Moving from Detection Centric to Prevention Centric Security Using Automation: A Survey

RVS Sravanthi and Nisha T N*
Symbiosis Centre for Information Technology, Symbiosis International (Deemed University), Pune, Maharashtra, India Email: nisha@scit.edu*

Abstract. In the present time, cybersecurity plays a crucial role in every aspect. Protecting data, hardware, software alone is not sufficient as the technology is growing exponentially and information is easily available. Regarding artificial intelligence data, Sentinel One platform, endpoint security shows that from February 20, 2020, to March 17, 2020, the trend was in an upward motion, as the attacks attempted has peaked to 145 threats per 1,000 endpoints, in comparison to 31 or 38 at the start of that period. According to the Q2 2018 Threat Study, the quarterly report by Nexus guard, the average denial-of-service (DDoS) attack grew to more than 26Gbps, up 500 percent in scale. Regardless of the complexities of the modern cyber climate, stereotypic defense solutions do not fulfill the information security requirements. Earlier detection techniques were sufficient to protect the cyber environment, but due to growing cyber threats such as Ransomware, malware, DDoS, we need strong protection techniques to restrict the threat's entry. Given this context, this study explains the evolution of the Preventive techniques and detective techniques; both the approaches are complementary, which would be discussed in this paper by considering Automation Technology. It introduces the survey of various Automation Technologies implemented for the advancement of prevention-centric security. Based on the evaluation metrics, the selection of better technology is concluded.

Keywords: Detection, Prevention, Network Security, Artificial Intelligence, Machine learning, Neural Network.

1. Introduction
As the number of new threats and indicators of incidents is steadily growing and there is no indication that this trend will be halted soon [1]. Only preventing and managing these threats individually has become almost impossible, as accurate classification or effective threat taxonomies vary within current solutions, and sometimes knowledge dissemination is fragmented or restricted to selected users, which presents considerable constraints [2].

In the era of 'Millennials' or 'social media generation,' individuals who grew up with technologies to become so-called digital natives, collaboration and sharing within a community has become a school of thought towards life [3]. This trend of sharing all kinds of information within a community for the IT-community can also be observed recently [4]. In community-driven domains such as IT, the fostering of cooperation and the exchange of knowledge is crucial. New threats can be detected quicker in a collaborative effort, and responses can be properly organized through the entire
population [5] owing to data protection on the one side and knowledge exchange. With all the growing technology and the cyber threats, detection of the attack is enough. We need a preventive system to block the attack and secure the system [6].

In this paper, we would discuss how automation has improved preventive techniques and move from detective techniques. We are aware of the basic network security system, Intrusion Detection System (IDS), which could not be alone sufficient for any work station that has bought the Intrusion Prevention System (IPS) back to the service. According to the Internet Security [7] Threat Report, there is an increase of 25% in several cyber-attack categories by implementing calamitous malware [8]. The spam attacks also continued to escalate in 2018, as they have done since 2015 every year. In recent times, we have learned that the Ransomware attacks have increased exponentially, along with data breaches to the organization that has disrupted the reputation and financial loss to the companies [9]. During the Covid-19 pandemic, lockdown remote working was mandatory, which led to the high growth of data theft and cyber-attacks [10]. According to Sophos IT security company reports, around 59% of cyber attacks were over cloud data [11].

This research paper is categorized in a particular format: Section 3 Systematic Literature Review discusses the Machine learning algorithms evolution of prevention centric from detection centric and provides the details about the Ransomware and its existing prevention strategy and the improved threat intelligence to protect data in the cloud and the remote working organization. In Section 4, the evaluation metrics and in Section 5 conclusion is discussed.

2. Literature Review

In recent times, the increase in data breach, malware attacks, zero-day vulnerability, and other cyber-attacks are directly proportional to the increase in technologies and innovations [12]. Automation of the technology is required as the threats are growing exponentially, and it is not feasible to work with the traditional models with human intelligence [13]. Automation is the processing as per pre-programmed rules. Artificial Intelligence is the processing of the pre-programmed rules to impersonate human behavior [14]. Machine Learning is a subset of AI, so it processes the pre-programmed rules to impersonate human behavior and iteratively improve its system [15]. Deep Learning is a subset of ML; thus, it processes the pre-programmed rules to impersonate human behavior and iteratively improve its system without any surveillance [16]. There are three fundamental approaches for automation that are explained in a simple diagram as follows. Figure 1 shows the Automation Technology Hierarchy.

![Figure 1: Automation Technology Hierarchy](image)

2.1 Artificial Intelligence

Artificial Intelligence techniques such as data mining, artificial neural networks, expert systems, and fuzzy logic can be combined with conventional statistical and procedural approaches for analyzing sensor data obtained [17], identifying patterns of detection, filtering, and correlating events to help intrusion prevention and security event management [18]. Statistical approaches have been used to
create models for intrusion and identification of faults, but these models cannot learn and adjust over the time-period [19]. Table 1 shows the Artificial Learning’s implemented for prevention-centric security.

**Table 1: Artificial Learning’s implemented for prevention centric security**

| Reference                  | AI Techniques                         | Learning’s                                                                 |
|----------------------------|---------------------------------------|---------------------------------------------------------------------------|
| (Klieber et al., 2016)     | First-order logic solver              | Implementing the first-order logic solver to validate access controls' security and apply the suitable condition if not. This vulnerability is present in the top 10 on the OWASP list (OWASP, 2017). |
| (K. Hasan et al., 2019)    | Alpha-Go (Tree search algorithm)      | Performs adequate prediction diagnosis of SIEM-based analysis data to automate threat correlator. |
| (Le et al., 2017)          | Symbolic Execution, Inductive Synthesis | In this paper, test cases are used to set up search space to identify standard repair code and test candidate fixes. |
| (Shoshtaishvili et al., 2018) | Symbolic execution and fuzzer.        | Search for vulnerabilities on contaminated data. Avoids the direction of the explosion of symbolic execution by integrating it intelligently with fuzzing techniques. |
| (Wong et al., 2018)        | Symbolic execution                    | According to the research paper, it is predicted that AI approaches, together with robust data management systems, would allow the surveillance data and significant infectious disease analysis to support potential disease generated through the medical professionals, healthcare service providers, and government agencies. |

**Table 2: Unsupervised Learning Techniques implemented for prevention-centric security.**

| References                  | Unsupervised Learning Techniques                      | Learnings                                                                 |
|-----------------------------|-------------------------------------------------------|---------------------------------------------------------------------------|
| (Saha et al., 2014)         | Support Vector Machine (SVM) and Rough Set Theory (RST) | Several Machine Learning algorithms would be shortlisted and experimented with over the IDPs application layer for a proof-of-concept to protect the current use cases. |
| (Johnson AP et al., 2020)   | Discriminative deep belief network (DDBN)             | According to the ROC comparison, the DDBN cyber intrusion prevention effect is efficient than those of the Hopfield, SVM, DBN-RFS, and GAN classifiers by different comparison trials, and it reduced classification error rate in cyber intrusion prevention. |
| (Diaz Rozo et al., 2017)    | Gaussian mixture model clustering, k-means clustering, hierarchical agglomerative clustering. | The clustering algorithm for the performance testing of a CPS for machine component knowledge is discovered. |
| (Omar Iraqi et al., 2019)   | Local Outlier Factor algorithm is combined with        | The framework is implemented in a Java environment. Its effectiveness and efficiency are |
the Clark distance evaluated on an open source ERP and enterprise-grade while comparing various outlier distance functions and detection algorithms.

(Z. Qu et al., 2018) GRU neural network The proposed model is an improved auto-encoder model. It identifies the links in long sequences with fast training and provides effective and accurate anomalies for the test data.

**Table 3**: Supervised Learning Techniques implemented for prevention centric security

| References                      | Supervised Learning Techniques                                            | Learnings                                                                 |
|---------------------------------|---------------------------------------------------------------------------|---------------------------------------------------------------------------|
| (Azab et al., 2016)             | Correlation-based Feature Selection (CFS) Algorithm and C4.5 Algorithm     | Classification of Network Information Flow Analysis (CONIFA) methodology is compared to be better than the Standard framework, and it is valid to detect zero-day versions of botnet. |
| (A. G. Bucevschi et al., 2019)  | Perceptron algorithm and by application of Conditional Mutual Information Maximization criteria | Detection of anomalies in file which contains PowerShell code. The model being equipped with the specific feature series provides detection rate better than the basic metric. |
| (Q. Shafi et al., 2018)         | k-fold cross-validation                                                   | The classifiers implemented were Alternate Decision Tree (ADT) classifier, E3ML, RNN, and MLP to improve the prevention of attacks on fog-based Software Defined Network (SDN) |
| (D. Su et al., 2019)            | n-fold cross-validation                                                   | In this paper, Machine learning classifiers Random Forest (RF), Logistic Regression (LR), Support Vector Machine (SVM), Decision Tree (DT), and along with Ensemble Learning to overcome the code obfuscation problem of locker-ransomware. |
| (Uwagbole et al., 2016)         | Two-Class Logistic Regression (TCLR) and Two-Class Averaged Perceptron (TCAP) | To prevent SQL Injection Attacks (SqliAs), numerical encoding is implemented by providing the input database to the Artificial Neural Network (ANN), Two-Class Logistic Regression (TCLR), and Two-Class Averaged Perceptron (TCAP). This approach was then made to the focus of the pragmatic assessment of this model's suitability in the precise classification of legitimate SqliAs, payloads, and web requests. |
| (E. Mitchell et al., 2015)      | Random algorithm Forest                                                  | This paper proposed a novel method of inertial, wearable sensor frame to differentiate between symmetric and asymmetric running patterns in an unconstrained environment. Using Short Time Fourier Transform (STFT) and other time-domain functions, the system can automatically distinguish asymmetry/symmetry. |

2.2 **Machine Learning**

Machine Learning is a model that has the concept of learning from past events and improving data processing automation [20]. It can be categorized into two categories unsupervised learning, where the
model learns that decision-making based on the inputs and supervision is not required, and supervised learning as the name suggests, required supervision, and it learns from the labeled training data previous experience [21]. Supervised learning has two types of techniques - Classification and Regression, and Unsupervised Learning has two types of techniques: cluster and Association [22]. Table 2 shows the Unsupervised Learning Techniques are implemented for prevention-centric security. Table 3 shows the Supervised Learning Techniques implemented for prevention-centric security.

2.3 Deep Learning

Deep learning methods aim to learn feature hierarchies with features from higher hierarchy levels generated by the composition of lower-level features [23]. Multi-level automatic learning features allow a system to learn the input and the output data directly from the complex functions mapping without relying entirely on human-made features. Deep learning is a class of topologies and algorithms that can be applied to a large array of issues [24]. The architectures of deep learning are Recurrent Neural Network (RNN) it is widely used for speech and hand recognition, Convolutional Neural Network (CNN) it is widely used for Natural language processing, image recognition, and video analysis and Deep Belief Network (DBN) it is widely used for Image recognition [25], failure prediction, natural language understanding, and information retrieval. Table 4 shows the Deep Learning Techniques implemented for prevention-centric security.

| Reference                        | Deep Learning Techniques                                                                 | Learning’s                                                                 |
|----------------------------------|------------------------------------------------------------------------------------------|----------------------------------------------------------------------------|
| (G. Xu et al., 2019)             | Text- Convolutional neural network (CNN) and Recurrent Neural Network (RNN)                | To improve sensitive information detection, Text-CNN is more efficient than RNN as it will improve the accuracy of detection; time efficiency is more and is efficient in model training for prevention of data leakage and protection of sensitive data. |
| (Lai et al., 2019)               | Mahalanobis distance                                                                      | The feature mapping method based on Mahalanobis distance was implemented based on Deep Learning. |
| To attack classification and achieve anomaly detection for SCADA systems (G. Xian et al., 2020) | Discriminative deep belief network (DDBN)                                                | DDBN method was used for large-scale. It is based on deep learning of non-local and local regularization to prevent an attack as well as detect any cyber-attack |
| (Sarker et al., 2020)            | IntruDTree Algorithm                                                                      | This model decreases the computational complexity by reducing the feature dimension. The model is effective in terms of accuracy in the prediction of unknown test cases also. |
| (Ding, L. et al., 2018)          | Convolution Neural Network (CNN) and Long Short-Term Memory (LSTM)                        | The model helps to provide visual feedback of the accurately detected unsafe behaviors, which would prevent accidents. This model prediction leads to perfunctory management interference, which would help to change the immediate action. |
| (Z. Li et al., 2018)             | Wasserstein generative                                                                    | The approach generated is a deep adversarial model. |
| Method/Algorithm/Learning Method | Description |
|---------------------------------|-------------|
| adversarial networks (WGANs) | learning method WGAN that is used to generate fuzzing data, and the method is significant for industrial security and is used for industrial control systems (ICS) testing, EtherCAT, and Modbus-TCP protocol. |
| Deep neural network (DNN) | The proposed model is based on a game model and Deep neural network (DNN); it is a wireless network defense method. It is experimented with to dissolve the inadequacy of fuzzy conclusion and subjective randomness of traditional wireless network defense methods. This method also generates the defense map and state attack of the network. |
| Deep Neural Networks (DNN), Long Short-Term Memory Recurrent Neural Networks (LSTM-RNN), and Deep Belief Networks (DBN) | A double Particle Swarm Optimization (PSO)-based algorithm is proposed to improve intrusion prevention for network security. The model selects the hyperparameters and subset in one process, and the deep learning algorithms test the model performance. |
| Convolution Neural Network (CNN) | The Novel Deep Learning Framework (NDLF) model is used to integrate two fields routing and image processing in a wireless sensor network to identify abnormal activities and data stream for Multipath routing in WSN. |
| Long Short-Term Memory (LSTM), Deep neural network (DNN), and Convolution Neural Network (CNN) | The ad-hoc data packets are captured using a plug-and-play device, and the deep network model using Convolution Neural Network (CNN), Deep neural network (DNN), and Long Short-Term Memory (LSTM) detects the XSS, DoS attacks, and SQL attacks and protects the ad-hoc network. |

### 3. Methodology

#### 3.1 Manage Cyber Security

Cybersecurity is the protection for hardware, software, and firmware of a computer. Cybersecurity is important as it consists of different sensor types of data such as financial data, personal data, government data, and even military data. To meet the business requirement, organizations share sensitive data through the internet [26]. Cybersecurity is an ever-evolving system from perimeter security to encryption; the steps for security have evolved. The rule of cybersecurity which is to be followed is Confidentiality, Integrity, and Availability. Organizations promote better adaptive and proactive methodology to detect and prevent attacks and secure the data from any attack or violation.

#### 3.2 Detection

An extremely critical situation occurs when detection of a system is compromised. Detection is a process of continuous scrutinizing of data to find any suspicious activity and raise the alarm so that the administrator could check the alert and mitigation actions could be taken accordingly. A defense in layers strategy should be implemented as there is no evidence that particular security is enough [27]. If we implement the defence in layers, even if one of them is failed the rest would be there to protect the system.
3.3 Prevention
It is always better to prevent than to pursue and prosecute. Prevention is a process of blocking or stopping any suspicious event from occurring. The drawback of a preventive system is the false positives could violate the integration of data. Preventive security measures comprise firewalls, gateways, and anti-virus. Following Security policies and installation and updating the software, anti-virus, and following preventive measures would lead to better protection of the system from cyber-attacks.

The detection techniques could not protect the remote workers of the organization, and the alerts were helpful. We need threat intelligence with deep learning as the attackers use better technology than the existing cyber protection. We will be discussing how to improve the existing techniques concerning malware attacks.

4. Results and Discussion
This paper survey has various aspects of prevention centric solution which are overpowering the detection centric solution. Automation plays a major role in security, so we have considered the three categories Artificial Intelligence, Deep Learning, and Machine Learning to understand better how these technologies are working. To understand the relativity and to help the evaluation, we have identified the eight metrics:

- Interpretability: The ease of understanding how a particular solution was achieved through the Algorithm.
- Faster detection of data packets: The algorithm's speed can detect the data and send the response.
- Feature Hierarchy: Gaining the maximum insights from a hierarchy of a particular feature.
- Hardware Dependency: For the execution of an algorithm, high-end hardware is required.
- The focus of accuracy: The objective of the Algorithm is to gain the maximum accuracy.
- The efficiency with fewer amounts of data: Algorithm which provides high efficiency with fewer amounts of data.
- Correlations between discrete occurrences: Algorithm to provide a better correlation between distinct instances.
- Maximum Execution Time: The Execution Time is maximum with the particular Algorithm.

Table 5 shows the Relativity Matrix for three Automation Technology

| Evaluation Metric                        | Artificial Intelligence | Machine Learning | Deep Learning |
|------------------------------------------|-------------------------|------------------|--------------|
| Interpretability                         | ×                       | ✔                | ×            |
| Faster detection of data packets         | ✔                       | ✔                | ✔            |
| Feature Hierarchy                        | ×                       | ×                | ✓            |
| Hardware Dependency (e.g., GPUs)         | ×                       | ×                | ✔            |
| Focus of Accuracy                        | ×                       | ✔                | ×            |
| The efficiency with fewer amount data    | ×                       | ✔                | ×            |
| Correlations between discrete occurrences| ✔                       | ×                | ×            |
| Maximum Execution Time                   | ×                       | ×                | ✔            |

Artificial Intelligence can automate all the tasks assigned, and it is not mandatory to add machine learning to Artificial Intelligence; it can still automate the task with training. The automated Algorithm can work efficiently with training, such as already discussed above. The correlations between discrete occurrences are highest in Artificial Intelligence. Data packets' detection is faster in AI than others,
which helps the prevention-centric techniques analyze and prevent the data packets, which correlate with malware data.

A strong ML classifier will optimize recall and precision. The trade-off might be present in those metrics. The price of misclassifications or wrong decisions should also be considered to finalize which metric should be given priority or more importance; depending on the context of a specific application and the commercial and/or organizational objectives, the decision is made. Recall and precision are standard metrics for evaluating classification algorithms, and it is more complicated to evaluate clustering algorithms. For further classification, the clusters have to be evaluated before giving the labeling and evaluation. A clustering algorithm can always produce a data set division with its structure in the data. Various approaches may result in different clusters, and even different parameters or input patterns of different order may alter the final results for the same algorithm.

In Deep Learning neural network is used mostly to detect anomalies and training of the past relevant data to learn the prevention techniques in a better way. The more technology is growing, the more attacks occur, so prevention-centric is being opted rather than detection, so the technology's improvement will also occur. It takes a huge amount of time to process the data as the feature hierarchy is performed, and that requires high dependency on hardware such as GPUs and TPUs and the execution time is huge for the deep learning algorithm, which can be implemented to identify new threats and help in the study to move from detection centric to prevention centric security.

5. Discussion
Cyber threats continue to spread due to its lucrative business. With the increase in digital technology in the financial sector, the Internet of Things (IoT) and internet users have created more vulnerability to cybercriminals, requiring advanced security systems for detection and tracking systems and prevention to obstruct cybercriminals. The more the world moves towards automation, the better the security should be. The traditional Intrusion Detection Model and Prevention Model can no longer be used for a critical organization database. We need to automate the security to eliminate human errors and inculcate the current technology in our protection models. To achieve a better prevention model for cybersecurity, a design that is an amalgamation of the machine learning algorithm with the traditional methods of detection and prevention would be recommended. Even though we have a list of known threats in network security, Ransomware, and fog computing still with the rapid evolution of technology and enhancement in the existing features would lead to more attacks that are not only static but dynamic also.

6. Conclusion
In this paper, cautious evaluation is presented about how Automation algorithms would help predict, prevent, and keep the data protected from various attacks. With the changing nature of the danger and sophisticated evasive strategies proliferating, it is crucial to provide a methodology that can learn several levels of representations corresponding to various levels of abstractions. These levels form a cascade of concepts. Hidden layers can serve as inputs to the next layer with these concepts, and in method, creation of feature representations in internal layers to arrive at accurate or near accurate performance to detect and predict multi-stage cyber attacks. The focus of accuracy is most in Machine Learning, and the algorithms provide better efficiency with less amount training and testing data, which could lead to better algorithms for the prevention centric techniques, which concludes that the learning for prevention of attacks can be efficient if insights are gained from previous experiences and few other research studies which would help to protect the data in real-time.

References
[1]. Ponshanmugakumar, A., and R. Rajavel. "Design and Analysis of Steam Turbine Blade."
[2]. Rohit, Bhavani, and J. Rengamani. "Household Purposes in a Single Touch via Bluetooth Using Smartphones." Indonesian Journal of Electrical Engineering and Computer Science 9, no. 2 (2018): 351-353.

[3]. Augustus-Daddie, Joel, and Seth Accra Jaja. "Talent Management and Corporate Survival of the Nigerian Banking Industry."

[4]. Wambugu, Hannah, and Raymond Musyoka. "Consumer Behaviour in Regard to Recycling of Green Secondary Packaging in Kenya."

[5]. NO, Emma Collins. "IMPACT OF FOREIGN DIRECT INVESTMENT (FDI) ON THE GROWTH OF TELECOMMUNICATION SECTOR IN NIGERIA: 1980-2014." International Journal of Management Science Research 2, no. 1 (2016): 98.

[6]. Wong, Zoie & Zhou, Jiaqi & Zhang, Qingpeng. (2018). Artificial Intelligence for infectious disease Big Data Analytics. Infection, Disease & Health. 24. 10.1016/j.idh.2018.10.002.

[7]. Teryima, Sev Joseph, Emakwu John, and Dewua Philip. "Strategy Formulation as an Imperative for Accomplishment of Company’s Mission and Goals’ Attainment in Profit Oriented Organizations: A Survey of Nigeria Breweries Plc and Flour Mills of Nigeria Plc, Lagos."

[8]. Atakpa, Ime Willie. "Motivation and Organizational Citizenship Behaviour of Academics in Universities in Akwa Ibom State, Nigeria."

[9]. Diaz Rozo, Javier & Bielza, Concha & Larranaga, Pedro. (2017). Machine learning-based CPS for clustering high throughput machining cycle conditions. North American Manufacturing Research Conference NAMRC 45.

[10]. Fatehi, Kamal, and Douglas R. Moodie. "A More Relevant Nomenclature: Supply Network Management."

[11]. Onuoha, Onuoha A., and Chinedu N. Ogbuji. "Appraisal of the Performance of Palm Produce Marketers in Nigeria: Implications of the Abolition of Palm Produce Marketing Board." International Journal of Managerial Studies and Research 3, no. 11 (2015): 1-7.

[12]. Azab, Ahmad & Alazab, Mamoun & Alais, Mahdi. (2016). Machine Learning Based Botnet Identification Traffic. 1788-1794. doi: 10.1109/TrustCom.2016.0275.

[13]. G. Bucevschi, G. Balan and D. B. Prelipcean. (2019). Preventing File-Less Attacks with Machine Learning Techniques.21st International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC) pp. 248-252, doi: 10.1109/SYNASC49474.2019.00042.

[14]. Yang, Chunlei, and Ting Yang. "Study on Operation Mode of China’s Stadiums."

[15]. Venkadesh, Mr PR, MBA BE, and R. Ganapathi. "General Public’s Awareness, Attitude towards Carbon Trading and their Perception about Impact of Carbon Trading on the Environment." Carbon 3 (2015): 0-74.

[16]. Ravichandran, S. "Internet connected high tech street lighting system using RTOS." Int J MC Square Sci Res 9, no. 1 (2017): 331-334.

[17]. Hai, Khuong Thi Thu. "Influenced Factors on Employees’ Attitudes toward Organizational Change at Vietnam-Hungary Industrial University."

[18]. G. Xu, C. Qi, H. Yu, S. Xu, C. Zhao and J. Yuan. (2019). Detecting Sensitive Information of Unstructured Text Using Convolutional Neural Network. International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC) pp. 474-479, doi: 10.1109/CyberC.2019.00087.

[19]. Anyim, F. C., U. U. Ikeije, and J. O. Ekwoaba. "Union Membership: Organizing Workers in the Shop and Distributive Industry in Nigeria." (2014).

[20]. Sayyad, Nermeen. "Importance of Social Media in Business Firm in Palestine & its Effects." (2018).

[21]. Sarker, I.H.; Abushark, Y.B.; Alsolami, F.; Khan. (2020). A.I. IntruDTree: A Machine Learning Based Cyber Security Intrusion Detection Model. Symmetry, 12, 754.
[22]. Yandari, Aprilya Dwi, and Erina Sudaryati. "The Effect of Procyclinical on Income Smoothing with Financial Leverage as Moderation Variables in Banking Companies." International Journal of Managerial Studies and Research (IJMSR) 6, no. 11 (2018): 64-68.

[23]. Z. Li, H. Zhao, J. Shi, Y. Huang and J. Xiong. (2019). An Intelligent Fuzzing Data Generation Method Based on Deep Adversarial Learning. IEEE Access, vol. 7, (pp. 49327-49340). doi: 10.1109/ACCESS.2019.2911121.

[24]. Wang, Xifeng & Zhang, Xiaoluan. (2019). Wireless Network Attack Defense Algorithm Using Deep Neural Network in Internet of Things Environment. International Journal of Wireless Information Networks. 26. 10.1007/s10776-019-00430-1.

[25]. Elmasry, Wisam & Akbulut, Akhan & Zaim, Abdul. (2019). Evolving deep learning architectures for network intrusion detection using a double PSO metaheuristic. Computer Networks. 168. 10.1016/j.comnet.2019.107042.

[26]. Krishnaveni, P., Sutha, J. (2020). Novel deep learning framework for broadcasting abnormal events obtained from surveillance applications. J Ambient Intell Human Comput.

[27]. Feng, Fang & Liu, Xin & Yong, Binbin & Zhou, Rui & Zhou, Qingguo. (2018). Anomaly detection in ad-hoc networks based on deep learning model: A plug and play device. Ad Hoc Networks. 84. 10.1016/j.adhoc.2018.09.014.