American Journal of Computer Science and Technology
2022; 5(2): 108-114
http://www.sciencepublishinggroup.com/j/ajcst
doi: 10.11648/j.ajcst.20220502.22
ISSN: 2640-0111 (Print); ISSN: 2640-012X (Online)

Exploring Artificial Intelligence for Network Security: A Case Study of Malware Defence

Li Peng, Tuyatsetseg Badarch

School of Information Technology and Design, Mongolian National University, Ulaanbaatar, Mongolia

Email address:
ba.tuyatsetseg@mnun.edu.mn (T. Badarch)

To cite this article:
Li Peng, Tuyatsetseg Badarch. Exploring Artificial Intelligence for Network Security: A Case Study of Malware Defence. *International American Journal of Computer Science and Technology*. Special Issue: *Advances in Computer Science and Future Technology*. Vol. 5, No. 2, 2022, pp. 108-114. doi: 10.11648/j.ajcst.20220502.22

Received: April 5, 2022; **Accepted**: May 11, 2022; **Published**: May 24, 2022

Abstract: AI has many applications in network security. Network security is one of the most challenging situations. The paper carries out AI based network security analysis and prevention ways of the deep learning models in the network security. We focus on some specific AI applications including voice supervision of public network, malicious code monitoring, smartphone intrusion monitoring, HTTP security monitoring, mobile phone malicious APK code monitoring are bringing the solutions for network security. We studied there are powerful methods such as mobile phone malicious APR code monitoring employed Artificial Neural Network (ANN) model which detects and mitigates predictable and unpredictable DDoS attacks (TCP, UDP, and ICMP protocols). HTTP is running over TCP, then the web server can face many TCP-related attacks, therefore, we have an experiment of HTTP security monitoring, mobile phone malicious APK code monitoring. This paper presents a potential security threats from malicious uses of AI, and proposes ways to better prevent, and mitigate these threats. When planning HTTP service protection, we present it is important to keep in mind that the attack surface is much broader than just the HTTP protocol. We suggest promising areas for further research that could expand the AI based solutions for development of cloud computing-related technologies, and the combination of cloud computing and deep learning technology in the security area.

Keywords: Network Security, AI Network Security, Deep Learning

1. Introduction

The development of artificial intelligence has led to the emergence of many fields including Machine Learning (ML), computer vision, etc. In terms of cyber security strategies, AI and ML are the fields that will be utilized in the near future. In such cases, a scenario-based evaluation of electronic information security models may be the best answer, although it still faces future challenges [1]. With the development of science and technology, computer network communication technology has also been effectively stimulated. As an indispensable part of the Internet, the emergence of network communication provides a lot of convenience for people's life. However, in terms of the current situation, there are still some deficiencies in domestic network communication. This paper mainly takes the security status and significance of network communication as the starting point, combined with AI, and aid in the exploration and analysis of the future.

2. Exploration of Artificial Intelligence

Exploration of artificial intelligence is a new science that studies and develops the simulation, extension, extended theory, method, technology, and application system of human intelligence. It belongs to a branch of computer science. In today's world, businesses rely on internal computer systems and the Internet, and they can't afford to have their operations disrupted [2]. The imitation of human beings enables human wisdom to be reflected through machines and gives it the ability to analyze and solve problems. In certain aspects, artificial intelligence exceeds human intelligence. Artificial intelligence is currently implemented in a broad range of fields, which only furthers the cause of science. The challenge to security from identified and unidentified risks indicates the need for an extension of ongoing risk management systems

[3]. Simultaneously, the development of information technology and networks has had a great impact on production and daily life. AI models require specialized cybersecurity and protection solutions to minimize vulnerabilities and ensure better privacy of information. Every industry from daily shopping to business communications relies on networks which brings much convenience to our lives. However, there are some risks that occur in the process of using this easement of life due to the characteristics of network virtualization. We are often attacked by trojan horses, extortion viruses, and other network viruses. In the face of such situations, how to effectively prevent it is a problem that we need to focus on. Therefore, the traditional network security management models are not enough to protect our networks from these attackers. Strengthening network security management through artificial intelligence is the main trend of future development.

3. Deep Learning

Deep learning, one of the most prominent components of AI, and is making a huge progress in solving challenges related to network security threats [4]. ANNs are made up of two visible layers (an input layer and an output layer) as well as one or more hidden layer. The focus of artificial intelligence is deep learning. Figure 1 shows the main structure of learning methods. Deep learning is a nonlinear neural network structure with multiple hidden layers. The deep neural network is composed of an input layer, several hidden layers, and an output layer. There are several neurons in each layer, and there are connection weights between neurons.

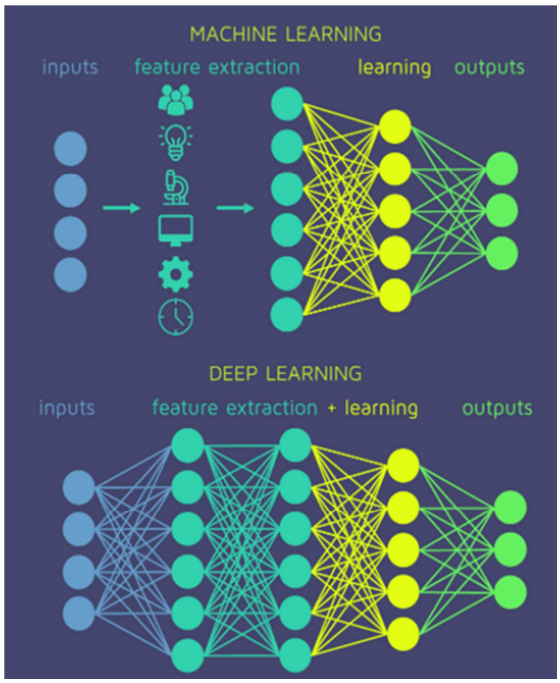

Figure 1. *Hidden layers architecture.*

Each neuron simulates human neuron cells, and the connection between nodes simulates the connection between nerve cells. Although complete automation of detection and analysis is a desirable goal, deep learning's performance in cybersecurity should be evaluated with sensitivity [5].

Figure 2 shows the nomenclature of current deep learning models for information security of a network. Many studies have shown that deep learning technology can assist us in developing the finest security models.

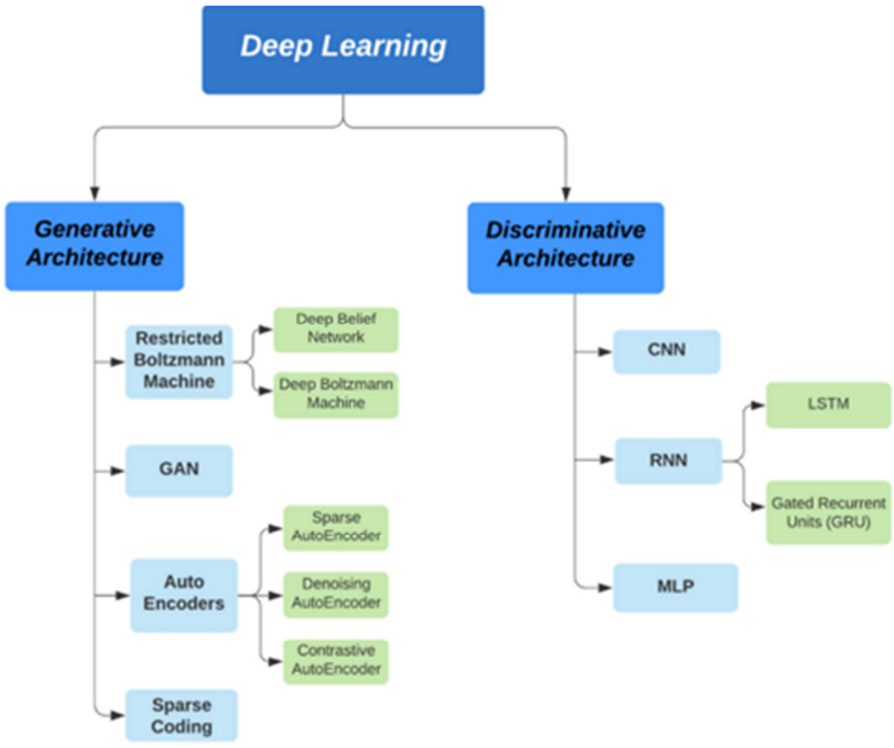

Figure 2. *Nomenclature of current deep learning models for electronic information security.*

DBNs or RBMs or deep autoencoders coupled with classification layers, restricted Boltzmann machines (RBMs), recursive neural networks (RNNs), and several other hybrid DL models have been successfully deployed and have shown promising results in terms of electronic information security, described in detail by Daniel S. Berman et al [6-7]. Typical deep learning models include a convolutional neural network, DBN and stack self-coding network models. A deep Boltzmann machine (DBM) is a type of artificial neural network (ANN) that can be put to use in approximate probability models. Artificial neural networks (ANNs) are based on the biological neural networks seen in the human brain and are analogous to them. They are built up of artificial neurons that are interconnected and interact with one another [13-14].

4. On the Deep Learning Models in Network Security

Typically, in terms of performance, the deep learning models have surpassed the generic machine learning approaches. Unlike traditional machine learning approaches, deep learning models use layers of multiple artificial neurons to work efficiently at a level that can learn extremely complex tasks without being explicitly programmed [8]. DL models have a deep learning capability. Moreover, DL models generate an output without any external intervention.

In this paper, we tend to focus on the important approaches in recent AI-enabled techniques, especially, DL to enhance a sense of security in mobile networks.

4.1. Public Network Voice Supervision

5G networks that are currently in trend have also implemented deep generative models [9]. It includes a 5G traffic modelling approach as well as a strategy for determining the required spectrum for privatized 5G networks. By learning from real traffic traces obtained from a large mobile network operator, the generative model is able to produce realistic traffic.

4.1.1. Characteristics of Public Mobile Network Voice Transfer

As a research result, deep neural networks in public mobile network applications efficiently handle the basic objective of information security. Information security in mobile networks is one of the applications of AI enabled networks. It is capable of intrusion detection, network analysis, and even modelling the time series profile of public LTE networks [10]. The main problems are:

(1) Increase in voice crime;
(2) Huge voice volume;
(3) Different from text analysis (sensitive keywords);
(4) The error rate of the existing speech recognition system is too high.

4.1.2. Principles of Public Network Voice Supervision

Firstly, a large number of speech samples are entered into the deep learning neural network, and the abstract features of speech samples are obtained. This allows for obtaining the speech feature information base.

Second, the speech information obtained in the previous step is entered into the deep learning neural network to obtain the abstract representation of speech information, which is compared with the speech feature database.

Finally, a classifier can distinguish normal information from suspicious information. Normal information is ignored directly, suspicious information is recognized as text information through speech recognition, and is screened manually, to realize the analysis and early warning of speech information.

4.2. Deep Learning Models Based on Artificial Intelligence

Existing security solutions appear to be insufficient for the impending mobile technologies, which has increased transmission rates on networks. With improvements in AI technology, complex models are making breakthroughs in the security of various critical applications, many of which are based on mobile networks [1].

4.2.1. Malicious Code Monitoring for Network Security

This is clear that only smart technologies can help defend against sophisticated cyber devices, with the sophistication of malware and cyber-arms increasing exponentially in the past two years [11]. Regarding the study, we can understand what will happen as cybercrime overtakes certain protections. When the security of knowledge depends entirely on human-based surveillance capacities, then someone is in trouble. After that, cybercrime isn't necessarily pursuing a fixed timetable and shouldn't suit your susceptibility to cyber protection either [12]. From AI studies, using search terms such as “Electronic Information Security”, “Cyber Security models”, “Mobile Network Security”, “Cyber-attack”, “Artificial Intelligence”, “Machine Learning”, “Deep Learning Security model” roughly 1800 plus articles were found [12-15].

Malicious codes such as mobile ransomware, crypto mining, fraudulent apps, and banking trojan horses are among the most common dangers to mobile networks. Malicious code refers to computer code intentionally written by individuals or organizations that have potential security risks to computers or networks. It usually includes malicious shareware, advertising software, trojan horses, viruses, worms, etc. Each kind of malicious code has different varieties.

4.2.2. Automation of Detection Based on Deep Learning Models

Many studies have shown that deep learning technology can assist us in developing the security models. The network model is mainly divided into three modules (Figure 3):

(1) Data preprocessing;
(2) Operation code feature extraction;
(3) Deep confidence network module.

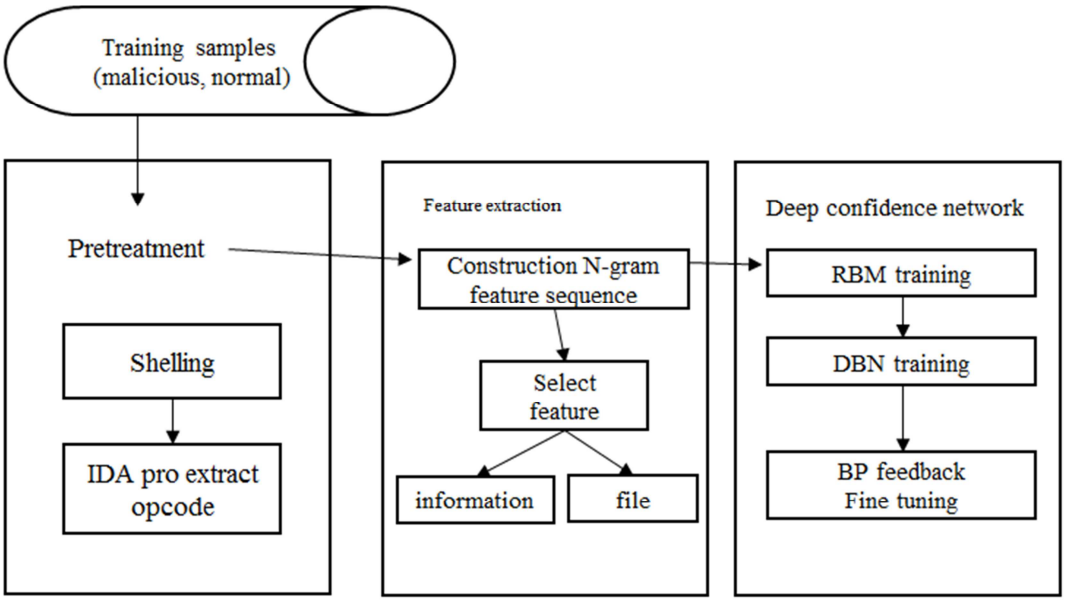

Figure 3. *Main modules of DBN.*

Although complete automation of detection and analysis is a desirable goal, deep learning's performance in cybersecurity should be evaluated with sensitivity [6].

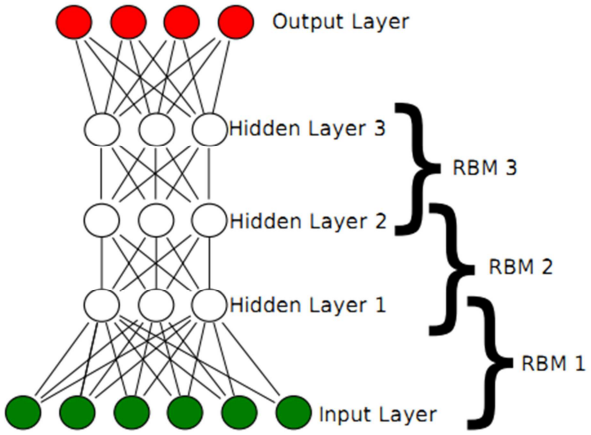

Figure 4. *Unsupervised feedback structure.*

Malware detection of Deep convolutional neural networks (DCNN) has an advanced feature to enable.

1) Hand-engineered malware features have no requirements.
2) To make the process easier, the network is trained end-to-end to understand suitable properties and conduct classifications.
3) After the model has been trained, it may be effectively and executed on a GPU with efficiency, permitting a large number of files to be scanned rapidly.
    1. (RBM), the adjustment process of restricted a Boltzmann machine is the adjustment process between each layer from bottom to top, and the weights of the whole depth model are initialized in this way;
    2. Unsupervised feedback adjustment of deep belief network (DBN) is implemented. First, it carries out a bottom-up identification model transformation, then performs a top-down generation model transformation, and finally, through continuous adjustment between different levels, the generation model can reconstruct the original sample with low error, to obtain the essential characteristics of this sample (Figure 4). This is the highest abstracted representation of the depth model.
    3. BP feedback adjustment: fine-tune the BP feedback based on the error between the original class mark of the sample and the target output to adjust the weight of the whole network layer.

4.3. Smartphone Features of Intrusion Detection System

Intrusion Detection System (IDS) is implemented in Artificial Neural Network (ANN), Stacked Auto Encoder (SAE) [13]. Regarding this feature, we can select the most important features only to reduce their dimensionality which is suitable for resource-constrained devices. It can reduce input features.

4.3.1. Main Features of Smartphone Intrusion Detection

Intrusion detection is a preventive security mechanism. RBM and RNN [14] use smartphone featured intrusion detection mechanism that can manage traffic fluctuation. In addition, this technique provides optimization of the computational resources at any point in time along with the refinement of performance and behavior of analysis and detection procedures. The architecture may adapt and adjust by itself. The anomaly detection system depends on the amount of network flows gathered in real-time from 5G subscribers' user equipment, reducing resource consumption and maximizing efficiency [14].

By monitoring smartphone status and network behavior, it can detect -when intrusive behavior occurs. Deep learning intrusion detection has two main directions: to find the rules

and patterns of intrusion and compare them with the training model and to be used for anomaly detection to find out the user's normal behavior and create a normal behavior library. Due to the abundance of network traffic handled by a RAN, the model is not trained accurately for a real-time environment.

4.3.2. Features of Deep Belief Network

In mobile networks, Deep Belief Networks can be particularly useful for information management and transmission. Deep belief network is mainly composed of restricted Boltzmann machine model (RBM) and BP neural network by Greeshma Arya et al. [15]. Given that data transfer in 5G WSN communication may be performed efficiently. The detection scheme is unaffected by the number of attacked data, and certain degrees of noise in the surroundings.

1. Process the input data, and then use RBM for unsupervised training to make the output features of each layer more significant. This ensures the most retained feature information when the original features are mapped inward to different spaces. The next step is to form a training model and obtain more obvious feature information;
2. The last layer uses BP neural network. BP network layer receives the feature vector output by the RBM layer as its input data and the training process of this layer are supervised. After the number of layers is obtained, the classification parameter is set to 2. From here, the final error value is obtained, and the corresponding accuracy is calculated.

5. Analysis of Malicious Features Based on HTTP Content

There are challenges of adversarial AI and ethical AI applications, leading to special recommendations on key considerations for fielding AI systems that align with democratic values, civil liberties, and human rights [16-18]. To pursuit of resistant systems, computer science R&D has been underway on methods for making AI systems more resistant to adversarial machine learning attacks [19]. According the related study, mobile phone malicious APR code monitoring employed Artificial Neural Network (ANN) model to detect and mitigate predictable and unpredictable DDoS attacks (TCP, UDP, and ICMP protocols). HTTP is running over TCP, then the web server can face many TCP-related attacks [20].

5.1. HTTP Malicious Behavior

With the development of web applications, the use scope of the HTTP protocol is further expanded, and it also begins to become the main carrier of the network's malicious behavior. Therefore, many malicious behavior characteristics are reflected in the request data. Many web attacks such as SQL injection, cross-site script attack, cookie tampering, and other malicious behaviors are reflected in HTTP requests, and the attack methods of requests are changeable. The malicious characteristics are not only reflected in a specific place but also concentrated in the path or other parts.

5.2. HTTP Security Monitoring Model

When planning HTTP service protection, it is important to keep in mind that the attack surface is much broader than just the HTTP protocol. In this article, we focus on HTTP security monitoring. First, the HTTP request format and malicious characteristics are analyzed. According to the data characteristics, a large number of features are designed from the three aspects: structure, length and characters. Moreover, a sensitive thesaurus is automatically generated to count the number of sensitive words in the request content, which is also regarded as one of the characteristics of describing the request.

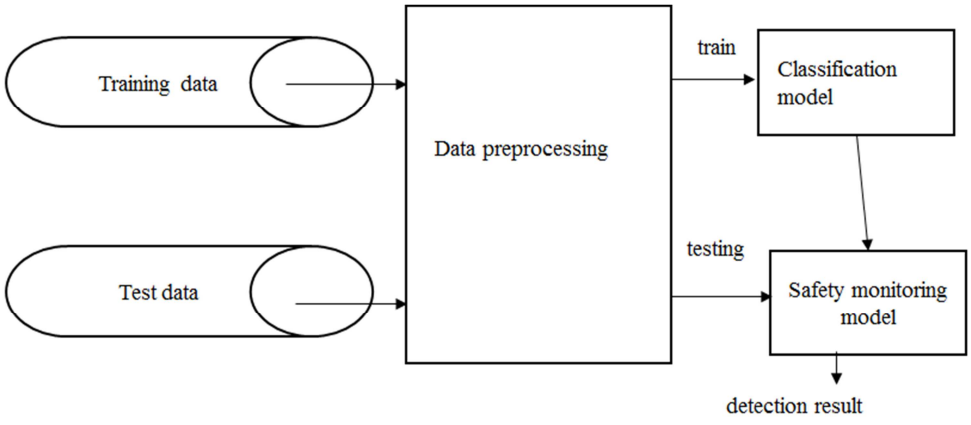

Figure 5. *Feature selection algorithm.*

Then, information entropy is used to select the distinguishing features from the designed features, and these selected features are used to quantify the request (Figure 5). After training the security detection model with a classification algorithm, it can be used to detect the category of data.

5.3. Mobile Phone Malicious APK Code Monitoring

The number of mobile intelligent devices and user data traffic on Android platforms have increased exponentially. The Android malicious application detection system based on

deep learning has broken through the technical barrier of low efficiency of traditional algorithms. It has not only achieved feasibility proof in theory, but also achieved good detection results in practical verification;

It is mainly divided into three modules: (1) APK code feature extraction module, (2) "training" module, (3) unknown APK sample detection module;

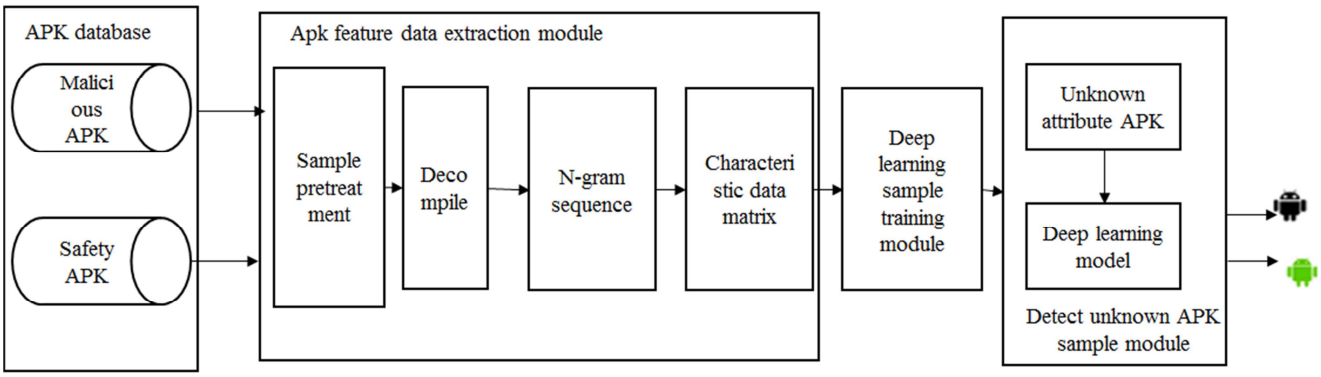

Figure 6. *Mobile phone malicious APK code monitoring.*

The process is (Figure 6):

(1) Static code analysis technology is used to extract multi-class behavior feature data of Android applications;
(2) Convert the characteristic data into sample characteristic matrix;
(3) Then the convolution neural network algorithm file is used to train the sample characteristic matrix;
(4) Finally, batch download the Android application that does not participate in the training of the deep neural network, and then execute the system steps for its APK to obtain the relevant prediction report of unknown sample APK.

6. Conclusion

At present, the application of deep learning in information security is still in its infancy, but it provides a new idea for the current field of information security. With the development of deep learning, the application of deep learning in information security will be more and more mature and extensive. We focus on security approaches based on AI enabled techniques that can be employed for the network security.

With the development of cloud computing-related technologies, cloud computing and deep learning technology can be combined to study information security technology.

Acknowledgements

I want to thank my advisor, for her significant help.

References

[1] Chaitanya Gupta, Ishita Johri, Kathiravan Srinivasan, Yuh-Chung Hu, et al. (2022). A Systematic Review on Machine Learning and Deep Learning Models for Electronic Information Security in Mobile Networks Sensors, Special Issue Emerging Sensor Communication Network based AI/ML Driven Intelligent IoT), 2022, 22 (5), 2017. https://doi.org/10.3390/s22052017.

[2] Ashenden, D. Information Security management: A human challenge? Inf. Secur. Tech. Rep. 2008, 13, 195–201.

[3] Suo, H.; Liu, Z.; Wan, J.; Zhou, K. Security and privacy in mobile cloud computing. In Proceedings of the 9th International Wireless Communications and Mobile Computing Conference (IWCMC), Sardinia, Italy, 1–5 July 2013; pp. 655–659.

[4] Ahmad, Z.; Khan, A. S.; Shiang, C. W.; Abdullah, J.; Ahmad, F. Network intrusion detection system: A systematic study of machine learning and deep learning approaches. Trans. Emerg. Telecommun. Technol. 2020, 32, e4150.

[5] Apruzzese, G.; Colajanni, M.; Ferretti, L.; Guido, A.; Marchetti, M. On the Effectiveness of Machine and Deep Learning for Cyber Security. In Proceedings of the 2018 10th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia, 29 May–1 June 2018.

[6] Berman, D. S.; Buczak, A. L.; Chavis, J. S.; Corbett, C. L. A Survey of Deep Learning Methods for Cyber Security. Information 2019, 10, 122.

[7] Kong, L.-J. An improved information-security risk assessment algorithm for a hybrid model. Int. J. Adv. Comput. Technol. 2013, 5, 2.

[8] Luong, N. C.; Hoang, D. T.; Gong, S.; Niyato, D.; Wang, P.; Liang, Y.-C.; Kim, D. I. Applications of Deep Reinforcement Learning in Communications and Networking: A Survey. IEEE Commun. Surv. Tutor. 2019, 21, 3133–3174.

[9] Kim, D.; Ko, M.; Kim, S.; Moon, S.; Cheon, K.-Y.; Park, S.; Kim, Y.; Yoon, H.; Choi, Y.-H. Design and Implementation of Traffic Generation Model and Spectrum Requirement Calculator for Private 5G Network. IEEE Access 2022, 10, 15978–15993.

[10] Xiao, A.; Liu, J.; Li, Y.; Song, Q.; Ge, N. Two-phase rate adaptation strategy for improving real-time video QoE in mobile networks. China Commun. 2018, 15, 12–24.

[11] Use of Artificial Intelligence Techniques / Applications in Cyber Defense. (n.d.). Retrieved 14 August, 2020, from https://www.researchgate.net/publication/333477899_Use_of_Artificial_Intelligence_Techniques_Applications_in_Cyber_Defense.

[12] Parati, N., & Anand, P. (2017). Machine Learning in Cyber Defence. International Journal of Computer Sciences and Engineering, 5 (12), 317–322.

[13] Aminanto, M. E.; Kwangjo, K. Deep Learning-based Feature Selection for Intrusion Detection System in Transport Layer 1). In Proceedings of the Korea Institutes of Information Security and Cryptology Conference, Seoul, Korea, 30 November–2 December, 2016.

[14] Maimo, L. F.; Gomez, A. L. P.; Clemente, F. J. G.; Gil Pérez, M.; Perez, G. M. A Self-Adaptive Deep Learning-Based System for Anomaly Detection in 5G Networks. IEEE Access 2018, 6, 7700–7712.

[15] Arya, G.; Bagwari, A.; Chauhan, D. S. Performance Analysis of Deep Learning-Based Routing Protocol for an Efficient Data Transmission in 5G WSN Communication. IEEE Access 2022, 10, 9340–9356.

[16] "Establishing Justified Confidence in AI Systems," Chapter 8, Report of the National Security Commission on AI, March 2021. https://reports.nscai.gov/final-report/chapter-7/

[17] E. Horvitz J. Young, R. G. Elluru, C. Howell, Key Considerations for the Responsible Development and Fielding of Artificial Intelligence, National Security Commission on AI, April 2021.

[18] Kumar, Ram Shankar Siva, et al. Adversarial machine learning-industry perspectives. 2020 IEEE Security and Privacy Workshops (SPW). IEEE, 2020.

[19] A. Madry, A. Makelov, L. Schmidt, et al. Towards deep learning models resistant to adversarial attacks, ICLR 2018. https://arxiv.org/pdf/1706.06083.pdf

[20] Saied, A.; Overill, R. E.; Radzik, T. Detection of known and unknown DDoS attacks using Artificial Neural Networks. Neurocomputing 2016, 172, 385–393.