

Bibliometric and Systematic Review of Artificial Intelligence (AI) Applications in Cyber Threat Intelligence (AACTI) Publications

Eke Roberts Ndukwe¹ and Onyegebu Laetitia Nneka²

¹Information Systems Engineering, Center of Information & Communication Technology, University of Port Harcourt, Rivers State, Nigeria. ²Computer Science Department, Faculty of Computing, University of Port Harcourt, Nigeria.

Corresponding author: ekenroberts@gmail.com

Abstract

The rise in cyber threat has overwhelmed the monetary resources and human ability to analyze and combat every new form of such threats in the Critical industries e.g. financial sector. As digital presence is increasing, there is a large amount of personal and financial information that should be protected from cyber threat. Cyber threat can ruin the reputation of an organization or letdown the organization completely. This paper reviews AI applications on cyber threat intelligence publications. It compared the different AI techniques employed and the types of attack. The study adopted the bibliometric and systematic literature review method, and data (160KB) were sourced from Scopus, researchgates, googlescholar and academia between 2007 to 2023. The review revealed that application of AI in controlling cyber threat has advantages and disadvantages; however, the advantages outweigh the disadvantages. It was observed that with the speedy and efficient technology required to operate AI systems, they are likely to improve the protection of customers and businesses in the cyberspace. This is proven by the increasing deployment of AI engines rather than conventional scanning engines in cyber security. However, the AI techniques used are limited to machine learning and deep learning, whereas deep reinforcement learning is yet to be effectively explored.

Keywords: cyber threat intelligence; artificial intelligence; systematic review; publications.

Introduction

Recently, the entire scholarly world and businesses have paid intense consideration to cyber threat intelligence. It is important to note that the idea is not new, as it has truly contributed significantly to maintaining network security for many years, as computers have been able to communicate. As opposed to being merely data, intelligence also includes the ultimate result of investigation and must be actionable in order to meet the demands of present-day security mechanisms designed to cope with and respond to attacks via the internet. Intelligence can be thought of as the knowledge and information gained about an attacker through investigation and evaluation. Brown *et al.* (2015) demonstrates the ongoing need for obtaining more threat intelligence and the predicament in successfully handling huge quantities of data. There is a relationship between data, information and intelligence. To get maximum value from threat reconnaissance structures and protection, it is essential to comprehend the stark differences among noise, vulnerability data, information, and

cognitive ability. Following is a summary of cyberthreats that come under the broad category mentioned previously:

Malware is a type of malicious software created by cybercriminals or hackers to disrupt or damage the computer of a legitimate user. It can take many different forms, including

- **Viruses** – a bit of computer code that can copy itself, attaches to clean files, spreads throughout a computer system, infects files, and corrupts data
- **Trojans** – Malware that sneaks onto a computer by masquerading as trusted software. Cybercriminals trick people into installing Trojans on their computers in order to harm them or collect data.
- **Spyware** – This type of malware aims to gather data on a person or organization and communicate it to another party in a way that harms the user, frequently without the user's awareness. For instance, it might steal credit card information.
- **Ransomware** – a type of malicious software that prevents users from accessing their files and data while threatening to delete it if they fail to pay a ransom.
- **Adware** - sometimes known as software funded by advertisements, is a type of program that can propagate malware.
- **Server Query Language (SQL) injection** – a sort of cyberattack used by cybercriminals to attack data-driven systems. In this attack, malicious SQL statements are put into an entry field and allowed to run. As a result, they have access to the database's sensitive information.
- **Phishing** – is the practice of cybercriminals attempting to get sensitive information or data, such as usernames, passwords, credit cards, etc., through emails that look to be sent from a trustworthy source.
- **Man-in-the-middle attacks (MitM)** – are eavesdropping attacks/attempts that requires for the attacker to intercept and transmit messages between two parties that erroneously believe they are speaking with one another. We can use the situation where a hacker could intercept data being sent between the victim's device and the network on an insecure WiFi network as an example.

The Distributed Denial-of-Service (DDoS) Attack

An availability-dependent invasion is a cyber-attack launched by an unsavory actor with the intention of destabilizing an online service. One of the most significant security issues impacting websites is availability-centered assaults, which employ an assortment of channels of attack (low-flow raids, TCP & HTTP/S floods, SSL attacks, etc.). The well-nigh recurrent kind of strikes have been denial-of-service (DoS) assaults. In a DoS attack, the attacker overwhelms the target with numerous requests or data, exhausting its processing or network assets and preventing access by genuine users. To put it simply, a DoS attack happens when an intruder uses the resources of one machine to drain the resources of another, stopping it from functioning normally. A straightforward DoS attack via just one computer won't cause large web servers to function worse (Radware, 2016). On the

opposite hand, offenders who employ numerous machines to increase their effectiveness routinely launch DDoS assaults. Distributed DoS attacks have only really been around since the latter part of June to the beginning of July 1999. The first known DDoS attack appears to have taken place in August 1999 when a solitary University of Minnesota computer was taken inaccessible for over two days using the DDoS utility Trinoo (Kessler C. Gary, 2000). When numerous attacker machines are used to carry out an attack, it is referred to as a distributed denial-of-service (DDoS) attack. In order to decimate the targeted machine of network capabilities like memory, CPU, or link connectivity, a large number of compromised devices identified as zombies or bots will initiate a threat described as a distributed denial-of-service (DDoS) flooding operation. DDoS attacks may be further categorized according to the fact that the attack data is sent straight to the target or via middlemen. In a direct assault, the attacker sends attack communications to the object of attack directly using an enormous amount of infiltrated workstations. In contrast, an indirect attack attacks the connections between itself and additional functions which the casualty depends on to function, as opposed to striking the victim explicitly. Instances of secondary DDoS onslaughts include link flooding attacks such as crossfire attacks (Jing *et al.*, 2018; Misra *et al.*, 2017) core melt attacks, (Wang *et al.*, 2018; Yang *et al.*, 2018). The shortcomings of traditional cybersecurity methods have largely been overcome thanks to a variety of new innovations. These tools include Big Data, Blockchain, and Behavioral Analytics, for instances. Big Data technology can be used to identify anomaly-based infiltration and scams in the realm of cybersecurity. The fundamental prerequisite for anomaly-based detection of breaches approaches is a software framework with reasoning processes. In a typical behavior-based solution, discrepancies away from the acquired model are discovered by observing user actions, network data, or native systemic issues engagement. Typically, the models are separated into two categories: legitimate incursion and abnormal penetration. Every time a legitimate pattern deviates to aberrant markings, it is regarded as an abnormal intrusion. (Razaq *et al.*, 2016). The deuce main techniques applied to fraud identification employing big data are (i) statistical analysis and (ii) artificial intelligence. (Bajpai & Arushi, 2018).

Artificial Intelligence

The manner in which Machine Learning (ML), Deep Learning (DL), and Artificial Intelligence (AI) relate to one another and what their connection is are certain of queries and areas of uncertainty. Artificial intelligence (AI) expansion started in the mid- of the 20th century, making it a comparatively recent occurrence. Nevertheless, the idea that made-up sculptures might be intelligent and emotional has a long history and is portrayed in Greek and Egyptian myths. (McCorduck, 1979). A symposium conducted in 1956 at Dartmouth College is often cited as the catalyst for AI research. At this meeting, Marvin Minsky and John McCarthy coined the term "artificial intelligence" to distinguish it from related disciplines like cybernetics. (Haenlein & Kaplan, 2019). Through this duration, AI technology

had advanced to the extent during it was regardless capable of speaking English and resolving algebraic problems. By the middle of the 1960s, the U.S. Department of Defense had significantly increased funding for AI studies owing to the confidence of the period. (Russell & Norvig, 2021). Unfortunately, the early enthusiasm for this emerging science did not endure, and in the 1970s, enthusiasm for AI technology began to wane. In the 1980s, the development of artificial intelligence platforms saw short growth. Nevertheless, a handful of contemporary technological advances in the late 1980s were additionally operationally as well as commercially feasible, so this revival was only momentary. This marked the start of a second break-in AI development. (Russell & Norvig, 2021). In the later 1990s and earlier 2000s, AI technology underwent a further resurgence. During this period, a handful of uses for AI was identified which involve data mining, logistics, and medical evaluation. (Russell & Norvig, 2003).

In a logical sense, artificial intelligence (AI) is a contemporary technological science that investigates and creates concepts, approaches, tools, and implementations to mimic, supplement, and enhance mankind's intelligence. (Smith & Eckroth, 2017). It has a branch of computer science that seeks to understand the fundamentals of intelligence and develop new types of clever machines that act like people. This field includes research in the fields of robotics, computer vision, natural language processing, and specialist systems. AI is capable to replicate the communication flow that powers human cognition and perception. AI has the ability to outperform human intelligence even though it provides not yet match it.

Application of AI in Cyber Threat Intelligence

AI has a significant impact upon both sociological and commercial advancement (Tegmark, 2017). Additionally, it has emerged as one of the main technologies of technological advancement, opening up both possibilities and potential hazards. According to a Gartner survey (Costello, 2019), 37% many businesses have previously used AI in several capacities. AI is regarded as having a "dual-use perspective" in the information and cyber security fields, which means it may be executed to reinforce cyber defenses as well as improve intrusions. (Müller-Quade *et al.*, 2019). Positively speaking, AI can be deployed to defend in opposition to cyberthreats. (Costello, 2019). Malware, spam, phishing emails, and DDoS can all be spotted more precisely thanks to AI. This has the potential to greatly improve ICT security. At the same time, AI has the potential to greatly increase the efficiency and scalability of cyberattacks. AI monitors whether a password is written down or when the user logs in for the first time to look for behavioural anomalies that criminals are anticipated to exhibit. (Hosseini *et al.*, 2011). AI is able to spot tiny hints that could possibly normally go unobserved and can impede the hacker collective's progress. Human hackers will persist to look for weaknesses in all systems, encompassing AI, in the continuous game of cybercrime chess. Because it is human-controlled, artificial intelligence can still be defeated. essentially AI is exceptional in its propensity to integrate and synthesize data, it might solely work as

well as it was intended (Hosseini *et al.*, 2011). The coders will need to implement new preventive mechanisms as hackers adapt to the Artificial Intelligence algorithms (Roy *et al.*, 2017).

The foundation for our present-day pervasive AI use proved specifically laid in the 20th century, which established Artificial Intelligence as a distinct study realm (Russell, 2010). The advancements achieved in machine learning, particularly in deep learning, are directly responsible for the decade's accelerated growth. (Tegmark, 2017). The improved efficiency of IT networks, the vastly expanded amount and quality of information the developing AI training, and the development of greater effective AI procedures are additional factors driving the elevated use of AI innovations (Pohlmann, 2019) in addition to the expanded info accessibility (Christen *et al.*, 2020). AI is likewise known as preventive AI whenever it is employing in a good way to defend towards cyber threats. (Mirsky *et al.*, 2022). The main objective of cyber defense is to fend off internet attacks and safeguard the availability, integrity, and secrecy of a company's ICT network and infrastructure. Conventional security infrastructures, like those used to protect data packages, operate on the premise of guidelines or identifiers without examining the substance or context-specific conduct. Standard signature-based security solutions for malware detection exclusively catches between 75% and 95% of untargated massive malware assaults and merely 27% of focused malware cyber-attacks (Pohlmann, 2019a). When adversaries also employ AI techniques to target ICT equipment, the recognition frequencies of ICT systems without any measure of AI are unable to be maintained at the identical standard of assurance and prevention (Pohlmann, 2019a). Owing to its traits and abilities, AI has the potential to significantly impact the cyber defense field when used successfully. Convolutional Neural Networks, Linear Regression (LR), k-Nearest-Neighbor (kNN), Random Forest (RF), k-Means, and Support-Vector Machines (SVM) are AI techniques with enhanced utility against cyber threats [Pohlmann, 2019b]. Contingent on data integrity and reliability, these approaches each have benefits and downsides. (Li, 2018). In addition to its efficiency in evaluating broad data volumes (such as log files); sequence examination and identification, anomaly tracking (such as 10,000 login attempts per second which indicates the possibility of a cyberattack), pattern estimation and predict (such as an impending server shutdown), clustering and categorization and pattern recognition, AI is a beneficial technological advance in cyber threat intelligence and for knowledge safeguarding in generally. (e.g., malware, or spam email). Few applications of AI in cyber threat intelligence having the author(s), the cyber threat type, method & result and the AI technique were summarized in below literature review

Krishnan Sadhasivan and Balasubramanian (2017) - Network intrusion - A novel adaptive governed by rules multi-agent IDS for secure data transfer inside a network was described in the paper. For the purpose of creating rules, the suggested approach was combined with different multi-agent systems. 41 characteristics and 99 data from the KDD cup were used.

After that, the method recommended was used, and the results produced a precision of 97.47%. [Multi-agent system].

Pamukov (2017) - IoT network intrusion – In this study, a number of appealing features of an AIS-based IDS to feed IoT were found, including propagated designing, self-governing, compact size, operator independent incident management, affordability, and efficiency between Inter-IDS instances. Ultimately, a hierarchical layering strategy was implemented, during which the vulnerability revealing layer deployed NSA locally on energy inhibited gadgets and the knowledge consolidation layer used DT to handle the complexity of a vast network of interlinked NSA infrastructure. [Artificial immune system].

(Hodo *et al.*, 2016) - Threat analysis - demonstrated an artificial neural network to find intrusion in the Internet of Things network. One input layer, one concealed layer, and one output layer made up the suggested model. Both a backwards learning algorithm and a feedforward method were used to train the suggested model. The suggested model was successful in recognizing the intrusions with a confidence of 99.4% and a low erroneous probability. [Neural network (ANN)].

Roy *et al.* (2017) - Network Intrusion - a deep neural network has been advocated for identifying intrusion attempts. A multi-level feed-forward neural network with two hidden layers made up the suggested model. The network's weightings were learned using a backpropagation technique. SVM underperformed the suggested model in terms of accuracy and error. Having an overall error rate of 0.0961%, it acquired an accuracy of 99.99%. [Neural network (ANN)]

Aldhaheeri *et al.* (2020) - IoT Network intrusion - showed a brand-new blended approach that makes use of a dendritic cell algorithm and deep learning. The model's primary goals were to increase productivity and lower false-positive rates in order to minimize the number of erroneous notifications in the IoT network. The most crucial aspects of the data were selected by the proposed model using the information gain technique. The signal was categorized as either Danger or Safe using signal categorization. In order to guarantee that neurons' output falls within the range of 0 to 100, Selu relied on as the activation function. For DoS, DDoS, surveillance, and information vandalism, the suggested methodology was capable of achieving accuracy levels of 99.8%, 99.9%, 99.10%, and 98.56%, correspondingly (Artificial immune system DeepDCA).

The majority of exchange of knowledge devices, particularly mobile networks, are at a extraordinary security risk, according to weaknesses and breaches of security, identifying supplies is the fundamental step in analyzing a system's security or determining risks.

Statement of Research Problem

Finding a thorough strategy that is ideal for perilous situations in cyber-attacks is highly important. This supports the use of the most advanced technique for anticipating information security risks and subsequently mitigating them whenever necessary. The potential attack situations and the intended target may also influence the ideal design. As

a result, adequate study is needed to address electronic information security. As discussed in the following segments, as cyberattacks, especially those targeting mobile networks, rise in frequency, so do our systems' abilities to defend against them. The basic categorization of artificial intelligence methods is shown in Figure 1. However, the intersection of artificial intelligence and cybersecurity spans a wide range of academic disciplines. The methods of deep learning have the potential to be used to create complex models for malware categorization, cyber threat perception, and recognition of intrusions in a wireless network. To reduce shortcomings, improve the confidentiality of data, and allow secure collaborative learning surroundings, AI models need dedicated cybersecurity and safeguarding resolutions. Kong (2013). Many variant disciplines, including machine learning, natural language processing, computer vision, etc., have emerged as a result of the growth of artificial intelligence. (Suo *et al.* (2013); Gan *et al.* (2013); Narudin *et al.* (2016); Zhang *et al.* (2014); Yang *et al.* (2015); Deng *et al.* (2015); Chamola *et al.* (2021)). Among the supreme well-known branches of AI, deep learning, has made significant strides in addressing problems relating to risks to information security. (Serey *et al.*, 2021; Zhang & Kantarci, 2019).

Therefore, the aim of the present study is to carry out a bibliometric and systematic review of publications in "application of AI in cyber threat intelligence.

Research Objectives

Achieving the aim of this research, the following are to be met:

- i. publication trend in application of artificial intelligence in cyber threat
- ii. systematic review of application of AI technique to CIC-DDoS 2019 Dataset comparative analysis of AI techniques used cyber threat intelligence

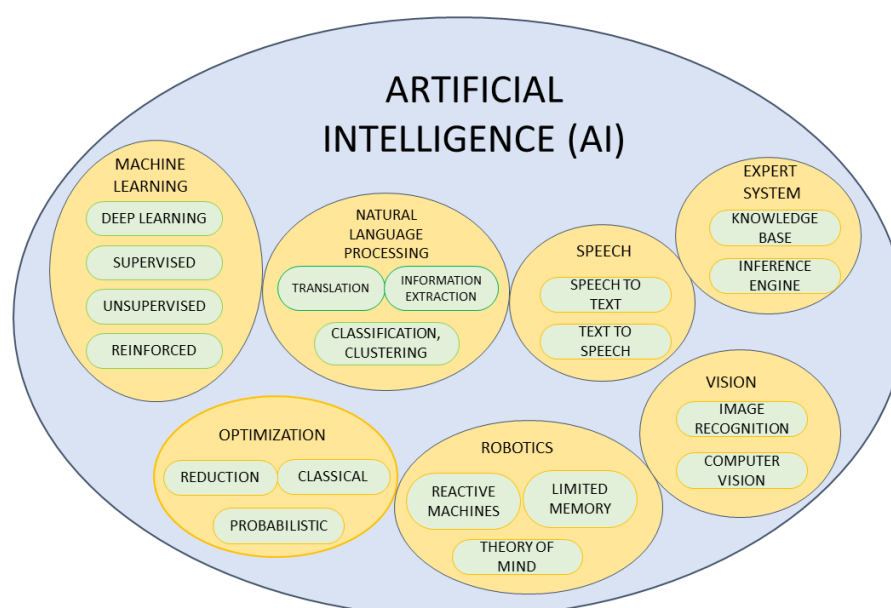


Figure 1. The classification of artificial intelligence (AI) techniques (Gupta *et al.*, 2022).

Methodology

Systematic Literature Search

A methodology used in this review paper entails a comprehensive literature search that aims for a comprehensive study authentication report, rendering readers how the studies were identified along with where the review's results fit into the pertinent body of evidence. In order to extract primarily peer-reviewed literature and a couple of conference papers published from the start date of 2007 to 2023, a systematic search of the literature was performed in several databases, which involves Scopus (<https://www.scopus.com/inward/record.uri?eid=2-s2.0-85136280391&doi=10.11591%2fijai.v11.i4.pp1607-1614&partnerID=40&md5=d786d06aaga541593d224772e8d877b>, 2023), Researchgate, Google, and Academia. Because there were so few publications in other languages, the search was limited to studies in the English language, which had little bearing on the decision-making process. Key words were developed to identify research studies, initial key words were centered on the different cyber threat intelligence in the banking sector. The research titles, abstracts, bibliographies, and subject headings were also searched, essentially to ensure relevant and vital literatures were collated. Additionally, references of selected publications helped in identifying other research studies that offered valuable data and information on AI techniques used in cyber threat detection in past works. However, some database did not yield vital result due to lack of access to publications and lack of adequate information. The steps involved in systematic review process is presented in Figure 2.

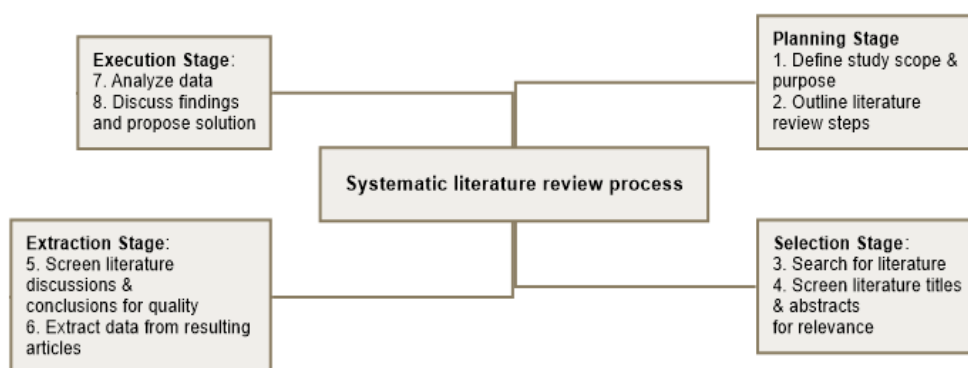


Figure 2. Systematic literature review process (Okoli & Schabram, 2010)

Data Analysis

For the purpose of data analysis, this review relied on a comparative analysis method. (Schneider & Wagemann, 2010). The various AI approaches were contrasted in order to determine the most precise program for use in cyber threat and spotting. The complicated nature of the algorithm, the predictive power, the length of time required to solve the problem, and the time since the method first emerged all factor into the adoption of AI.

Additionally, the advantages and disadvantages of various AI methods were contrasted. Utilizing VOSviewer software and Excel 2019, the dataset (160KB) with 387 publications that were acquired from Scopus and pieces of literature from Google Scholar, Research Gate, and academia across 2007 and 2023 were investigated. VOSviewer is the administration for fashioning and visualizing bibliometric networks (Van Eck et al., 2010). Such relationships can be built according to citation, bibliographic coupling, co-citation, or co-authorship connections and involve journal articles, researchers, and other data. Additionally, it provides text mining capabilities that can be used to create and display co-occurrence networks of significant concepts taken from a corpus of scientific literature. It has been used by several researchers (Perianes-Rodriguez *et al.*, 2016; Van Eck & Waltman, 2011; Waltman & Van Eck, 2013).

Results

Results of Inclusion and Exclusion

The database search yielded 387 publications, most of the studies were retrieved from Scopus database. After removing duplicate copies and papers on AACTI publications, 340 papers were selected for this study. 119 document results from TITLE-ABS-KEY (ai AND applications AND on AND cyber AND threat AND intelligence) and

268 document results from TITLE-ABS-KEY (applications AND of AND artificial AND intelligence AND on AND cyber AND threat AND intelligence). Source of dataset from Scopus:

[https://www.scopus.com/results/results.uri?sort=plf-](https://www.scopus.com/results/results.uri?sort=plf-f&src=s&st1=AI+Applications+on+Cyber+threat+Intelligence&sid=ab03ede6ee2f71ae35605c3873cc149d&sot=b&sdt=b&sl=59&s=TITLE-ABS-KEY%28AI+Applications+on+Cyber+threat+Intelligence%29&origin=searchbasic&editSaveSearch=&yearFrom=Before+1960&yearTo=Present)

[f&src=s&st1=AI+Applications+on+Cyber+threat+Intelligence&sid=ab03ede6ee2f71ae35605c3873cc149d&sot=b&sdt=b&sl=59&s=TITLE-ABS-](https://www.scopus.com/results/results.uri?sort=plf-f&src=s&st1=AI+Applications+on+Cyber+threat+Intelligence&sid=ab03ede6ee2f71ae35605c3873cc149d&sot=b&sdt=b&sl=59&s=TITLE-ABS-KEY%28AI+Applications+on+Cyber+threat+Intelligence%29&origin=searchbasic&editSaveSearch=&yearFrom=Before+1960&yearTo=Present)

[KEY%28AI+Applications+on+Cyber+threat+Intelligence%29&origin=searchbasic&editSaveSearch=&yearFrom=Before+1960&yearTo=Present.](https://www.scopus.com/results/results.uri?sort=plf-f&src=s&st1=AI+Applications+on+Cyber+threat+Intelligence&sid=ab03ede6ee2f71ae35605c3873cc149d&sot=b&sdt=b&sl=59&s=TITLE-ABS-KEY%28AI+Applications+on+Cyber+threat+Intelligence%29&origin=searchbasic&editSaveSearch=&yearFrom=Before+1960&yearTo=Present)

51 literatures were chosen for this review, and study methodologies and designs for a comprehensive examination of chosen papers were also used for evaluation. The majority of the publications chosen are journal pieces, conference papers, and chapters for books. From 2007 through 2022, the publication pattern reveals an ascending order. However, in 2023, 2 articles were released. But from 2020 to 2022, there was a sharp rise in publications (Figure 2). Additionally, a power model with an R-squared value of 0.954 has been computed to forecast the cumulative publications of the AACTI. Since the power equation demonstrated a high correlation, it can be used to adhere to the R-squared value in Figure 2.

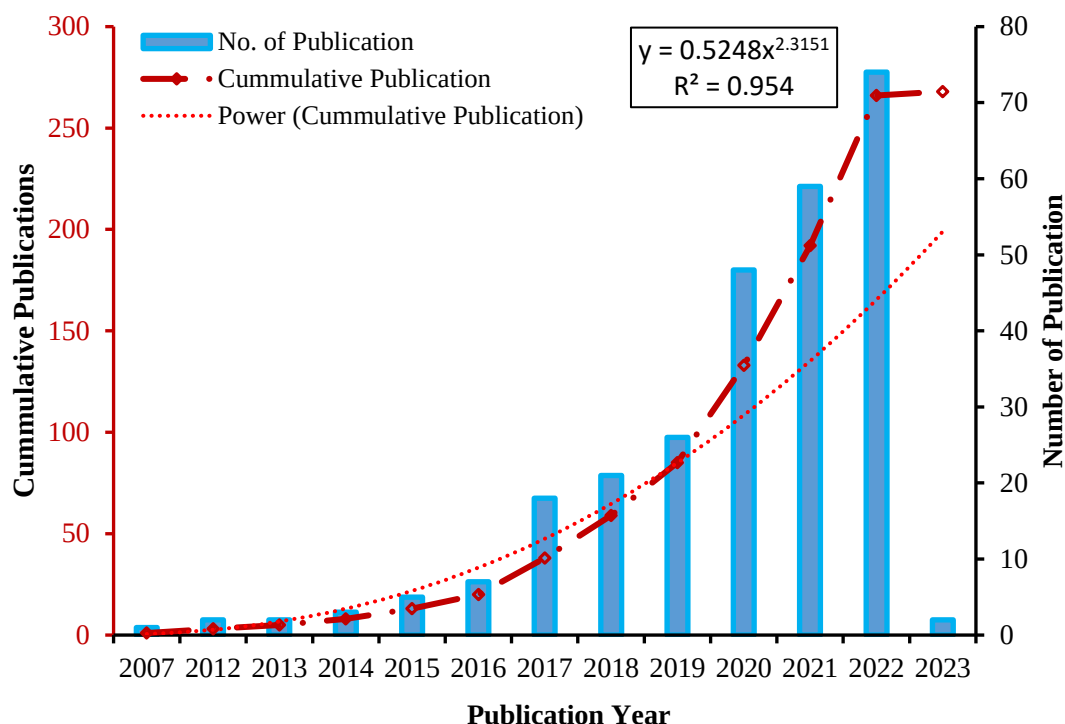


Figure 3. The number of publications in each year of AACTI from 2007 to 2023 in Scopus

The network visualization depiction in Figure 3 shows that cyber security is the second-most-frequently used keyword in AACTI papers after artificial intelligence. This attests to the widespread use of artificial intelligence (AI) in cyber threat analysis. Other pertinent terms in this context include threat detection, cyber-attacks, security, the internet of things, criminality, and malware. IoT, machine learning, and deep learning are artificial intelligence (AI) methodologies used in the area of AACTI, as depicted in Figure 3. The machine-learning method that was most prevalent at the time was the decision tree. Additionally, it showed that "IEEE ACCESS" Journal was the most frequently cited journal for AACTI publication. (Figure 3). Figure 4 gives an unambiguous signal that ICT-related journals like "procedia computer science," "computer security," "internet of things," and "advances in neural information" are the ones that publish the majority of the papers on AI applications in cyber threat intelligence. Additionally, Table 1 shows how many times the cited journals have been referred to. The greatest total link strength and number of citations (4318 and 293, respectively) are found in the IEEE ACCESS journal, which precedes the internet of things journal. 18 countries have been recognized as having publications, alongside the USA being the top-ranking country with 55 publications and 525 citations. (Table 2). The colours in Tables 1 and 2 show the range of values; numbers that fall within an identical range have colouration that are comparable.

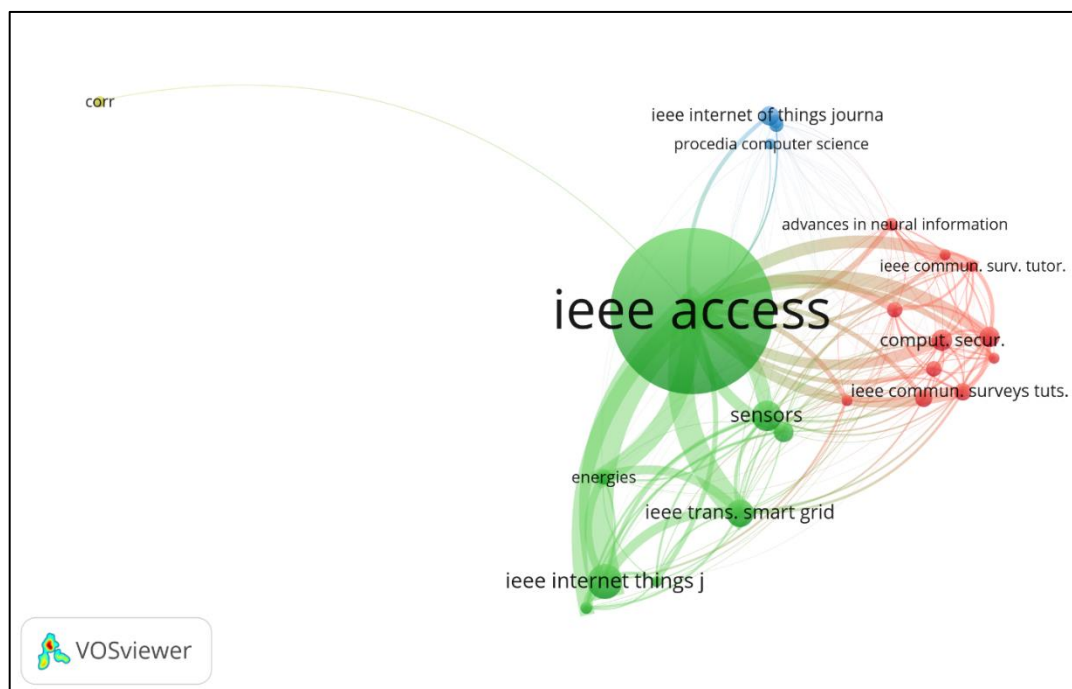
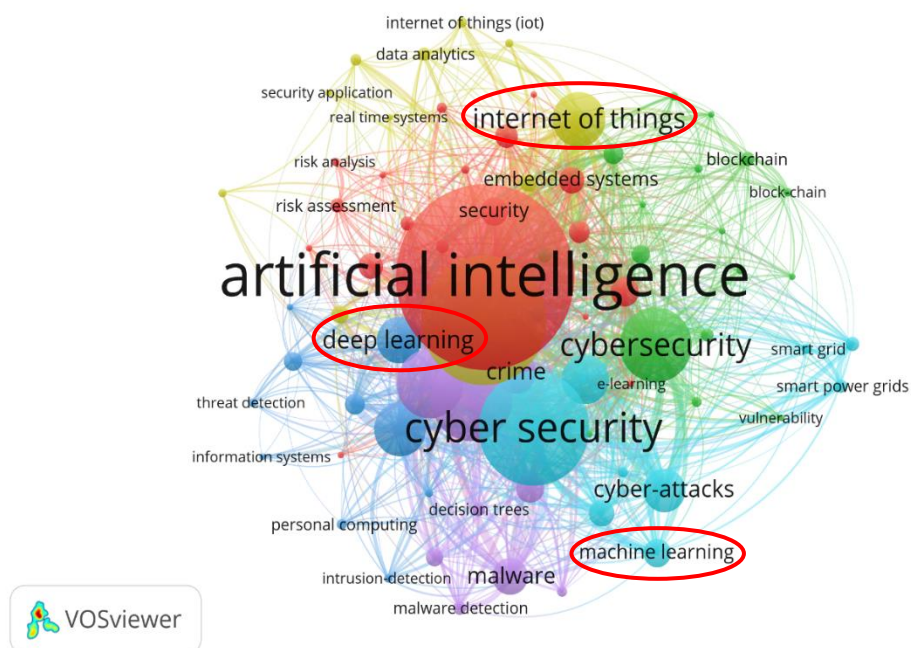


Figure 5. Cited sources (Journal) of AACTI Publications

Table 1. Cited Journals of AACTI Publications

Journals	Citations	Total link strength
ieee access	293	4318
ieee internet things j	62	1406
sensors	55	888
ieee trans. smart grid	49	1339
comput. secur.	38	616
ieee internet things j.	37	829
electronics	36	596
ieee internet of things journal	35	132
ieee commun. surveys tuts.	32	665
j. netw. comput. appl.	31	376
energies	29	843
expert syst. appl.	29	330
neurocomputing	28	540
computers & security	26	73
computer networks	25	74
advances in neural information processing systems	23	356
ieee commun. surv. tutor	22	654
comput. secur	21	340
computer	21	380
corr	21	16
future gener. comput. syst.	21	418
ieee commun. surv. tutor.	20	632
nature	20	264
procedia computer science	20	51

Table 2. Number of Publications and Citations Per Country

Country	Documents	Citations	Total link strength
United states (USA)	55	525	6
India	51	215	6
United Kingdom (UK)	21	256	2
Australia	19	327	7
China	18	64	2
Germany	12	93	0
Russian federation	11	49	0
Saudi Arabia	11	145	7
Greece	9	36	0
Italy	9	28	0
Canada	8	56	0

France	8	69	0
Qatar	6	49	0
Bangladesh	5	122	5
Norway	5	61	1
Pakistan	5	43	0
South Korea	5	42	2
Spain	5	51	0

Review of Related Literatures on Application of AI Technique to CIC-DDoS 2019 Dataset

Liu *et al.* (2022) in this research, two machine learning models—the Logistic Regression model and the linear Support Vector Machine (SVM)—were introduced as a defense against DDoS attacks. Principal Component Analysis (PCA) and Recursive Feature Elimination (RFE), two methods for reducing the number of dimensions, are used in the preparation of the data. The mean cross-validation accuracy is used to evaluate the efficacy of models. Experimental findings demonstrate that the linear SVM model surpasses the Logistic Regression model on the DDoS Evaluation Dataset. (CIC-DDoS 2019). Additionally, PCA-based models had higher and more consistent accuracy metrics than RFE-based models did. Overfitting is prone to happen in computational models of learning with RFE, according to their analysis of losses on the training and testing sets. There were no assessments made between various models using different dimensionality reduction techniques that might enhance the efficacy of DDoS attack prediction.

Amaizu *et al.* (2021) affirms the existence of a reliable DL-based DDoS assault detection system. A feature extraction method like PCC and two DNN models with different designs are combined to create the proposed framework. It is intended to recognize DDoS assaults and the different kinds that have taken place. The authors investigated the proposed framework using quaternary distinct situations over an industry-recognized dataset. (i.e. CICDDoS2019 dataset). The results showed that the framework could identify DDoS attacks with an accuracy of 99.66% and a loss of 0.011. The outcomes of the specified discovery scheme were also contrasted with those of modern approaches like KNN, SVM, Deep-Defense, and CNN ensemble. The recommended method outperformed them all, with the exception of the CNN ensemble. In relation to recall and accuracy, the CNN ensemble performs better than the recommended scheme. The proposed model's performance in a real-time scenario would be hampered by its intricate foundation, which will increase tracking period.

Spyridopoulos *et al.* (2013) DDoS attacks should be characterized as one-shot, non-cooperative, zero-sum games, the authors of the study suggest. The research examines different pairings of the cost of an attack, the number of attacking nodes, and the characteristics of malicious traffic probability distributions. The impacts on firewall performance and design are the authors' main emphasis. The findings show that if it is believed that the attacker thinks about the cost of an attack, the defensive network may

select firewall arrangements that mitigate the expense of the losses despite the attacker's chosen motions.

Hwang *et al.* (2020) outlined D-PACK, a method for detecting abnormal traffic that combines a Convolutional Neural Network (CNN) and an unsupervised deep learning model (like an auto encoder) to automatically profile traffic trends and filter out abnormal traffic. D-PACK only examines the primary few bytes of the first few packets in each flow to facilitate early discovery. The outcomes show that D-PACK still works with over 100% accuracy using just the first distich packets of each stream and has an extremely low false-positive rate of 0.83 %. The method might be used as a blueprint for creating online anomalous warning systems that decrease the number of processed packets while simultaneously actively thwarting harmful flows.

Li and Lu (2019) A DDoS attack detection method based on LSTM model and deep belief network feature extraction is provided by the work. This technique first extracts IP packet characteristics by means of a deep belief network then builds an LSTM traffic prediction model, and finally employs the LSTM model to identify DDoS attacks. The DDoS attack detection device can use this method. The model can accurately predict typical network traffic trends, spot DDoS attack-related deviations, and address upcoming DDoS attack detection techniques.

Desai *et al.* (2020) this paper uses the TCP protocol and a heterogeneous machine learning arrangement to identify DDoS attacks in SDN environments. Accuracy, recognition pace, and false alarm rate were used as performance metrics to assess the suggested method. KNN is an unsupervised machine learning strategy that outperforms the SVM approach used in the TCP protocol at identifying assaults. They succeeded to increase accuracy, detection rate, and false alarm rate using the suggested composite machine learning model in reference to a simple machine learning model. (SVM- KNN). It is possible to build ensemble machine learning models to detect DDoS attacks in the data domain by imposing security constraints in the flow table.

Eghtesad *et al.* (2019) recommended employing Deep Reinforcement Learning to find the best MTD (Moving Target Defense) strategies. Based on a known model of adaptive MTD, they developed finding an MTD strategy as a method of determining a policy for a partly observable Markov decision process. The use of compact memory models significantly enhances training effectiveness. They provide thorough numerical statistics to back up their claim that their method significantly outperforms the competition. In this research, they only proposed a DQL-based MTD method for a single defensive agent. The discovered policy, however, could occasionally not be the optimal choice due to the variable nature of the opponent's strategy.

Cil *et al.* (2021) presented the DL model, which incorporates feature extraction and classification techniques in its framework. Three hidden layers with a total of 50 units each, three units in the output layer, and 69 units in the input layer make up the DNN model. Dataset 1 and Dataset 2 are the two portions of the authors' division of the CICDDoS2019

dataset. The two types of traffic in Dataset 1 are typical and attack. Dataset 2's goal is to categorize the various types of DDoS attacks. The DNN model has provided a reliable result for early intervention, suitable for applications in real-time, with a detection accuracy of about 100% for DDoS attacks on Dataset 1. Additionally, it identifies DDoS attacks on Dataset 2 with an accuracy of about 95%. The recommended model has lower accuracy when used for multiclass classification.

Alghazzawi *et al.* (2021) claims that current research works for predicting DDoS attacks have produced a variety of unexpected outcomes when using machine learning (ML) classifiers and conventional methods for feature encoding. In these earlier attempts, deep neural networks were also used to extract features without having to keep track of the sequence data. The current study suggests using a hybrid deep learning (DL) model, especially a CNN with BiLSTM (Bidirectional Long/Short-Term Memory), to effectively predict DDoS attacks using benchmark data. By rating and selecting the features that received the highest scores in the given data set, only the most crucial features were selected. The findings showed that during training with the data set CIC-DDoS2019, the proposed CNN-Bi-LSTM had an accuracy of up to 94.52 %. The Chi-squared measure being a single statistical tool used to find key features is one of the constraints of this research.

Feng *et al.* (2020) in this investigation paper, a novel Reinforcement-Learning-based L7 DDoS assault defense method is proposed. To assist a reinforcement learning agent in deciding how to respond to L7 DDoS attacks, they show a multi-objective reward function. As a result, the agent may use a variety of strategies to protect the victim in various situations while continuously monitoring and analyzing the victim server. When an L7 DDoS attack is severe, the agent will actively block as numerous malicious requests as it can, protecting the functionality of the victim server (even if it means blocking a small number of genuine inquiries in the process). In all other cases, the agent will passively block malicious requests, concentrating on reducing collateral harm caused by authorized requests. In relation to the assessments, the method can avoid most collateral damage and stop 98.73% of malicious messages from applications after an assault.

Comparative Analysis of AI Techniques Used

The accuracy of the AI methods made use of and the outcomes obtained serves as the primary evaluation parameter in this analysis. Pattern analysis, filtering, and decision-tree analytics are examples of comparative analysis techniques that are used to compare texts. Therefore, the algorithm's flexibility is one of the various comparative factors. The summary of AI techniques and their performances are indicated in Table 3.

Table 3. Summary of AI techniques and their level of accuracy in prediction of cyber threat detection

AI Technique	Algorithm (classification models)	Cyber Threat Detection	Level of accuracy (%)
Expert System	Adaptive Expert System (AES)	Detecting sophisticated cyber attacks	76.5 – 99.1
Machine learning techniques	ANN, KNN	Phishing Emails	92.2
Fuzzy Logic	Fuzzy C-means	Detecting Phishing Websites	96.1
Machine learning techniques	K-Means, KNN, Fuzzy C-Means, SVM, NB, RBF, Ensemble	Phishing Detection	91.28
Machine learning techniques	NB, DT, ANN, KNN,	Network Intrusion	99.07
Machine learning techniques	MLP, J48, RF, DT, ANN	Network Intrusion	93.7
Machine learning techniques	NB, SVM, Ensemble	Spam and Phishing Email filtering	99
Machine learning technique	DT, RF, Gradient Boosting	Detect phishing websites	98.4
Machine learning techniques	LR	Phishing Detection	98.4
Genetic algorithm	FWP-SVM-genetic algorithm	Network intrusion	100

NB is Naïve Bayes; RF random forest; DT; decision tree; LR logistic regression; SVM support vector machine; ANN artificial neural network; MLP multi linear programming.

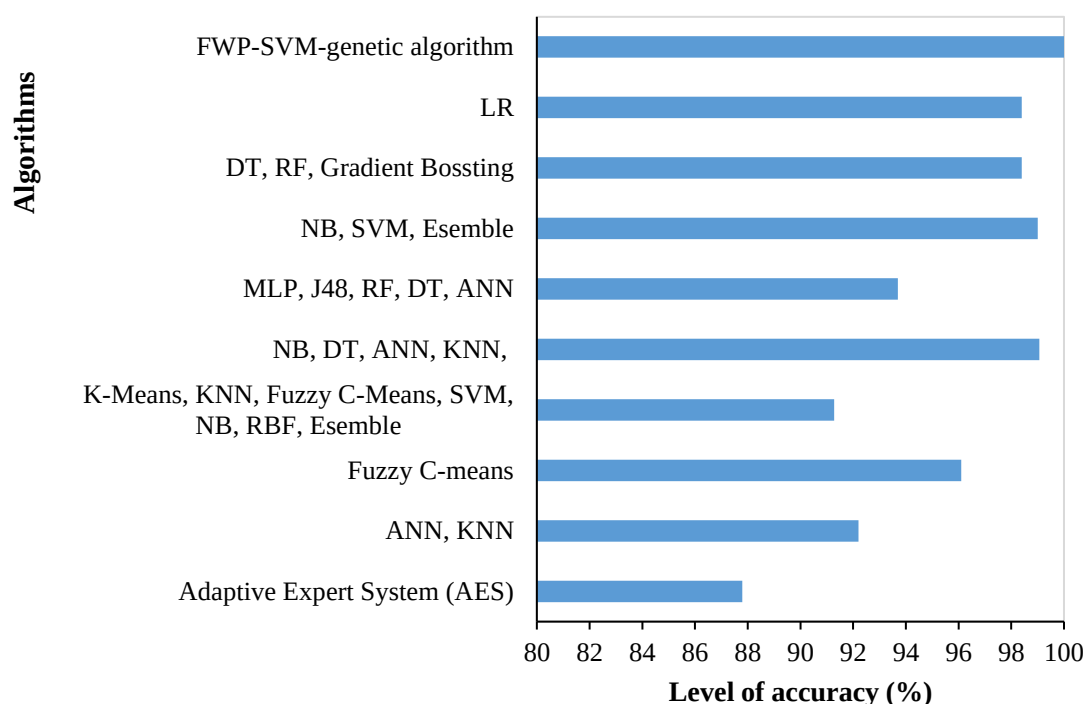


Figure 5. The different AI algorithms used in cyber threat detection classification

As illustrated by Figure 5, it was discovered that Genetic Algorithm (GA) has the greatest degree of accuracy in classifying cyber threats, followed by machine learning procedures like NB, DT, ANN, and KNN. As can be seen, genetic algorithms are the second most popular AI method after machine learning. On the assumption of juxtaposition, no literature containing implementations for deep reinforcement learning was discovered. However, there is scarcity of literature on deep reinforcement learning (DRL) applications in DDoS attacks.

Discussion of Systematic Review

Even though the use of AI techniques was successful back then, the advancement of technology makes it challenging to apply such methods today. AI has prompted the development of signature-based methods that can assist a company in identifying 95% of threats. (Conti *et al.*, 2018). This is how businesses use AI to support threat hunting by integrating behavioral analysis to find attacks. Artificial intelligence is required for finding vulnerabilities in systems belonging to an organization. It can devour tons and tons and tons of data that demonstrates how the business can advance in preventing cyber threats. When cyber dangers threaten the security of businesses and individuals, AI in cyber threat intelligence is viewed as a technological advancement. An organization's initial move is to comprehend what threat intelligence entails. Threat intelligence is evidence-based information on the patterns in cyber threats, including implications, indicators,

mechanisms, and context-specific guidance. Threat intelligence gives researchers access to all the data they need to stay one step beyond criminals and threats along with responding to them in the most effective way possible. Cyber dangers can be managed with the aid of artificial intelligence. For instance, the business can shorten the amount of time it takes to recoup from a security breach, helping them to avoid incurring financial losses. When there are cyberattacks, AI makes sure there is a quicker reaction. Artificial intelligence is capable of effectively processing unstructured data in a cyber danger. In this regard, it picks up on the behavior quickly and monitors it in order to guarantee ample response time, which helps in preventing all types of cyber threats. Additionally, leverage can be used by artificial intelligence to deal with threat intelligence feeds in order to discover threat tendencies. Event logs and data about weaknesses are identified in this, enabling the company to take preventative action and compile security observations methodically.

Although, the emergence of AI in cyber threat intelligence (AACTI) can be beneficial but challenging too (Taddeo, 2019; Taddeo & Floridi, 2018a; Taddeo & Floridi, 2018b). Consequently, the biggest challenges in applying AI to cyber threat intelligence are (i) designing an AI system that doesn't interfere with cybersecurity operations, (ii) ensuring that the given AI system has scalable oversight, and (iii) resolving the issue where, as supplementary research into new technologies advances, AI started emergent more sophisticated and self-developing, eventually replacing humans (Rashmi, 2018). Essentially computational intelligence techniques have been widely used in the fields of computer security and forensics, some moral and legal dilemmas emerge as technology develops, including those involving secrecy and power (Siddiqui *et al.*, 2018). But there is a lot of room for AI to be used in defense in the future. Numerous studies and experiments are being conducted to identify the negative impacts of AI use. Before artificial intelligence methods can be used in the real world, numerous efforts are being made to find remedies for these negative effects. (Siddiqui *et al.*, 2018). Several used cases are being tested for ensuring the proper application of AI in cybersecurity with attacks on networks leading all kinds of attacks.

Because the terrain of cyber security is quickly shifting from identification, discretionary response, and remediation to computerized mitigation, AI presents possibilities for cyber security. AI is able to recognize complicated and novel changes to attack extensibility. Traditional technology concentrates on known intruders and intrusions, which can lead to blind spots when trying to detect novel intrusions that exhibit unusual behaviors. Smart technology was used to address the shortcomings of prior security technology. For instance, the restricted intranet's actions can be observed, and any overt changes to the way privileged access is used could pose a risk. Security specialists now have the advantage they need to stop threats beforehand they create any problems thanks to anticipatory artificial intelligence.

Conclusion

This review article shows how AI is revolutionizing every facet of cyber threat intelligence. AI techniques have demonstrated their exciting possibilities in the advancement of the field of cyber threat intelligence through their practical application in terms of data analytics for evaluating and identifying any cyber danger in a computer system. Furthermore, it has been found that using AI methods instead of traditional detection techniques reduces the usual time needed to identify threats and anomalies. Furthermore, AI techniques that assist in strengthening the input, delivering an unstructured protocol for cyber threat intelligence, and other things help to enhance the accuracy and unpredictability of the detection process. However, the degree of accuracy in cyber threat detection varies depending on the various AI techniques and algorithms employed. The systematic review shows that, when compared to other machine learning algorithms like ANN, KNN, DT, NB, etc., the FWP-SVM-Genetic Algorithm has the best measure of accuracy in detecting network intrusion. Real-time intelligence systems based on IoT can be created to warn and make the user aware of the potential threats and cyberattacks a network is susceptible to in addition to aiding in discovering them.

Furthermore, it has been proven through experience in DDoS protection that security against significant threats can be achieved with very little resource investment. Reviews of publications show that research on artificial neural networks provides the results of AI that are most directly applicable to cybersecurity. Cybersecurity implementations of neural networks persist. Complex cyber-security strategies are still desperately required in many fields where neural networks weren't the best technology. These areas include knowledge control, situation understanding, and decision support. The most interesting in this scenario is expert machine development.

Recommendations

- i. AI needs continuous human collaboration and training. Alongside, researchers should focus on current AI techniques such as deep reinforcement learning for complex cyber threat intelligence applications. In addition, developing software systems with standard logic for effective defense against the growing cyber-attacks.
- ii. It would also be appropriate to conduct research that contributes to cyber threat intelligence (CTI) methodology in order to broaden CTI's base.

References

- Aldhaheeri, S., Alghazzawi, D., Cheng, L., Alzahrani, B., & Al-Barakati, A. (2020). DeepDCA: novel network-based detection of IoT attacks using artificial immune system. *10*(6), 1909.
- Alghazzawi, D., Bamasaq, O., Ullah, H., & Asghar, M. Z. (2021). Efficient detection of DDoS attacks using a hybrid deep learning model with improved feature selection. *11*(24), 11634.
- Amaizu, G. C., Nwakanma, C. I., Bhardwaj, S., Lee, J., & Kim, D.-S. (2021). Composite and efficient DDoS attack detection framework for 5G networks. *188*, 107871.
- Bajpai, A., & Arushi, A. (2018). Big data analytics in cyber security. *6*(7), 1.

- Brown, S., Gommers, J., & Serrano, O. (2015). From cyber security information sharing to threat management. Proceedings of the 2nd ACM workshop on information sharing and collaborative security,
- Chamola, V., Jolfaei, A., Chanana, V., Parashari, P., & Hassija, V. (2021). Information security in the post quantum era for 5G and beyond networks: Threats to existing cryptography, and post-quantum cryptography. 176, 99-118.
- Christen, M. et al. (2020) When algorithms decide for us: Opportunities and risks of artificial intelligence (transl. from german) URL: https://www.researchgate.net/publication/340720749-Wenn_Algorithmen_fur_uns_entscheiden_Chancen_und_Risiken_der_kunstlichen_Intelligenz (accessed: 24 Nov 2021), 55.
- Cil, A. E., Yildiz, K., & Buldu, A. (2021). Detection of DDoS attacks with feed forward based deep neural network model. 169, 114520.
- Conti, M., Dargahi, T., & Dehghantanha, A. (2018). *Cyber threat intelligence: challenges and opportunities*. Springer.
- Costello, K. (2019). Gartner survey shows 37 percent of organizations have implemented AI in some form. 23(05), 2022.
- Deng, S., Yue, D., Fu, X., & Zhou, A. (2015). Security risk assessment of cyber physical power system based on rough set and gene expression programming. 2(4), 431-439.
- Desai, V., Pradhani, A., & Majukar, S. (2020). Detection of DDoS Attack in TCP protocol using Hybrid Machine Learning Techniques.
- Eghtesad, T., Vorobeychik, Y., & Laszka, A. (2019). Deep reinforcement learning based adaptive moving target defense.
- Feng, Y., Li, J., & Nguyen, T. (2020). Application-layer DDoS defense with reinforcement learning. 2020 IEEE/ACM 28th International Symposium on Quality of Service (IWQoS),
- Gan, X.-s., Duanmu, J.-s., Wang, J.-f., & Cong, W. (2013). Anomaly intrusion detection based on PLS feature extraction and core vector machine. 40, 1-6.
- Gupta, C., Johri, I., Srinivasan, K., Hu, Y.-C., Qaisar, S. M., & Huang, K.-Y. (2022). A systematic review on machine learning and deep learning models for electronic information security in mobile networks. 22(5), 2017.
- Haenlein, M., & Kaplan, A. (2019). A brief history of artificial intelligence: On the past, present, and future of artificial intelligence. 67(4), 5-14.
- Hodo, E., Bellekens, X., Hamilton, A., Dubouilh, P.-L., Iorkyase, E., Tachtatzis, C., & Atkinson, R. (2016). Threat analysis of IoT networks using artificial neural network intrusion detection system. 2016 International Symposium on Networks, Computers and Communications (ISNCC),
- Hosseini, R., Qanadli, S. D., Barman, S., Mazinani, M., Ellis, T., & Dehmeshki, J. (2011). An automatic approach for learning and tuning Gaussian interval type-2 fuzzy membership functions applied to lung CAD classification system. 20(2), 224-234.
- Hwang, R.-H., Peng, M.-C., Huang, C.-W., Lin, P.-C., & Nguyen, V.-L. (2020). An unsupervised deep learning model for early network traffic anomaly detection. 8, 30387-30399.
- Jing, X., Yan, Z., & Pedrycz, W. (2018). Security data collection and data analytics in the Internet: A survey. 27(1), 586-618.
- Kessler C. Gary. (2000). *Defenses Against Distributed Denial of Service Attacks* <https://www.garykessler.net/library/ddos.html>
- Kong, L.-j. (2013). An improved information-security risk assessment algorithm for a hybrid model. 5(2).
- Krishnan Sadhasivan, D., & Balasubramanian, K. (2017). A fusion of multiagent functionalities for effective intrusion detection system. 2017.
- Li, J.-h. (2018). Cyber security meets artificial intelligence: a survey. 19(12), 1462-1474.

- Li, Y., & Lu, Y. (2019). LSTM-BA: DDoS detection approach combining LSTM and Bayes. 2019 Seventh International Conference on Advanced Cloud and Big Data (CBD),
- Liu, Z., Qian, L., & Tang, S. (2022). The prediction of DDoS attack by machine learning. Third International Conference on Electronics and Communication; Network and Computer Technology (ECNCT 2021).
- Mirsky, Y., Demontis, A., Kotak, J., Shankar, R., Gelei, D., Yang, L., Zhang, X., Pintor, M., Lee, W., & Elovici, Y. (2022). The threat of offensive ai to organizations. 103006.
- Misra, S., Tan, M., Rezazad, M., Brust, M. R., & Cheung, N.-M. (2017). Early detection of Crossfire attacks using deep learning. <https://doi.org/>
- Müller-Quade, J., Backes, M., Buxmann, P., Eckert, C., & Holz, T. (2019). *Cybersecurity research: Challenges and course of action*.
- Narudin, F. A., Feizollah, A., Anuar, N. B., & Gani, A. (2016). Evaluation of machine learning classifiers for mobile malware detection. 20, 343-357.
- Okoli, C., & Schabram, K. (2010). A guide to conducting a systematic literature review of information systems research.
- Pamukov, M. E. (2017). Application of artificial immune systems for the creation of IoT intrusion detection systems. 2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS),
- Perianes-Rodriguez, A., Waltman, L., & Van Eck, N. J. (2016). Constructing bibliometric networks: A comparison between full and fractional counting. 10(4), 1178-1195.
- Pohlmann, N. (2019). Artificial Intelligence and Cyber Security - immature but necessary (transl. from german). In: T-Sicherheit – Fachmagazin für Informationssicherheit und Compliance. Publisher: DATAKONTEXT-Fachverlag. URL: <https://norbert-pohlmann.com/wpcontent/uploads-/2019/04/393-K%C3%BCnstliche-Intelligenz-und-Cybersicherheit-Unausgegorenaber-notwendig-Prof.-Norbert-Pohlmann.pdf> (accessed: 26 Nov 2021), 523 – 524.
- Radware. (2016). *DDoS Survival Handbook*. Radware, Inc.
- Rashmi, B. (2018). Impact of artificial intelligence on cyber security. 6(12), 67-79.
- Razaq, A., Tianfield, H., & Barrie, P. (2016). A big data analytics based approach to anomaly detection. Proceedings of the 3rd IEEE/ACM international conference on big data computing, applications and technologies,
- Roy, S. S., Mallik, A., Gulati, R., Obaidat, M. S., & Krishna, P. V. (2017). A deep learning based artificial neural network approach for intrusion detection. Mathematics and Computing: Third International Conference, ICMC 2017, Haldia, India, January 17-21, 2017, Proceedings 3,
- Russel, S., & Norvig, P. (2003). Artificial Intelligence–A Modern Approach. Person Education. 736-741.
- Russell, S., & Norvig, P. (2021). Artificial intelligence: a modern approach, global edition 4th. 19, 23.
- Russell, S. J. (2010). *Artificial intelligence a modern approach*. Pearson Education, Inc.
- Schneider, C. Q., & Wagemann, C. (2010). Qualitative comparative analysis (QCA) and fuzzy-sets: Agenda for a research approach and a data analysis technique. 9(3), 376-396.
- Serey, J., Quezada, L., Alfaro, M., Fuertes, G., Vargas, M., Ternero, R., Sabattin, J., Duran, C., & Gutierrez, S. (2021). Artificial intelligence methodologies for data management. 13(11), 2040.
- Siddiqui, M. Z., Yadav, S., & Husain, M. S. (2018). Application of artificial intelligence in fighting against cyber crimes: a review. 9(2), 118-122.
- Smith, R. G., & Eckroth, J. (2017). Building AI applications: Yesterday, today, and tomorrow. 38(1), 6-22.
- Spyridopoulos, T., Karanikas, G., Tryfonas, T., & Oikonomou, G. (2013). A game theoretic defence framework against DoS/DDoS cyber attacks. 38, 39-50.
- Suo, H., Liu, Z., Wan, J., & Zhou, K. (2013). Security and privacy in mobile cloud computing. 2013 9th International Wireless Communications and Mobile Computing Conference (IWCMC),

- Taddeo, M. (2019). Three ethical challenges of applications of artificial intelligence in cybersecurity. 29, 187-191.
- Taddeo, M., & Floridi, L. (2018a). How AI can be a force for good. 361(6404), 751-752.
- [Record #46 is using a reference type undefined in this output style.]
- Tegmark, M. (2017). Being human in the age of artificial intelligence.
- Van Eck, N. J., & Waltman, L. (2011). Text mining and visualization using VOSviewer.
- Van Eck, N. J., Waltman, L., Dekker, R., & Van Den Berg, J. (2010). A comparison of two techniques for bibliometric mapping: Multidimensional scaling and VOS. 61(12), 2405-2416.
- Waltman, L., & Van Eck, N. J. (2013). A smart local moving algorithm for large-scale modularity-based community detection. 86, 1-14.
- Wang, J., Wen, R., Li, J., Yan, F., Zhao, B., & Yu, F. (2018). Detecting and mitigating target link-flooding attacks using SDN. 16(6), 944-956.
- Yang, G., Hosseini, H., Sahabandu, D., Clark, A., Hespanha, J., & Poovendran, R. (2018). Modeling and mitigating the core melt attack. 2018 Annual American Control Conference (ACC),
- Yang, K., Zhang, K., Ren, J., & Shen, X. (2015). Security and privacy in mobile crowdsourcing networks: challenges and opportunities. 53(8), 75-81.
- Zhang, B.-y., Yin, J.-p., Wang, S.-L., & Yan, X.-a. (2014). Research on virus detection technique based on ensemble neural network and SVM. 137, 24-33.
- Zhang, Y., & Kantarci, B. (2019). AI-based security design of mobile crowdsensing systems: Review, challenges and case studies. 2019 IEEE International Conference on Service-Oriented System Engineering (SOSE)