Artificial Intelligence Techniques in Cybersecurity Management

Mercy Ejura Dapel[1][0000-0003-3953-706X], Mary Asante[2],
Chijioke Dike Uba[1] and Michael Opoku Agyeman[1][0000-0002-3734-4451]

[1]Centre for Advanced and Smart Systems (CAST), University of Northampton, UK,
[2]University of Warwick Coventry UK,
Michael.OpokuAgyeman@northampotn.ac.uk

Abstract. The rapid development in internet services led to a significant increase in cyberattacks. The need to secure systems and operations has become apparent as cybersecurity has become a national concern. Cybersecurity involves techniques that protect and control systems, networks, hardware, software, and electronic data from unauthorised access. Developing an effective and innovative defensive mechanism is an urgent requirement as traditional 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 cyberattacks. To support this, researchers are focusing on approaches like Artificial Intelligence (AI) to improve cyber defence. 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, Cyberattacks, Cyber threats, Cybersecurity.

1 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 as cybercriminals exploit the vulnerability of individuals who use computer networks and rely on third party and cloud based data storage [2]. Providing security for systems has become difficult. Hackers are becoming smarter and more innovative in exploiting individuals and organisations. With cyberattacks and data breaches coming to light daily, cyberattacks have been ranked among the top 5 most likely sources of severe global risk [3]. Cyber fraud have become complex to track as cyber theft can originate from any part of the world. Organisations have become challenged with the complexity of cyberattacks which calls for the adoption of AI or intelligent methods to mitigate them. AI is a rapid growing technology that can analyse millions of datasets to track down cyber threats and prevent data breaches. 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, they have demonstrated effectiveness in detecting cyber-attacks with low false alarm rate.
Advancement in AI has 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 defence [9].
.

2 Related Surveys on AI in Cybersecurity

Vinayakumar et al. [10] proposed a highly scalable and hybrid deep neural network to monitor network traffic and host level events to raise alert for unforeseen cyberattacks proactively. They employed distributed and parallel machine learning algorithms with optimization techniques making them capable of handling a high volume of network and computing resources. Their scalability and real-time detection of malicious activities from early warning signals made their framework stand out. Artificial neural network (ANN) approach was employed as the computational model. To

increase training speed and avert over fitting, batch normalization and dropout approach was used. Machine learning techniques were compared, deep neural network performed well by detecting and classifying unforeseen and unpredictable cyber-attacks in real-time.
Sokolov et al. [11] analysed 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 is capable of real-time intrusion detection, inline intrusion prevention and network security monitoring.

Maimo et al. [12] explored a self-adaptive system for anomaly detection that identifies cyber-threats in 5G mobile networks, deep learning techniques was used to analyse network traffic by extracting features from network flows. The authors proposed a high-level cyber defence 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 flows 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. Random forest proved to be more robust, it could generalise 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 outperform 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 and 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] proposed the effectiveness of attention mechanism for intrusion detection based on Convolutional neural network (CNN) and LSTM model utilizing a 2018 dataset. 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. Mat et al. [18] adopted deep learning to analyse traffic, focusing on mitigating cyber-attacks with machine learning. Assembly module for statistics collection and adaptive machine learning module for analysing traffic and enforcing policies are the two main functionalities 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 analysing cyber-threat to match potential attack profiles by filtering malicious connections 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 Lenet 5 to classify network threats. The authors developed an improved behaviour-based model for anomaly detection by training a CNN to extract enhanced behaviour 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 algorithms were used. They showed the highest anomaly detection accuracy and improved performance of 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 cyberthreats. 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, Autoencoder 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 DNN and conventional machine learning models was carried out where both DCNN and LSTM models showed exceptional accuracy on the test dataset, this demonstrates the fact that Deep learning is a feasible and 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. Khaw et al. [25] proposed a deep learning based cyber-attack detection system to detect cyber-attack 25 minutes after the cyber-attack begun to enhance cybersecurity at its embryonic stage.

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 intrusion detection system (IDS) is widely accepted as a technique to monitor malicious activities [26].

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.

The growth of modern cyber infrastructure made network security more important. It is estimated that a trillion devices will be connected to the Internet by 2022 [28]. In-

trusion Detection Systems are tools with objective to detect unauthorized use and abuse a host network [29].

3 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, it utilises algorithms that make predictions and analysis possible of cyber threats in real-time. Neural networks have been used to detect classifying data as normal and abnormal [30]. Swarm intelligence methods handle feature selection to identify new intrusion. Technologies like expert systems and intelligent agents are applied to secure internet networks and improve intrusion detection performance [31]. With AI, complexity and model training times is reduced. Presenting new algorithms is a challenge and an opportunity for researchers [32]. AI is quickly becoming a tool for automating threat detection and responding effectively than traditional 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 thereby increasing accuracy and speed of cyber response. The major disciplines in AI are fuzzy logic, natural language processing, deep learning, machine learning, robotics and computer vision.

3.1 AI as a tool in combating cyberattacks Why Cybersecurity is essential

With the pace and increase in cyber-attacks, human intervention is insufficient for timely and appropriate response.AI technology is becoming very essential to information security, it is capable of analysing millions of data to track down 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 [33].This technology gathers large amount of data to identify suspicious behaviour that might lead to cyber threat. Processing and analysing 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 [34]. According to a report by Capgemini, the effort and cost of detecting and responding to cyber threats is lowered by 15% in some organisations with AI as more data is analysed. This technology learns from past patterns to become proficient in identifying suspicious activities thereby protecting information [35]. AI capabilities and adaptive behaviour can overcome the deficiencies of traditional cybersecurity tools.

3.2 Why Cybersecurity is essential

In the current digital age, data is susceptible to unauthorized access [36]. We live in a world where data is connected and stored on devices. This data contains sensitive information such as personal information, financial data, intellectual property and other forms of data which are exposed to unlawful access [37]. The world's fastest growing crimes are cyber-attacks. Cybercriminals have become smarter and their tactics are resilient to conventional cyber defense mechanisms. According to cybersecurity ventures report, global cybercrime is expected to grow by 15% yearly over the next 5years with financial loss reaching about $10.5 trillion USD annually [39]. Data

breach report that 43% of breaches are targeted at businesses [40]. Not only are businesses and organisations at risk, individuals are also at risk. It is important that everyone is aware of hazards associated with internet network use.

3.3 AI Algorithms in Cybersecurity

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

3.4 Impact of AI in Cybersecurity Management

AI presents advantages in several areas, cybersecurity is one of them. AI technology is capable of analysing millions of datasets to track cyber threats. The most significant contribution of AI is anomaly intrusion detection. This study reported improvement in accuracy, intrusion detection rate with reduced false alarm. Sezari et al. [23] demonstrated the performance of a system while comparing the false alarm rates of models on KDD 1999 Cup dataset, they applied a highly optimized deep feed forward 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. Utilising deep learning provided a system behaviour model that selects abnormal behaviour and is reliable with less complexity. Hsu et al. [22] 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 unseen 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 analyse 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 Maimo 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 Artificial Neural Network (ANN) [41]. CNN can detect anomalies in industrial control systems by detecting majority of attacks with low false positive rate [42]. A study conducted by Hashim et al. [43] showed that LSTM has high detection accuracy in securing websites from external breaches. Vinayakumar et al. [10] analysed 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.

3.5 Cybersecurity Frameworks and Solutions

This section presents analysis of cybersecurity frameworks and solutions (see Table 1).This table present cybersecurity solutions with the viewpoint from 2018 to 2021.

TABLE 1
Cybersecurity Frameworks and Solutions

Author	Framework/solutions	Cybersecurity Solution Used	Focus	Future Development
Johansson [44]	Countermeasures against coordinated cyber-attacks towards power grid systems	Cryptography	Intrusion Detection	investigate specific countermeasures against Coordinated cyber-attacks that must be tai- lored towards critical infrastructure beyond power grids.
Vinayakumar et al. [10]	Deep learning approach for intelligent intrusion detection system	Deep neural net-Works	Intrusion Detection	Adding a module for monitoring DNS and BGP events in the network by adding more nodes to the cluster. Improve performance by training complex DNNs architecture on advanced hardware through distributed ap- proach.
Sokolov et al. [11]	Analysis of cybersecurity threats in cloud applications using deep learning techniques	Deep neural net-Works	Intrusion Detection	Build a comprehensive framework for cybersecurity threat detection in the cloud
Maimo et al. [12]	A self-adaptive deep learning-based system for anomaly detection in 5G networks	Deep Neural net-Works	Anomaly detection	Extend experimental work related to detection/classification of deep learning models. Train two different levels using real data to evaluate the accuracy of anomaly detection.
Abraham et al. [8]	A comparison of Machine learning approaches to detect Botnet Traffic	Random Forest	Anomaly-based intrusion detection	Extend this approach to identify botnet traffic across a large network. Setup an online, quick response system that can identify, trigger and quarantine botnet traffic
Lin et al. [45]	Using Convolutional Neural Networks to network intrusion detection for cyber-threats	CNN	Intrusion Detection	Not stated in paper
Karatas et al. [46]	Deep learning in intrusion detection systems	Deep Learning	Network Intrusion detection	For future work using newest datasets with alternative deep learning approaches will behelpful.
Zhang et al. [13]	A multiple-layer representation learning model for network-based attack detection	DNN (CNN)	Intrusion detection	gcForest and CNN can be applied to various datasets for intrusion detection.
Zhong et al. [14]	Applying big data based deep learning system to intrusion detection	Deep learning	Intrusion detection	Future direction is to focus on advanced decision fusion algorithms combining outputs from different deep learning models. How to reduce the required minimum com- putational resources to achieve similar performance will be studied in the future
A. Dey [15]	Deep IDS: A deep learning approach for intrusion detection based on IDS 2018	Deep Learning (CNN And LSTM)	Intrusion detection	Implementing this methodology holds great scope for the future
Dawoud et al. [16]	Internet of things Intrusion Detection: A deep learning approach	Unsupervised deep learning	IoT Intrusion detection	Further investigation for deep learning in intrusion detection systems

Lin et al. [47]	ERID: A deep learning-based approach towards efficient real-time intrusion detection for IoT	ERID-unsupervised deep learning approach	IoT Intrusion detection	Not stated in the paper
Ishaque et al. [17]	Feature extraction using deep learning for Intrusion detection system	Deep learning	Intrusion detection	Not stated in the paper
Isa et al. [18]	Native software defined networks (SDN) intrusion detection using machine learning	Auto encoder and random forest algorithm	DDoS attack/Intrusion detection	Implementation and adoption of SDN-based intrusion mitigation architecture for further prevention process
Zeng et al. [20]	Deep full range: A deep learning based network encrypted traffic classification and intrusion detection framework	CNN, LSTM and Stack auto encoder	Network intrusion detection	Not stated in paper
Hsu et al. [22]	A deep reinforcement learning approach for anomaly network intrusion detection system	SVM and Random Forest	Network intrusion detection	Not stated in paper
Dey et al. [21]	Flow based anomaly detection in software defined networking: A deep learning approach with feature selection method	Gated Recurrent Unit- Long Short Term Memory (GRU-LSTM)	Network Intrusion detection	Implement the proposed model in a real environment with real traffic of network
Sezari et al. [23]	Anomaly-based network intrusion detection model using deep learning in airports	Feed forward neural network	Network intrusion detection	In the future simulation of local network of airports including series of modern and malicious network intrusion attacks like ran- somware to test and validate the model under predefined conditions.

4 Conclusion

This paper presented a survey of existing research on the application of AI in Cybersecurity. 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. Cybersecurity frameworks and solutions with viewpoint from 2018 to 2021 were summarised. Over the years, information and communication technology has advanced and cyberattack surface have continued to grow rapidly. Increased frequency of cyber-attacks has reinforced the need for cybersecurity initiatives. Traditional techniques have become inadequate in mitigating complex cyber-attacks, therefore solutions that are capable of tackling cyber threats in real-time is required. LSTM proved to be effective in terms of computational complexity while maintaining low training time. Random forest showed high accuracy in anomaly intrusion detection. It is important to highlight that there is no one size fits all solution to cybersecurity challenges. It can be considered as a holistic approach. In the future, LSTM and random forest can be combined as protection solutions for cybersecurity.

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. Yar, M. and Steinmetz, K.F., 2019. Cybercrime and society. Sage.
3. Ping, P., Qin, W., Xu, Y., Miyajima, C. and Takeda, K., 2019. Impact of driver behavior on fuel consumption: Classification, evaluation and prediction using machine learning. IEEE Access, 7, pp.78515-78532.
4. Ghahramani, M., Qiao, Y., Zhou, M.C., O’Hagan, A. and Sweeney, J., 2020. AI-based modeling and data- driven evaluation for smart manufacturing processes. IEEE/CAA Journal of Automatica Sinica, 7(4), pp.1026-1037.

5. Yu, K.H., Beam, A.L. and Kohane, I.S., 2018. Artificial intelligence in healthcare. Nature biomedical engineer- ing, 2(10), pp.719-731.
6. M. Chassignol, A. Khoroshavin, A. Klimova, and A. Bily- atdinova, 2018. Artificial Intelligence trends in edu- cation: a narrative overview. Procedia Computer Science, 136, pp.16-24.
7. M.J. Smith, 2018. Getting value from artificial intelli- gence in agriculture. Animal Production Science, 60(1), pp.46-54September 2020 Healthcare Data Breach Report: 9.7 Million Records Compromised https://www.hipaajournal.com/september-2020-healthcare-data-breach-report-9-7-mil lion-records-compromised/
8. B. Abraham, A. Mandya, R. Bapat, F. Alali, D. E. Brown, and M. Veeraraghavan, "A Comparison of Machine Learning Ap proaches to Detect Botnet Traffic," Proc. Int. Jt. Conf. Neural Nfile///C/Users/Admin/Desktop/ARTIFICIAL 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.2018.2879990Trautman, L.J. (2016). Corporate Directors and Officers Cybersecurity Standard of Care: The Yahoo Data Breach. SSRN Electronic Journal.
10. R. Vinayakumar, M. Alazab, K. P. Soman, P. Poor- nachandran, A. Al-Nemrat, and S. Venkatraman, "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. Micro electron. MIPRO - Proc., pp. 441–446, doi: 10.23919/MIPRO.2019.8756755.
12. L. Fernandez Maimo, A. L. Perales Gomez, F. J. Garcia Clemente, M. Gil Perez, and G. Martinez Perez, "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, 2019. A multiple-layer representation learning model for network-based attack detection. IEEE Access, 7, pp.91992-92008.
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, 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, 2020, October. Native SDN intrusion detection using machine learning. In 2020 IEEEEighth International Conference on Communications and Networking (ComNet) (pp. 1-7). IEEE.
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 learn- ing 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 De- tection System,” 2020 IEEE 9th International Conferenceon 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, A. Abiri Jahromi, M. F. M. Arani, S.Sanner, D. Kundur, and M. Kassouf, “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 Net- work for Cyberattack Detection in the Industrial Internet of Things,” IEEE Access, vol. 9, pp. 55595–55605, doi: 10.1109/ACCESS.2021.3071766.

28 Santos, L, Carlos Rabadão and R Gonçalves. “Intrusion detection systems in Internet of Things: A literature review.” 2018 13th Iberian Conference on Information Systems and Technologies (CISTI) (2018): 1-7.

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

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

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

32 I. Wiafe, F. N. Koranteng, E. N. Obeng, N. Assyne, A. Wiafe, and S. R. Gulliver, “Artificial Intelligencefor Cybersecurity: A Systematic Mapping of Literature,” IEEE Access, vol. 8, pp. 146598–146612,, doi: 10.1109/ACCESS.2020.3013145.

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

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

35 L.lazic, 2019, October. Benefit from Ai in cybersecurity. In The 11th International Conference on Business Information Security (BISEC-2019), 18th October 2019, Belgrade, Serbia.

36 Li, L., He, W, Xu, L., Ash, I., Anwar, M. and Yuan, X., 2019. Investigating the impact of cybersecurity policy awareness on employees’ cybersecurity behavior. Inter- national Journal of Information Management, 45, pp.13- 24.

37 J.P.Choi, D.S.Jeon and B.C.Kim, 2019. Privacy and personal data collection with information externalities. Journal of Public Economics, 173, pp.113-124.

38 N.Kshetri, 2019. Cybercrime and cybersecurity in Africa.Journal of Global Information Technology Management,22(2), pp.77-81.

39 E.Prester, J. Wagner, G. and G.Schryen, 2020. Fore- casting IT security vulnerabilities–An empirical analysis.Computers & Security, 88, p.101610.

40 S.A.Talesh, 2018. Data breach, privacy, and cyber insurance: How insurance companies act as “compliance managers” for businesses. Law & Social Inquiry, 43(2),

pp.417-440.

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

42 M. Kravchik, and A. Shabtai, 2018, January. Detect- ing cyber-attacks in industrial control systems using convolutional neural networks. In Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and Privacy (pp. 72-83).

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

44 J. Johansson, "Countermeasures against Coordinated Cyber-Attacks towards Power Grid Systems." 2019, [Online]. Available: https://www.diva- portal.org/smash/record.jsf?pid=diva2:1353250.

45 W.H.Lin, H.C.Lin, P.Wang, Wu, B.H. and J.Y.Tsai, 2018, April. 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.

46 G.Karatas, O.Demir, and O.K.Sahingoz, 2018, December. Deep learning in intrusion detection systems. In 2018 International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT) (pp. 113-116). IEEE.

47 M.Lin, B.Zhao, and Q.Xin, 2020, October. ERID: A Deep Learning-based Approach towards Efficient Real- Time Intrusion Detection for IoT. In 2020 IEEE Eighth International Conference on Communications and Net- working (ComNet) (pp. 1-7). IEEE.