.

[18]. B. V. Kumar, K. K. Srinivas, P. Anudeep, N. S. Yadav, G. V. Kumar and P. A. Harsha Vardhini, "Artificial Intelligence Based Algorithms for Driver Distraction Detection: A Review," 2021 6th International Conference on Signal Processing, Computing and Control (ISPCC), 2021, pp. 383-386, doi: 10.1109/ISPCC53510.2021.9609349.

[19]. N. Karennagari, K. Yashwanth Reddy, V. K. Gurrala, K. Srinivas, A. Peddi and Y. Padma Sai., "Infection Segmentation of Leaves Using Deep Learning techniques to enhance crop productivity in smart agriculture," 2021 6th International Conference on Signal Processing, Computing and Control (ISPCC), 2021, pp. 368-372, doi: 10.1109/ISPCC53510.2021.9609379.

[20]. R. S. Krishna, K. K. Srinivas, P. Anudeep and P. A. H. Vardhini, "Ear-Based Biometric System Using Artificial Intelligence," 2021 6th International Conference on Signal Processing, Computing and Control (ISPCC), 2021, pp. 377-382, doi: 10.1109/ISPCC53510.2021.9609409.

[21]. G. A. Chandra, K. K. Srinivas, P. Anudeep, S. R. Prasad, Y. Padmasai and P. Kishore, "Mental Health Disorder Analysis Using Convolution Neural Network Based Speech Signal Model With Integration Of Artificial Intelligence," 2021 4th International Conference on Recent Developments in Control, Automation & Power Engineering (RDCAPE), 2021, pp. 544-547, doi: 10.1109/RDCAPE52977.2021.9633637.

[22]. P. Koganti, K. S. K, A. P, S. K. R, P. Kishore and S. R. Prasad, "Satellite based Road Tagger GPS Radio-Navigation system with Integration of Artificial Intelligence," 2021 4th International Conference on Recent Developments in Control, Automation & Power Engineering (RDCAPE), 2021, pp. 536-539, doi: 10.1109/RDCAPE52977.2021.9633626.

[23]. P. Singh, K. K. Srinivas, A. Peddi, B. Shabarinath, I. Neelima and K. A. Bhagavathi, "Artificial Intelligence based Early Detection and Timely Diagnosis of Mental Illness - A Review," 2022 International Mobile and Embedded Technology Conference (MECON), 2022, pp. 282-286, doi: 10.1109/MECON53876.2022.9752219.

[24]. V. S. Sree, C. S. Koganti, S. K. Kalyana and P. Anudeep, "Artificial Intelligence Based Predictive Threat Hunting In The Field of Cyber Security," 2021 2nd Global Conference for Advancement in Technology (GCAT), 2021, pp. 1-6, doi: 10.1109/GCAT52182.2021.9587507.

[25]. K. Srinivas, U. Vijitha, G. A. Chandra, K. S. Kumar, A. Peddi and B. S. Uppala, "Artificial Intelligence based Optimal Biometric Security System Using Palm Veins," 2022 International Mobile and Embedded Technology Conference (MECON), 2022, pp. 287-291, doi: 10.1109/MECON53876.2022.9752324.

[26]. S. Kandala et al., "Artificial Intelligence based Techniques for COVID-19 Vaccinations – A Review," 2022 International Mobile and Embedded Technology Conference (MECON), 2022, pp. 337-342, doi: 10.1109/MECON53876.2022.9752112.

[27]. K. K. Srinivas, A. Peddi, B. G. S. Srinivas, P. A. H. Vardhini, H. L. P. Prasad and S. K. Choudhary, "Artificial Intelligence Techniques for Chatbot Applications," 2022 International Mobile and Embedded Technology Conference (MECON), 2022, pp. 292-296, doi: 10.1109/MECON53876.2022.9751887.

[28]. K. K. Srinivas, A. Peddi, S. K. Ramakuri, P. A. H. Vardhini, P. S. Avinash and R. Sirimalla, "Artificial Intelligence-Driven Techniques to Advanced Signals and Communication Systems," 2022 International Mobile and Embedded Technology Conference (MECON), 2022, pp. 307-310, doi: 10.1109/MECON53876.2022.9752011.

[29]. K. K. Srinivas, P. Vangara, R. Thiparapu, R. Sravanth Kumar and K. A. Bhagavathi, "Artificial Intelligence based Forecasting Techniques for the Covid-19 pandemic," 2022 International Mobile and Embedded Technology Conference (MECON), 2022, pp. 297-301, doi: 10.1109/MECON53876.2022.9752240.

[30]. J. Kuppala, K. K. Srinivas, P. Anudeep, R. S. Kumar and P. A. H. Vardhini, "Benefits of Artificial Intelligence in the Legal System and Law Enforcement," 2022 International Mobile and Embedded Technology Conference (MECON), 2022, pp. 221-225, doi: 10.1109/MECON53876.2022.9752352.