A Survey on Artificial Intelligence Techniques in Cybersecurity Management

Mercy Ejura Dapel
Faculty of Arts, Science and Technology
University of Northampton
Northampton, United Kingdom
e-mail: mercy.dapel@northampton.ac.uk

Mary Asante
Faculty of Arts, Science and Technology
University of Warwick
Coventry, United Kingdom
e-mail: mary.asante@warwick.ac.uk

Chijioke Dike Uba
Faculty of Business and Law
University of Northampton
Northampton, United Kingdom
e-mail:Chijioke.Uba@northampton.ac.uk

Michael Opoku Agyeman
Faculty of Arts, Science and Technology
University of Northampton
Northampton, United Kingdom
e-mail:Michael.OpokuAgyeman@northampton.ac.uk

***Abstract*—The rapid development in Internet Services led to a significant increase in cyber-attacks. The need to secure systems and operations has become apparent as cybersecurity has become a global concern. Cybersecurity involves techniques that protect and control systems, networks, hardware, software, and electronic data from unauthorized access. Developing an effective and innovative defensive mechanism is an urgent requirement as conventional cybersecurity solutions are becoming inadequate in safeguarding information against cyber threats. There is a need for cybersecurity methods that are capable of making real-time decisions and respond to cyber-attacks. To support this, researchers are focusing on approaches like Artificial Intelligence (AI) to improve cyber defense. This study provides an overview of existing research on cybersecurity, using AI technologies. AI technologies made a remarkable contribution in combating cybercrimes with significant improvement in anomaly intrusion detection.**

Keywords-Artificial Intelligence; Cybercrime; Cyber-attacks; Cybersecurity; Security Threats.

I. INTRODUCTION

The rapid development in Information and Communication Technology (ICT) created positive implication to the global economy. The internet has improved the quality of life by providing a platform that facilitates knowledge sharing, communication and interaction, which is important for development and daily life [1]. In view of the benefits, the dark side abound. Cyber criminals exploit the vulnerability of individuals and organizations [2]. Providing security for systems have become difficult. Hackers are becoming smarter and more innovative in exploiting individuals and organizations. With cyber-attacks and data breaches coming to light daily, cyber-attacks have been ranked among the top 5 most likely sources of severe global risk [3]. Cyber fraud has become complex to track as cyber theft can originate from any part of the world. Organizations have become challenged with the complexity of cyber-attacks which calls for the adoption of intelligent methods like AI to mitigate them. AI is a thriving field that has been deployed in application areas such as manufacturing [4], healthcare [5], education [6], agriculture [7] and Cybersecurity. According to Abraham et al. [8], AI algorithms can predict previously seen and unseen attacks, it is effective in detecting cyber-attacks with low false alarm rate. Advancement in AI have produced technologies that can learn from past patterns to improve future experiences. Researchers and developed countries have adopted cybersecurity solutions like AI to improve cyber defense [9]. Some existing studies have discussed and summarized cybersecurity issues. To the best of my knowledge, none focused on AI in cybersecurity management systematically. Figure 1 summarized the key trends of events related to cybercrime over 2 decades as identified by Alqurashi [39]. Ransomware attacks have increased drastically over the last decade as illustrated. This article summarized progress in applying AI to tackle cybersecurity. The effectiveness of these solutions in detecting and preventing cyber-attacks is demonstrated. The remainder of this paper is structured as follows: Section II presents the background of study and related work. Section III presents the review methodology used to conduct the study. Section IV presents findings on AI in cybersecurity. Section V discusses future direction of AI in cybersecurity management. Section VI presents the research validation, limitation and concludes the paper.

II. BACKGROUND LITERATURE

A. *Artificial Intelligence for Cybersecurity*

With persistent cyber threats and advanced cyber-attacks emerging, cybersecurity researchers agree that information security is important. Consequently, a number of studies attempted addressing information security by adopting improved techniques such as anomaly intrusion detection and prevention systems, firewall setups and data encryption algorithms. Although some studies have argued that cybersecurity can be effectively tackled by focusing on human behavior. However, others argued that human behavior alone is insufficient.

Copyright (c) IARIA, 2022. ISBN: 978-1-61208-996-6

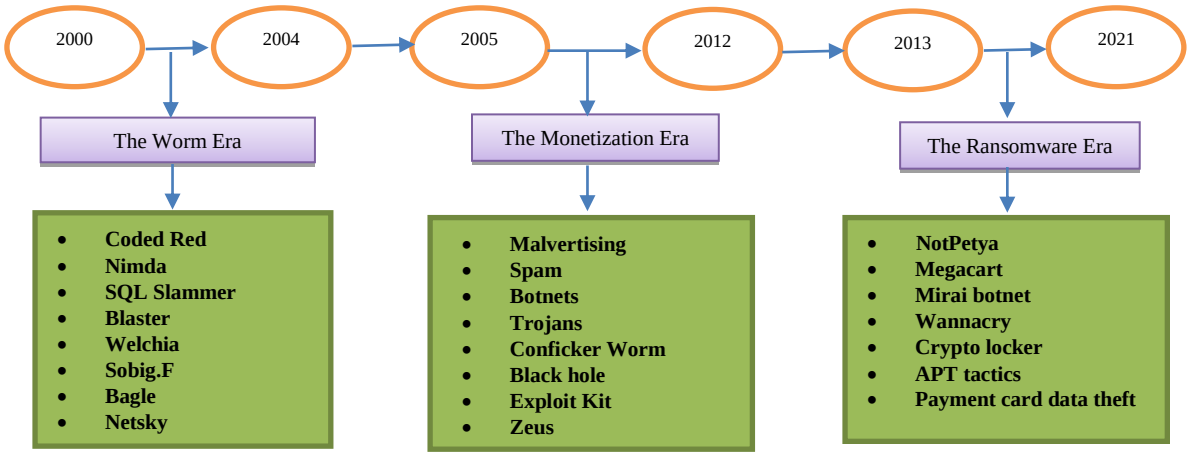

Fig. 1 20-year retrospective on cyber threats.

For instance, the volume of information handled by organizations calls for automation. Hence the need for balance between humans and technology in organizational security activities. Conventional cybersecurity approaches depend on tedious and manual processes, they rely on detect and respond measures that can't keep pace with the volume and velocity of current threats. Furthermore, the first generation of antivirus were designed to identify virus by scanning its bit signature, the assumption of this concept is that virus has the same structure and bit pattern in all instances. These signatures are fixed. Although the catalog of signatures are updated when devices are connected to internet network, the regular release of sophisticated malwares make this approach ineffective. The introduction of signature-less approaches that are capable of detecting and mitigating cyber-threats using newer methods such as AI and behavioral detections have been argued to be effective.

Advancements in AI applications made it possible to design an effective and efficient system that automatically detect and prevent malicious activities in cyberspace. These advancements have been adopted to support existing technologies as they provide mechanisms that better prevent and control cyber-attacks. In view of all the benefits AI provides, emerging cyber threats make it extremely difficult for researchers to identify the most efficient technique and its impact in cyberspace. The general perception among researchers suggest that AI has improved information security. To the best of our knowledge, these claims has not been substantiated. Existing studies have either demonstrated how their innovation outperformed a selection of existing methods or a sample of systems that compare algorithms to access their performance. Accordingly, a literature review is required to provide summary on issues, challenges and future research direction.

TABLE I
GOAL QUESTION METRIC

Purpose	The study analyzes
Issue	Publication trends, application domain, methods, impact, performance and future direction
Object	Existing articles on AI in cybersecurity
Viewpoint	Between 2018 to 2022

B. Related Work

Several existing studies have reviewed literatures on AI in cybersecurity management. For instance, Chan et al. [47] described the intrusion detection ability of AI while identifying false positives and using predictive analysis for storing data. Although their study provides meaningful insights to help people understand AI better, it is not systematic in presenting discussions. Li [48] summarized the intersection of AI and cybersecurity by reviewing the use of AI related algorithms. Their study classified AI applications and contributions as promising for integrated cybersecurity. However, the method used for the survey was not defined, it is open to bias, and therefore their survey cannot claim to be systematic when compared with guidelines proposed by Kitchenham et al. [50].

Waife et al. [51] conducted a systematic mapping review of AI for cybersecurity using quantitative and qualitative methods to analyze several articles. AI made a significant contribution in combating cybercrimes with improvement in false alarm rate for Intrusion Detection Systems (IDS). Al- though the study provides meaningful insights to researchers, the articles selection process was limited to the IEEE and ACM digital libraries. Therefore, their findings cannot be generalized. Sarker et al. [52] surveyed popular AI-driven cybersecurity concepts for protecting inter-connected systems from cyber-threat. The survey revealed that expert systems are used to tackle cybersecurity issues like unauthorized access intelligently, they explained the importance of intelligent cybersecurity management but failed to present an overview of trends in

Copyright (c) IARIA, 2022. ISBN: 978-1-61208-996-6

the domain, Johansson [49] explored a study on coordinated cyber-attacks towards power grid systems by utilizing IDS to provide internal network protection, he utilized qualitative approach and identified countermeasures suitable. However, the study did not follow Kitchenham et al. [50] guidelines, but it provides a foundation.

III. REVIEW METHODOLOGY

PRISMA, a Systematic Literature Review (SLR) protocol, is used in this paper to obtain insight on the application of AI in cybersecurity management as proposed by Kitchenham et al. [50]. PRISMA is a SLR that uses a well-defined methodology to identify, evaluate, and interprete relevant research by using unbiased, trustworthy, rigorous and repeatable methodology. By using PRISMA, the research method can be replicated. A set of keywords were used to identify studies related to AI in cybersecurity management through several database search engines. Keywords used in the search are Artificial Intelligence, Cybersecurity, cyber threats and Information Security. The words were combined to form a search phrase, they are Artificial Intelligence and/or cybersecurity, cyber threats and/or cybersecurity, cyber threats and/or Information security. The viewpoint for the search was limited to studies published from 2018 to 2022. This allowed for consideration of the most recent articles. IEEE xplore digital library, science direct, Google Scholar and other sources were used to select several literatures as mentioned by Kitchenham et al. [50] as they make up the majority of databases used for literature reviews. This was done to avoid bias and ensure that a wide database is covered in the selectionprocess.

250 articles were initially identified. All articles were sub- jected to inclusion and exclusion criteria to identify the state- of-the-art literature before analysis. Conference papers, jour- nals, and short papers etc. were all included. The wide search was to ensure that no relevant article was left out to avoid bias. Titles of articles that did not suggest the application of AI in cybersecurity management were excluded. Articles that are less than 4 pages and are written in languages other than English were also excluded. Abstracts that did not strongly discuss AI in cybersecurity were discarded to reduce bias in the selection process. In total, 67 articles were selected and included in the study.

The process employed is illustrated in Figure 2, it is a diagrammatic representation of the review process. In addition to the rationale of the study, research questions were identified. The search strategy and data extraction are based on inclusion and exclusion criteria. This is grouped into phases as suggested by Kitchenham et al. [50]. Review questions were formulated during the planning stage which forms the foundation for the study. The Goal Question Metric Approach (See Table 2) was adopted by Basili [35]. This approach has also been demonstrated by Yahya et al. [36] to be effective for eliciting the objectives of systematic reviews. This section gave a review of the methodology used to obtain insight into the application of AI in cybersecurity management.

TABLE II
RATIONALE AND REVIEW QUESTIONS

	Research Question	Motivation
RQ1	What publications featured AI in cybersecurity management?	To identify studies and countries where AI con- tributed to cybersecurity management with view- point from 2018 to 2022.
RQ2	What threats was AI addressing in cybersecurity management?	To identify AI solutions applied in cybersecuritymanagement.
RQ3	What impact does AI have in cybersecurity management?	To classify and identify impact/performance of AI in cybersecurity manage ment.
RQ4	What is the future direction for AI research?	To identify future direction of AI in cybersecurity management. This will provide direction for current and future researchers whose area of interest is cybersecurity management.

IV. REVIEW OF FINDINGS ON AI IN CYBERSECURITY

Information regarding the publication year, publication out lets with more than two articles on AI in cybersecurity and al- gorithms used was recorded. This study analyzed, summarized, and discussed the impact of existing methods. Below is the discussion of findings from the study.

A. Publication Trends on AI in Cybersecurity

The results in Figure 3 show that research publications on AI in cybersecurity have increased considerably. AI techniques started gaining rapid attention years before the viewpoint of this review (2018 to 2022), however from the year 2018, the margin of articles increased. The articles reviewed for the year 2018 accounted for 33% of the total selected articles for the primary study. The publications increased from 2019 to 2022. This indicates that studies on AI in cybersecurity management are increasing. The findings in Figure 4 indicate that publications are represented in different publishing outlets. Out of 67 articles on AI, 33 were published in IEEE Access journals and 9 were published at IEEE transactions on Informatics Forensics and Security Journal. These publication outlets listed above accounted for 40% out of the total number. See Figure 4 for the chart on publication distribution according to publication outlets.

Copyright (c) IARIA, 2022. ISBN: 978-1-61208-996-6

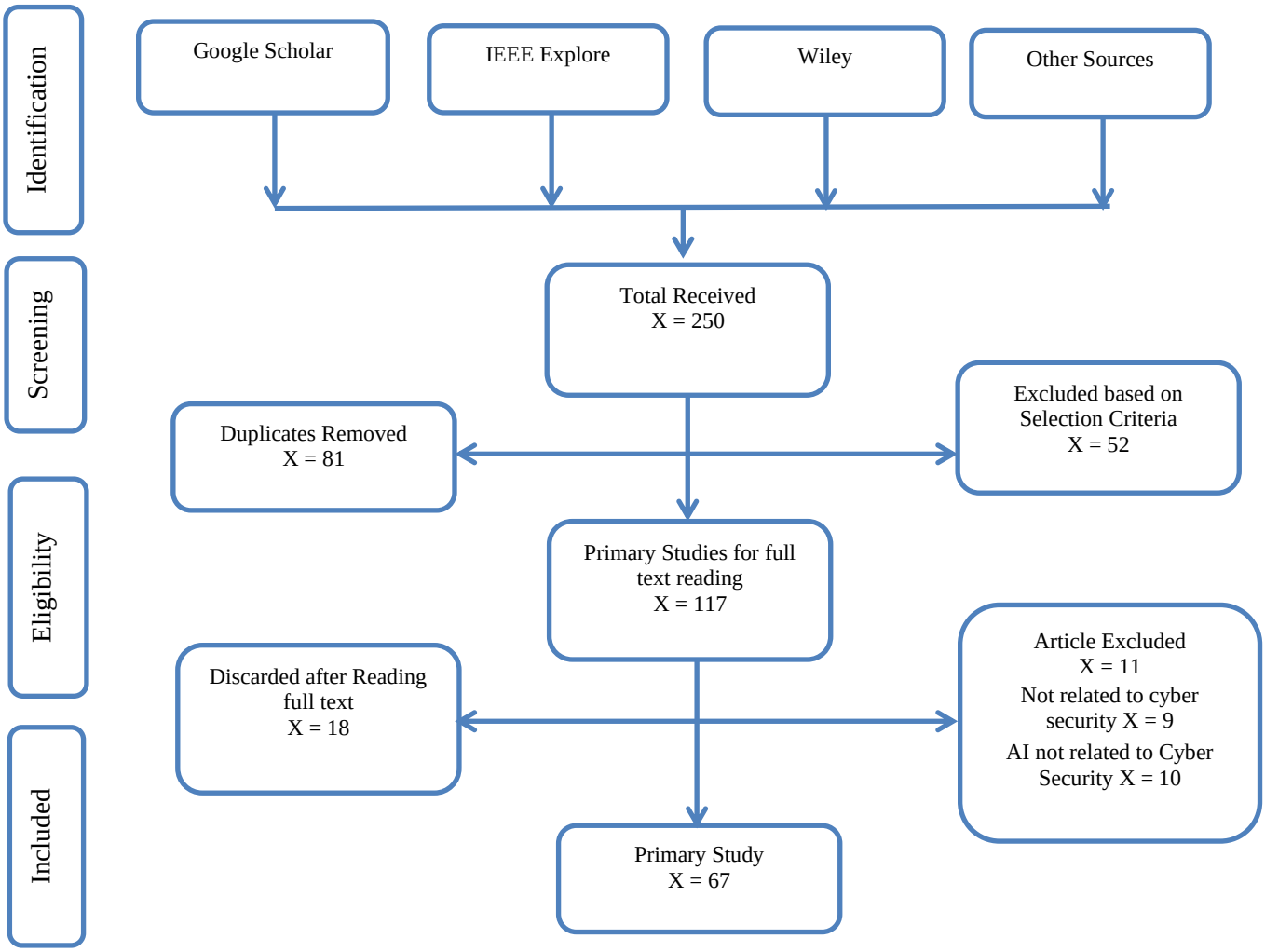

Fig. 2. Diagrammatic representation of PRISMA protocol.

The chart presents outlets with more than two publications. The next publication outlet that recorded most articles is Science Direct which recorded 4 papers, Wiley and IEEE transaction on neural network & learning recorded 3 articles each. The remaining publication outlets recorded two or less studies. Some were published in Transaction Signal Information Process over networks while other publications were recorded in books, conference papers and journals such as Engineering application for artificial Intelligence to mention a few. Similarly, it was observed that the research was skewed geographically. The address of the authors revealed that majority of the studies originated from countries in Asia. It can be deduced from Figure 5 that 58% of the articles originated from Asia. China recorded the highest number of publications, followed by India. Sudan and Norway recorded one publication each.

B. AI in Cybersecurity

AI was proposed in 1956 by John McCarthy as a science concerned with making computers behave intelligently like humans [8]. AI application has evolved significantly, it has a plethora of benefits in education, biometric systems, Internet of Things and cybersecurity among others. AI algorithms contribute to solving security issues. The cost and average time of detection and response to cyber threats is greatly reduced with the intervention of AI [34]. Neural networks have been used to detect classifying data as normal and abnormal [30]. Swarm intelligence methods handles feature selection to identify new intrusions.

Copyright (c) IARIA, 2022. ISBN: 978-1-61208-996-6

Technologies like expert systems and intelligent agents have been used to secure internet networks and improve intrusion detection performance [31].

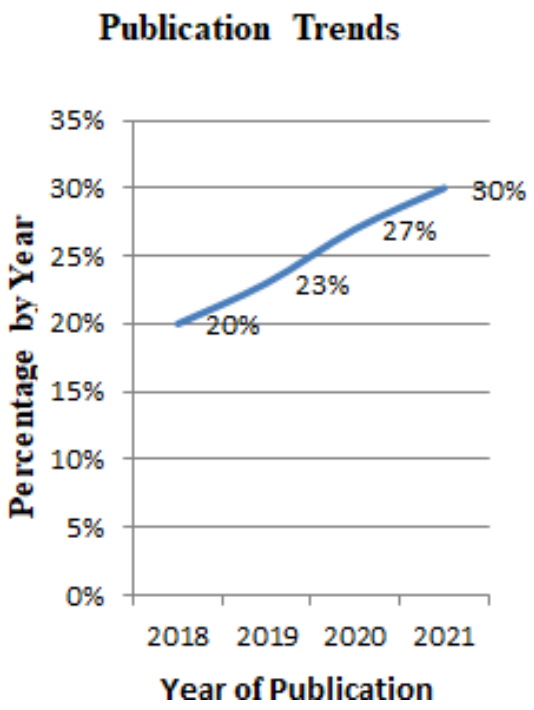

Fig. 3. Trends in primary studies from 2018 to 2021.

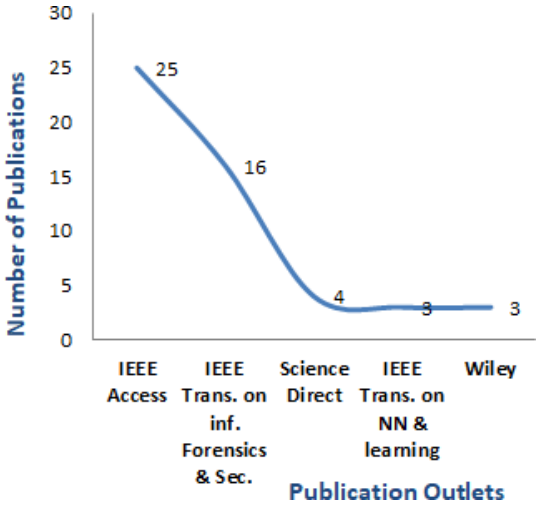

Fig. 4. Publication outlets with more than 2 articles on AI in Cybersecurity

With AI, complexity and model training time is reduced [32]. AI is quickly becoming a tool for automating threat detection and responding effectively than conventional human driven methods which are unable to keep up with volumes of viruses generated daily [30]. AI is relevant in threat detection, intrusion detection, fraud detection and cybersecurity, it has increased the accuracy and speed of cyber response. The major disciplines in AI are fuzzy logic, natural language processing, deep learning, machine learning, computer vision and robotics.

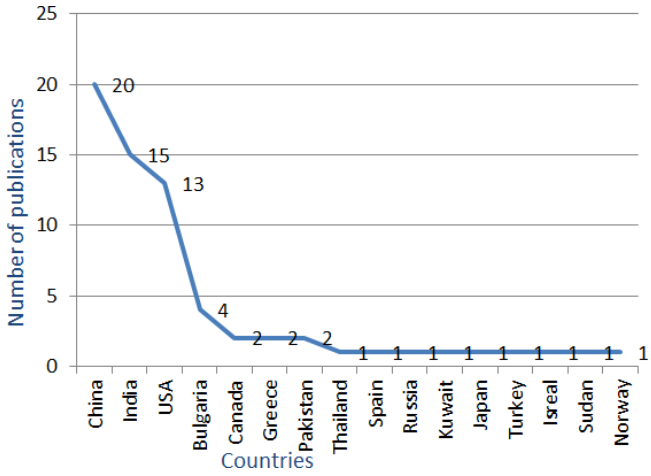

Fig. 5. Distribution of publication by country of origin of the corresponding author

This role of AI in cybersecurity have been displayed in applications that prevent and detect different types of attacks. Several studies that provide knowledge gaps and opportunities in the domain for current and future researchers were identified. The taxonomy informed the clustering in Table 1II.

C. AI as a Tool in Combating Cyber-attacks

With the pace and increase in cyber-attacks, human intervention alone is insufficient for timely and appropriate response. AI technology is becoming very essential to information security. It is capable of analyzing millions of data to detect and prevent cyber threats. It can deduce patterns and identify abnormalities in a computer network expeditiously. AI technologies use behavioral analysis to identify and detect anomalies that are indicative of an attack [32]. This technology gathers large amount of data to identify suspicious behavior that might lead to cyber threat. Processing and analyzing massive amount of data in seconds, using AI algorithms makes prediction of cyber threats possible before they occur, it also predicts future data breaches. With AI breaches can be responded to immediately an attack is detected by responding anonymously without human intervention and also by sending alerts and creating defensive patches [33]. According to a report by Capgemini, the effort and cost of detecting and responding to cyber threats is lowered by 15% in some organizations with AI, as more data is analyzed. This technology learns from

Copyright (c) IARIA, 2022. ISBN: 978-1-61208-996-6

TABLE III
TAXONOMY: AI TECHNIQUES USED IN CYBERSECURITY

Techniques used	Purpose	References
DNN (RNN, ANN, CNN)	Anomaly intrusion detection, Data security, traffic identification- tion, classification and comparison	[50],[44],[10],[40]
DNN	Cyberattack detection, cybersecurity, intrusion detection, Comparison	[54]-[55]
DNN (RNN, CNN)	Spam detection	[56]
DNN (RNN, CNN)	Ransomware/malware detection	[57],[58],[59]-[60]
DNN (RNN, CNN)	Situational Awareness	[61]
CNN	Image detection, intrusion detection, threat detection, Pattern recognition, web security	[62], [63]-[64]
Deep Learning, LSTM	Fraud detection, cybersecurity, intrusion detection, pattern Detection	[9], [65]
ANN, swarm optimization (SO)	Intrusion Detection	[66],[67]
KNN, K prototype cluster-Ing	Anomaly detection, cybersecurity	[38],[42]
Regression Model	Awareness	[45]
Random Forest	Comparison, Anomaly detection, traffic detection, malware Detection	[8], [46]
SVM	Spam detection, anomaly intrusion detection, malware detec-tion, cybersecurity	[47],[56]

past patterns to become proficient in identifying suspicious activities thereby protecting information [34]. AI capabilities and adaptive behavior can overcome the deficiencies of conventional cybersecurity tools

D. AI Algorithms in Cybersecurity

Several algorithms were identified from the primary studies. The dominant algorithms are Random forest (RF), Long Short-Term Memory (LSTM), Decision Tree (DT), Naive Bayesian algorithm, Adaptive Boost (AdaBoost), J48, Support Vector Machines (SVM), K-Nearest Neighborhood (KNN), Convolutional Neural Network (CNN), Artificial Neural Network (ANN), Fuzzy logic, Particle swarm optimization (PSO), Logistic Regression and Recursive Neural Network (RNN).

E. Impact of AI in Cybersecurity Management

AI presents advantages in several areas, cybersecurity being one of them. AI is considered as one of the promising technologies for tackling cyber threats. It is capable of analyzing millions of datasets to identify and prevent cyber-attacks. The most significant contribution of AI is anomaly intrusion detection. To overcome cybersecurity issues, Vinayakumar et al. [10] proposed a highly scalable and hybrid deep neural network, to monitor network traffic and host level events that raise alert for unforeseen

They employed distributed and parallel machine learning algorithms with optimization techniques, making them capable of handling volumes of network and computing resources. Their framework stood out due to scalability and real-time detection of malicious activities from early warning signals. To increase training speed and avert over fitting, batch normalization and dropout approach was used. Deep neural network performed well by detecting and classifying unforeseen and unpredictable cyber- attacks in real-time.

Sokolov et al. [11] analyzed cybersecurity threats in cloud applications using deep learning techniques to monitor data. Suricata engine and module based on Google tensor flow framework was used. They proposed a system that used neural classifiers for network traffic, spam comments, spam email and images. The suricata engine monitored network security and prevented intrusion in real-time.

Fernandez et al. [12] explored a self-adaptive system for anomaly detection that identified cyber-threats in 5G mobile networks. Deep learning techniques was used to analyze network traffic by extracting features from network flows. The authors proposed a high-level cyber defense architecture consisting of virtualized infrastructure (VI), virtualized network function (VNF), management and orchestration (MANO), operations and business support systems. Anomaly symptom detection (ASD) and network anomaly detection (NAD) were proposed to achieve effective network anomaly detection. Once an anomaly is produced from traffic generated, it is communicated to the monitoring and diagnosis module. The experimental result showed that the architecture can self-adapt to anomaly detection based on the volume of network flow gathered from users in real-time.

A botnet is one of the significant threats infecting devices today. Abraham et al. [8] compared the performance of five (5) Machine learning approaches and identified useful features to classify malicious traffic.

Copyright (c) IARIA, 2022. ISBN: 978-1-61208-996-6

Random forest proved to be more robust, it could generalize unseen bots' types.

Intrusion detection technology is a mechanism that monitors and prevents system intrusion. Zhang et al. [13] introduced a multiple-layer representation learning model for accurate detection of network-based attack and proposed a new data encoding scheme based on P-Zigzag to encode network traffic into two-dimensional gray-scale images for representation. Comparing the combination of gcForest and CNN allowed detection of imbalanced data with fewer hyper parameters, which increased computational efficiency. The experimental results showed that the combined algorithms outperformed single deep learning methods in terms of accurate detection and false alarm rate, thereby demonstrating its effectiveness in attack detection. The authors proposed a new intrusion detection method by combining random forest and LSTM to address the above challenges.

In view of the vast amount of data generated daily, and the increased interconnection of the internet infrastructure, Zhong et al. [14] proposed big data based on a hierarchical deep learning system that utilizes behavioral features. Companies can adapt it as a solution for the detection of intrusive attacks. The authors defined the hierarchical structure in five (5) phases. In the first phase, behavioral and content features are extracted using big data techniques. In the second phase, the dataset is separated into clusters, in the third phase, the root clusters of each sub tree is combined until the quality of the merged clusters dropped below the given threshold. In the fourth phase the deep learning model for each cluster was trained, while in the fifth phase, deep learning model was merged to select the most confident model. They concluded that it increased the detection rate of intrusive attacks when compared to a single model learning approach. Their strategy is effective in capturing data patterns for intrusive attacks.

A. Dey [15] utilized a 2018 dataset and proposed the effectiveness of attention mechanism for intrusion detection based on Convolutional Neural Network (CNN) and LSTM model. The authors observed increased performance based on LSTM.

Dawoud et al.'s [16] concept is based on unsupervised deep learning for revealing network threats and detecting anomalies by evaluating the use of restricted Boltzmann machines. This intrusion detection system is used to expose network threat and protect network assets. Their simulation study showed 99% detection accuracy with significant improvement.

Ishaque et al. [17] explored deep learning research by manipulating large amount of data using the functionality of computational intelligence. An important feature which the authors applied for dimensionality and attribute reduction is feature extraction. They concluded that the proposed system can detect attacks that are not hybridized.

Distributed denial of service (DDOS) attack has been a real threat to cyber infrastructure that can bring down ICT infrastructure. Isa et al. [18] adopted deep learning to analyze traffic, focusing on mitigating cyber-attacks with machine learning. Assembly module for statistics collection and adaptive machine learning module for analyzing traffic and enforcing policies are the two main functionalities that was proposed. Auto encoder and random forest algorithm possessed an accuracy of 98.4% with a decreased amount of training and execution time. The result proved that the model is optimally efficient for real-time intrusion detection.

Detecting cyber-attacks requires analyzing cyber-threats to match potential attack profiles. Malicious connections were filtered to improve the accuracy of threat detection and reduce false-positive rates. Lin et al. [19] focused their study on network intrusion detection, using enhanced CNN based on Lenets 5 to classify network threats. The authors developed an improved behavior-based model for anomaly detection by training a CNN to extract enhanced behavior features and identify threats. Their experiment showed overall prediction accuracy with 97.53% intrusion detection rate. The proposed model improves the accuracy of intrusion detection for threat classification.

Zeng et al. [20] proposed a Deep Full Range (DFR) framework comprising a network of encrypted traffic classification and intrusion detection. Three deep learning algorithms (CNN, LSTM and stack auto encoder SAE) were employed for traffic classification and intrusion detection. CNN was used to learn features of the raw traffic; LSTM was used to learn features from time-related aspects and SAE was used to extract features from coding characteristics. The full range consists of three algorithms capable of classifying encrypted and malware traffic within one framework without human intervention. The authors proved that the DFR could attain a robust and accurate performance on both encrypted traffic classification and intrusion detection.

Dey et al. [21] proposed Gated Recurrent Unit (GRU) - LSTM using Google's tensor flow that provided options to visualize network design. Their analysis showed that GRU - LSTM provided high accuracy with low false alarm rate. When compared, GRU-LSTM showed a strong potential in terms of accuracy for anomaly detection.

Hsu et al. [22] proposed a Deep Reinforcement Learning- based (DRL) for anomaly network intrusion detection. Their design revealed incoming network traffic by data sniffing and a pre-processing data module that checks the quality of data before it is fed for intrusion detection. This method can be adopted for self-updating and detecting abnormal incoming network traffic on real-time basis in company websites. SVM and Random Forest

Copyright (c) IARIA, 2022. ISBN: 978-1-61208-996-6

algorithms was utilized. They showed high anomaly detection accuracy and improved processing speed.

Privacy protection and national security in the cyber world depends on safe cyberspace. Network intrusion is one of the sophisticated actors stemming from cyber-threats. Sezari et al. [23] applied a deep feed forward network by modifying the parameters of the anomaly-based network. Their result demonstrated better performance with less complexity and a low false alarm rate. Therefore, their model is trustworthy and can be used to prevent intruders. It can detect unknown attacks based on its network features.

Naseer et al. [24] investigated the suitability of deep learning approaches for anomaly-based intrusion detection. They developed a model based on ANN, Auto encoder and RNN. The models were trained on NSL KDD training dataset and evaluated on the test dataset provided by NSL KDD. A Graphic Processing Unit (GPU) powered test bed using keras with theano backend was employed. A comparison between Deep Neural Network (DNN) and conventional machine learning models was carried out where both Deep Conventional Neural Network (DCNN) and LSTM models showed exceptional accuracy on the test dataset, this demonstrates the fact that Deep learning is a promising technology for intrusion detection.

Anomaly detection has received considerable attention in cybersecurity. The clandestine nature of cyber-attacks increased considerably where malware is installed through a supply chain. Malware eavesdrops and disrupts information exchange.

Huma et al. [27] proposed a detection approach deployed to secure incoming and outgoing traffic, they utilized the application of deep random neural network with multilayer perceptron and evaluated the scheme using two datasets DS205 and UNSW-NB15. They proposed a deep learning based cyber-attack detection system that detects cyber-attack 25 minutes after the attack was initiated to improve cybersecurity at its embryonic stage. It provided performance metrics like accuracy, precision, recall and F1 score which can be compared with several state-of-the-art attack detection algorithms. Classification of 16 different attacks was proposed, and accuracy of 98% and 99% was achieved.

Several industries have adopted the Industrial Internet of Things (IIoT) in smart homes, smart cities, connected cars and supply chain management which introduced new trends in business development. However, these edge devices have become exploitation points for intruders, it raised security and privacy challenge to the trustworthiness of edge devices by compromised devices that transmit false information to cloud servers. An IDS is widely accepted as a technique to monitor malicious activities [26].

The growth of modern cyber infrastructure made cybersecurity more important. It is estimated that a trillion devices will be connected to the Internet by 2022 [28]. IDS is an essential tool with objective to detect unauthorized use and abuse in the host network [29]. Sezari et al. [23] demonstrated the performance of a system while comparing the false alarm rate of models on KDD 1999 Cup dataset, they applied a highly optimized deep feedforward network by the modification of the model parameters. Their model achieved a highly accurate low false alarm and detection rate which can be used to detect and prevent intruders. Utilizing deep learning provided a system behavior model that selects abnormal behavior and is reliable with less complexity.

Khaw et al. [25] monitored network traffic to detect abnormal activities and ensured security of communication and information, using network intrusion simulation datasets (NSL-KDD and UNSW- NB15) on a real campus network. They proposed a Deep Reinforcement Learning-based (DRL) system with self-updating ability to detect abnormal incoming traffic. Dawoud et al. [16] explored the applicability of deep learning to detect anomaly in Internet of Things (IoT) architecture. They proposed an anomaly detection framework by evaluating the use of Restricted Boltzmann machines as generative energy-based model against auto encoders. The study showed approximately 99% detection accuracy. Deep learning algorithms showed positive results and achieved highest detection accuracy with high-performance speed that is effective in detecting false alarm rate (FAR), they can detect previously seen and un- seen threats, however deep neural network could perform better when given more data. Securing a large network in real-time is a challenge that was identified. Several studies focused on intrusion detection to analyze network traffic by extracting features from network flows and traffic fluctuation.

Deep learning algorithm can self-adapt to anomaly intrusion detection and predict network attacks, this was demonstrated in a study conducted by Fernandez et al. [12]. Abraham et al. [8] compared several machine learning algorithms, Random Forest had a superior model, it performed optimally for anomaly detection using cross-validation, and their overall result revealed that previously seen and unseen anomaly-based intrusion can be detected. An improvement in the reduction of false-positive alerts that enabled rapid response to cyber-threat was observed while using ANN [40]. CNN can detect anomalies in industrial control systems by detecting majority of attacks with low false positive rate [41]. A study conducted by Hashim et al. [42] showed that LSTM has high detection accuracy in securing websites from external breaches. Vinayakumar et al. [10] analyzed ransomware attacks and focused on Twitter as a case study, they concluded that deep learning can be used to monitor online posts and provide early warning about ransomware spread.

Copyright (c) IARIA, 2022. ISBN: 978-1-61208-996-6

TABLE IV. PUBLICATION YEAR AND AI SOLUTIONS (2018 TO 2022)

	Intrusion Detection	Spam detection	Malware detection	Image recognition	Traffic classification	Pattern recognition	Other	Total
2018	5	1	2	2	1		1	12
2019	3	1	4				5	13
2020	7	1	5	1	1		1	16
2021	9	2	11			1	3	26
Total	24	5	22	3	2	1	10	67

V. FUTURE DIRECTION OF AI METHODS IN CYBERSECURTY MANAGEMENT

Research directions in AI applications for cybersecurity records broad areas of application. Challenges in cybersecurity continue to emerge which makes it difficult for further research to focus on a specific area. Studies within similar areas are experimenting with different AI algorithms. From table IV, algorithms classified as other were identified to have been used in less than two applications. Researchers are adopting newer techniques. In particular, anomaly intrusion detection needs improvement by reducing model training time in complex systems. Accordingly, future studies may opt for novel techniques. There is a need for applications to be efficient and have performance that reduce computational complexity. However, it was emphasized that for neural networks to present best accuracy with low error, it must be given large dataset. Researchers should advocate a scalable framework that can learn from traffic without manual intervention and can be used in real time to raise alert of possible cyber-attacks.

Future studies may opt for LSTM that have shown improved performance with high accuracy and low computation time.

In recent years, AI applications for cybersecurity have gained interest from researchers. Remarkable contributions have been made in combating cybercrime linking to issues like anomaly intrusion detection and malware detection. Several applications demonstrated improvement with impact in various areas. These areas include prediction of network attacks, presenting best accuracy with the lowest error rate, detecting previously seen and unseen threats and monitoring online post to provide early warning about cyber-threats. The nature of recent research suggests promising result. However, there are some challenges. A significant number of studies did not state the algorithm used or the domain applied. Also, the variety of algorithms identified suggests that researchers are not accepting newer methods, but they are comparing the available algorithms to determine which algorithm is best for an identified situation. Therefore, it is necessary for researchers to investigate further as the latest trends are tending towards IoT. Gradually new modern world activities have moved to the cloud. It is now possible for systems to be connected to the internet and controlled from anywhere in the world. Internet of Things connects these devices to the internet. If companies and organizations can secure their devices with intelligent solutions, consumer confidence will increase.

VI. RESEARCH VALIDATION, LIMITATION AND CONCLUSION

This paper presented a survey of existing research on the application of AI in cybersecurity management. We reviewed the use of AI technologies (Algorithms) in detecting and preventing attacks in cyberspace. The importance and impact of AI in cybersecurity management was discussed. This study covered research centered on viewpoint from 2018 to 2022. Several scholarly databases with related studies were considered. The use of journals, conference papers short papers and more were used to avoid bias in the selection process.

This study confirms that deep learning is not only viable for intrusion detection but is also a promising technology for detecting known and unknown threats. The complexity of cyber-attacks requires techniques that are effective. AI has proven to be effective while maintaining low computation time with a focus on LSTM that have shown low training and computation time.

Over the years, information and communication technology has advanced and cyber-attack surface continued to grow rapidly. Increased frequency of cyber-attacks has reinforced the need for cybersecurity initiatives. Conventional techniques have become inadequate in mitigating complex cyber-attacks, therefore solutions that are capable of tackling cyber threats in real-time is required. AI has shown effectiveness in terms of computational complexity while maintaining low training time

AI is a technology with a range of computational models and algorithms. It deals with the design of intelligent systems that mimic human intelligence. Although AI can be used to fight cybercrime, it could also be exploited hackers. These intelligent security solutions can be considered and integrated into a comprehensive system in countries with low record of publications. AI can be considered as a holistic approach. The advantage of utilizing the above intelligent security solutions is greatly publicized, the integration remains open for further investigations.

REFERENCES

[1] S. Xu, “Cybersecurity Dynamics: A Foundation for the Science of Cybersecurity,” Adv. Inf. Secur., vol. 74, pp. 1-31, 2019, doi: 10.1007/978-3-030-10597-6 1.

[2] K. F. Steinmetz and M. Yar, “Cybercrime and society,” Cybercrime and Society, pp. 1–368, 2019.

[3] P. Ping, W. Qin, Y. Xu, C. Miyajima, and K. Takeda, "Impact of driver behavior on fuel consumption: Classification, evaluation and prediction using machine learning," IEEE Access, vol. 7, pp. 78 515–78 532, 2019.

[4] M. Ghahramani, Y. Qiao, M. Zhou, A. O. Hagan, and J. Sweeney, "AI based modeling and data-driven evaluation for smart manufacturing processes," IEEE/CAA Journal of Automatica Sinica, vol. 7, no. 4, pp. 1026–1037, 2020.

[5] K.-H. Yu, A. L. Beam, and I. S. Kohane, "Artificial in- telligence in healthcare," Nature biomedical engineering, vol. 2, no. 10, pp. 719–731, 2018.

[6] M. Chassignol, A. Khoroshavin, A. Klimova, and A. Bilyatdinova, "Artificial intelligence trends in education: a narrative overview," Procedia Computer Science, vol. 136, pp. 16–24, 2018.

[7] M. J. Smith, "Getting value from artificial intelligence in agriculture," Animal Production Science, vol. 60, no. 1, pp. 46–54, 2018.

[8] B. Abraham et al., "A Comparison of Machine Learning Approaches to Detect Botnet Traffic," Proc. Int. Jt. Conf. Neural N. Intell. Yr Retrosp. Two/New/A Hardware-Trojan Classif. Method Util. Bound. net Struct, vol.-July, doi: 10.1109/IJCNN.2018.8489096.

[9] R. Abdulhammed, M. Faezipour, A. Abuzneid, and A. Abumallouh, "Deep and Machine Learning Approaches for Anomaly-Based Intrusion Detection of Imbalanced Network Traffic," IEEE Sensors Lett., vol. 3, no. 1, pp. 2019–2022, doi: 10.1109/LSENS.2018.2879990.

[10] R. Vinayakumar et al., "Deep Learning Approach for Intelligent Intrusion Detection System," IEEE Access, vol. 7, pp. 41525–41550, doi: 10.1109/ACCESS.2019.2895334.

[11] S. A. Sokolov, T. B. Iliev, and I. S. Stoyanov, "Analysis of cybersecurity threats in cloud applications using deep learning techniques," 42nd Int. Conv. Inf. Commun. Technol. Electron. Microelectron. MIPRO - Proc., pp. 441–446, doi: 10.23919/MIPRO.2019.8756755.

[12] L. Fernandez et al., "A Self-Adaptive Deep Learning-Based System for Anomaly Detection in 5G Networks," IEEE Access, vol. 6, pp. 7700–7712, doi: 10.1109.2018.2803446.

[13] X Zhang, J Chen, Y. Zhou, L. Han and J. Lin, A multiple-layer representation learning model for network- based attack detection. IEEE Access, 7, pp.91992-92008. 2019.

[14] W. Zhong, N. Yu, and C. Ai, "Applying big data based deep learning system to intrusion detection," Big Data Min. Anal., vol. 3, no. 3, pp. 181–195, 2020, doi: 10.26599/BDMA.2020.9020003.

[15] A. Dey, Deep IDS. A deep learning approach for Intrusion detection based on IDS, 2nd Int. Conference Sustain. Technology Ind. 4.0, vol. 0, pp. 19–20, doi 10.1109/STI 50764.2020.9350411.

[16] A. Dawoud, O. A. Sianaki, S. Shahristani, and C. Raun, "Internet of Things Intrusion Detection: A Deep Learning Approach," IEEE Symp. Ser. Comput. Intell. SSCI, pp. 1516–1522, doi: 10.1109/SSCI47803.2020.9308293.

[17] M. Ishaque and L. Hudec, "Feature extraction using Deep Learning for Intrusion Detection System," 2nd Int. Conf. Comput. Appl. Inf. Secur. ICCAIS doi: 10.1109/CAIS.2019.8769473.

[18] M.M. Isa and L. Mhamdi, Native SDN intrusion detection using machine learning. In 2020 IEEE Eighth International Conference on Communications andNetworking (ComNet), pp. 1-7, IEEE. 2020.

[19] W. H. Lin, H. C. Lin, P. Wang, B. H. Wu, and J. Y. Tsai, "Using convolutional neural networks to network intrusion detection for cyber-threats," Proc. 4th IEEE Int. Conf. Appl. Syst. Innov. ICASI, pp. 1107–1110, doi:10.1109/ICASI.2018.8394474.

[20] Y. Zeng, H. Gu, W. Wei, and Y. Guo, "Deep-Full- Range: A Deep Learning Based Network Encrypted Traf fic Classification and Intrusion Detection Framework," IEEE Access, vol. 7, pp. 45182–45190, doi: 10.1109/AC-CESS.2019.2908225.

[21] S. K. Dey and M. M. Rahman, "Flow based anomaly detection in software defined networking: A deep learning approach with feature selection method," 4th Int. Conf. Electr. Eng. Inf. Commun. Technol. iCEEiCT, pp. 630–635, doi: 10.1109/CEEICT.2018.8628069.

[22] Y. -F. Hsu and M. Matsuoka,.A Deep Reinforcement Learning Approach for Anomaly Network Intrusion Detection System," 2020 IEEE 9th International Conference on Cloud Networking (CloudNet), 2020, pp. 1-6, doi: 10.1109/CloudNet51028.2020.9335796.

[23] B. Sezari, D. P. F. Moller, and A. Deutschmann, "Anomaly-Based Network Intrusion Detection Model Using Deep Learning in Airports," Proc. - 17th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. 12th IEEE Int. Conf. Big Data Sci. Eng. Trust pp. 1725–1729, doi: 10.1109/TrustCom/BigDataSE.2018.00261.

[24] S. Naseer et al., "Enhanced network anomaly detection based on deep neural networks," IEEE Access, vol. 6, pp. 48231–48246, doi: 10.1109/ACCESS.2018.2863036.

[25] Y. M. Khaw et al. "A Deep Learning- Based Cyberattack Detection System for Transmission Protective Relays," IEEE Trans. Smart Grid, vol. 12, no. 3, pp. 2554–2565, doi: 10.1109/TSG.2020.3040361.

[26] S. Qureshi et al. "A Hybrid DL-Based Detection Mechanism for Cyber-threats in Secure Networks," IEEE Access, vol. 9, pp. 1–1, doi: 10.1109/access.2021.3081069.

[27] Z. E. Huma et al., "A Hybrid Deep Random Neural Network for Cyberattack Detection in the Industrial Internet of Things," IEEE Access, vol. 9, pp. 55595–55605, doi: 10.1109/ACCESS.2021.3071766.

[28] L. Santos, C. Rabadao, and R. Gonçalves, "Intrusion detection systems in internet of things: A literature review," in 2018 13th Iberian Conference on Information Systems and Technologies (CISTI). IEEE, 2018, pp. 1–7.

[29] M. Wang, K. Zheng, Y. Yang, and X. Wang, "An Explain- able Machine Learning Framework for Intrusion Detection Systems," IEEE Access, vol. 8, pp. 73127–73141, doi: 10.1109.2020.2988359

[30] S. Zeadally, E. Adi, Z. Baig, and I. A. Khan, "Harnessing artificial intelligence capabilities to improve cybersecurity," IEEE Access, vol. 8, pp. 23 817–23 837, 2020.

[31] S. Aljawarneh, M. Aldwairi, and M.B. Yassein, Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model. Journal of Computational Science, 25, pp.152- 160, 2018

[32] P. Mishra, V. Varadharajan, U. Tupakula, and E.S. Pilli, A detailed investigation and analysis of using machine learning techniques for intrusion detection. IEEE Communications Surveys & Tutorials, 21(1), pp. 686-728, 2018.

[33] P. Parrend, J. Navarro, F. Guigou, A. Deruyver, and P. Collet, Foundations and applications of artificial Intelligence for zero-day and multi-step attack detection. EURASIP Journal on Information Security, 2018(1), pp.1-21. 2018

[34] B. Naik, A. Mehta, H. Yagnik, and M. Shah, "The impacts of artificial intelligence techniques in augmentation of cybersecurity: a comprehensive review," Complex & Intelligent Systems, pp. 1-18, 2021.

[35] V. R. Basili, "Goal question metric paradigm," Encyclopedia of software engineering, pp. 528–532, 1994.

[36] F. Yahya, R. J. Walters, and G. B. Wills, "Using goal- question-metric (gqm) approach to assess security in cloud storage," in International Workshop on Enterprise Security. Springer, 2015, pp. 223–240.

[37] Z. Liu, T. Qin, X. Guan, H. Jiang, and C. Wang, "An integrated method for anomaly detection from massive system logs," IEEE Access, vol. 6, pp. 30 602–30 611, 2018.

[38] R. K. Alqurashi, M. A. AlZain, B. Soh, M. Masud, and J. Al-Amri, "Cyber-attacks and impacts: A case study in Saudi Arabia," International Journal, vol. 9, no. 1, 2020.

[39] I. Siniosoglou et al., "A unified deep learning anomaly detection and classification approach for smart grid environments," IEEE Transactions on Network and Service Management, 2021.

[40] J. Lee, J. Kim, I. Kim, and K. Han, Cyber threat detection based on artificial neural networks using event profiles. IEEE Access, 7, pp.165607-165626, 2019.

[41] M. Kravchik, and A. Shabtai, Detecting cyberattacks in industrial control systems using convolutional neural networks. In Proceedings of the 2018 Workshop on Cyber-Physical Systems Security 2018, pp. 72-83.

[42] A. Hashim, R. Medani, and T.A. Attia, Defences against web application attacks and detecting phishing links using machine learning. In 2020 International Con ference on Computer, Control, Electrical, and Electronics Engineering (ICCCEEE), pp. 1-6, IEEE. , 2021.

[43] A. Iliev, N. Kyurkchiev, A. Rahnev, and T. Terzieva, Some models in the theory of computer viruses propagation. LAP LAMBERT Academic Publishing, 2019.

[44] W.H. Lin, H.C. Lin, P. Wang, B. H. Wu, and J.Y. Tsai, Using convolutional neural networks to network intrusion detection for cyber threats. In 2018 IEEE International Conference on Applied System Invention (ICASI) , pp. 1107-1110, IEEE , 2018.

[45] Z. Ma, H. Yuanyuan, and J. Lu, "Trojan traffic detection based on machine learning," in 2020 17th International Computer Conference on Wavelet Active Media Technology and Information Processing (IC- CWAMTIP). IEEE, 2020, pp. 157-160.

[46] A. Alzahrani and D. B. Rawat, "Comparative study of machine learning algorithms for sms spam detection," in 2019 Southeast Con. IEEE, 2019, pp. 1-6.

[47] L. Chan et al., "Survey of AI in cybersecurity for information technology management," in 2019 IEEE technology & engineering management conference(TEMSCON). IEEE, 2019, pp. 1–8.

[48] J.-h. Li, "Cyber security meets artificial intelligence: A survey," Frontiers of Information Technology & Electronic Engineering, vol. 19, no. 12, pp. 1462–1474, 2018.

[49] J. Johansson, "Countermeasures against coordinated cyber-attacks towards power grid systems: A systematicliterature study," 2019.

[50] B. Kitchenham et al., "Systematic literature reviews in software engineering-a systematic literature review," Information and software technology, vol. 51, no. 1, pp. 7–15, 2009.

[51] I. Wiafe et al., "Artificial intelligence for cybersecurity: a systematic mapping of literature," IEEE Access, vol. 8, pp. 146 598–146 612, 2020.

[52] I. H. Sarker, M. H. Furhad, and R. Nowrozy, "AI-driven cybersecurity: an overview, security intelligence modeling and research directions," SN Computer Science, vol. 2, no. 3, pp. 1–18, 2021.

[53] Q. Chang, X. Ma, M. Chen, X. Gao, and M. Dehghani, "A deep learning based secured energy management framework within a smart island," Sustainable Cities andSociety, vol. 70, p. 102938, 2021.

[54] L. Malhotra, B. Bhushan, and R. V. Singh, "Artificial intelligence and deep learning-based solutions to enhance cyber security," Available at SSRN 3833311, 2021.

[55] S. Wang et al., "Detecting android malware leveraging text semantics of network flows," IEEE Transactions on In- formation Forensics and Security, vol. 13, no. 5, pp.1096–1109, 2017.

[56] Z. Zhang and Q. Yu, "Modeling hardware trojans in 3d ics," in 2019 IEEE Computer Society Annual Symposium on VLSI (ISVLSI). IEEE, 2019, pp. 483–488.

[57] Z. Fang et al., "Statistical modeling of computer malware propagation dynamics in cyberspace," Journal of Applied Statistics, pp. 1–26, 2020.

[58] S. Y. Yerima and S. Sezer, "Droidfusion: A novel multilevel classifier fusion approach for android malware detection," IEEE transactions on cybernetics, vol. 49, no.2, pp. 453–466, 2018.

[59] G. Iadarola, F. Martinelli, F. Mercaldo, and A. San- tone, "Towards an interpretable deep learning model for mobile malware detection and family identification," Computers & Security, vol. 105, p. 102198, 2021.

[60] P. Feng, J. Ma, C. Sun, X. Xu, and Y. Ma, "A novel dynamic android malware detection system with ensemble learning," IEEE Access, vol. 6, pp. 30 996–31 011, 2018.

[61] S. Srinivasan et al., "Deep convolutional neural network based image spam classification," in 2020 6th Conference on data science and machine learning applications (CDMA). IEEE, 2020, pp. 112–117.

[62] B. Bayar and M. C. Stamm, "Constrained convolutional neural networks: A new approach towards general purpose image manipulation detection," IEEE Transactions on Information Forensics and Security, vol. 13, no. 11, pp. 2691–2706, 2018.

[63] A. Lakshmanarao, P. S. P. Rao, and M. B. Krishna, "Phishing website detection using novel machine learning fusion approach," in 2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS). IEEE, 2021, pp. 1164–1169.

[64] A. Dal Pozzolo et al. "Credit card fraud detection: a realistic modeling and a novel learning strategy," IEEE transactions on neural networks and learning systems, vol. 29, no. 8, pp. 3784–3797, 2017.

[65] J. Lee, J. Kim, I. Kim, and K. Han, "Cyber threat detection based on artificial neural networks using event profiles," IEEE Access, vol. 7, pp. 165 607–165 626, 2019

[66] A. S. Sadiq et al., "An efficient ids using hybrid magnetic swarm optimization in wanets," IEEE Access, vol. 6, pp. 29 041–29 053, 2018.

[67] G. Kabanda, "Performance of machine learning and other artificial intelligence paradigms in cybersecurity" Oriental journal of computer science and technology 13.1, 2020, pp. 1-21.

Copyright (c) IARIA, 2022. ISBN: 978-1-61208-996-6