ICIC Express Letters
Part B: Applications
Volume **11**, Number **12**, December **2020**

ICIC International ©2020 ISSN 2185-2766
pp. **1115–1123**

CYBERSECURITY BECOMES SMART USING ARTIFICIAL INTELLIGENT AND MACHINE LEARNING APPROACHES: AN OVERVIEW

Siham Hamadah and Darah Aqel

Faculty of Science and Information Technology
Al-Zaytoonah University of Jordan
Airport Road, P.O.Box 130, Amman 11733, Jordan
{ siham; D.aqel }@zuj.edu.jo

Received March 2020; accepted June 2020

Abstract. *With the rapid increasing of technology devices and the development of Internet, cyber-attacks are changing quickly and more and more attackers appear which lead more difficult threats in cybersecurity. Moreover, the world is facing Internet of Things devices which generate large volumes of data that cause a lot of new cyber threats. Cybercrimes cost a lot and make companies lose millions of dollars every year. Cybersecurity is a top concern at many companies. So, we need smart approaches to protect data against different threats which are difficult to know. Recently, researchers are developing systems based on Artificial Intelligence (AI) and machine learning to create defense approaches and protect data with high level of security and less cost. AI can help companies to identify threats automatically and find links between potential risks fast. This form of identification eliminates human errors from the process. This paper discusses AI-based cybersecurity various models that focus on machine learning and deep leaning algorithms. The results of this study show that machine learning and deep learning that simulate the human mind are more effective approaches than the traditional ones to solve security problems.*

Keywords: Cybersecurity, Artificial intelligence, Machine learning, Deep learning, Cyber-attacks

1. **Introduction.** In recent years, which are Internet-based era, technology and its applications are facing new generation of cyber threats. The devices that are connected to Internet and the connection among them need to be protected using strong security systems. Also, different unseen network attacks need to be identified. Some of the common cyber-attacks are phishing, Denial of Service attack (DoS), malware, hacking, spamming, and social engineering. Threats should be assessed by understanding potential bad actors, what they are trying to do, and why. The limitations of the existing systems make job of attackers and intruders easy to enter any systems through hidden doors. Cybercrime can potentially seriously disrupt and damage the business of any organization. Cybersecurity is considered one of the main solutions that address all of these threats and attacks. It is based on a set of processes and technologies that helps protect organizations' data assets or individuals' data from cyber-attacks and unauthorized access. In general, cybersecurity systems analyze the generated data carefully in real time, either this data is multimedia or non-multimedia [1,2].

Recently, many researchers have begun to use Machine Learning (ML), deep learning, and data mining algorithms in the cybersecurity domain to solve all of the cyber-attacks. ML and deep learning are branches of AI that can simulate human thinking and are similar to human intelligence. ML focuses on computational statistics and predictions, and gives computers the ability to learn from data and improve with experience and with

DOI: 10.24507/icicelb.11.12.1115

time. Deep learning, a new field of ML, mimics human brain to interpret images, sounds, and texts. It is based on layer-by-layer training algorithms [3,4].

In general, ML and deep learning methods have proved their efficiency in many different domains such as cybersecurity [6,10,13], natural language processing [22-24] and agriculture [25]. ML, data mining, and deep learning algorithms are applied widely in cybersecurity issues. Some studies focus on traditional ML techniques for cybersecurity, while others focus on data mining and deep learning algorithms. All of algorithms are fields of AI and are overlapped as shown in Figure 1. These algorithms are divided into three categories, supervised, unsupervised, and deep learning. Moreover, all of them have three phases: training, validation, and testing, and they mimic human brain. Also, datasets used for training and testing the algorithms play an important role in representation of the ML algorithms and should be analyzed carefully. The correct choice of dataset and the size of it are also important for relevant security research and affect the training and testing of the systems. Some datasets were designed long time ago and may not contain any information about current cyber-attacks [1,3].

FIGURE 1. AI approaches used for cybersecurity

Our article gives a comprehensive study on using different ML algorithms for building strong cybersecurity systems. This study is organized as follows. Cybersecurity is discussed in Section 2. Literature review is presented in detail in Section 3, embedded with comparative table. Section 4 discusses the main findings of our study. Section 5 provides a conclusion of our study.

2. **Cybersecurity.** Cybersecurity is the protection of digital devices and their communication channels (hardware, software, and data) to keep them stable, dependable, and free from danger, threats, and malicious attacks. It is also known as information technology security or electronic information security. Cybersecurity focuses on protecting computer systems from unauthorized access and alteration damage in cyberspace or in the Internet. Cybersecurity systems consist of computer (host) security systems and network security systems. Those systems have antiviruses, firewall, and Intrusion Detection Systems (IDSs). Cybersecurity researchers and designers aim to maintain data and provide the confidentiality, integrity, and availability of information [3,11,17].

The awareness of the current networks or host security system activities are very important in the area of cybersecurity to detect and respond to cyber threats. There are three methods of cyber intrusion detection. The first method is misuse-based detection, also called signature-based detection, the second one is anomaly-based detection, while the last one is hybrid detection. Basically, it was developed to improve the performance of intrusion detection, increase the detection rate of known attacks, and reduce the false positive rate for unknown attack [15].

The main threats that face cybersecurity are as follows [16]:

- **Cybercrime** (computer crime), which is based on an attack on information about individuals, corporations, or governments. Cybercrime includes single actors or groups targeting systems for financial gain or unauthorized access gain.
- **Cyberwar**, which is politically motivated and often involves information gathering or use of technology to attack a nation and create damage.
- **Cyber-terror**, which is based on using the Internet to conduct violent acts that are intended to weaken the electronic systems and cause panic or fear to achieve political gain.

Cybersecurity systems have been applied in different domains. For instance, they appear in safety-critical systems such as medical devices, banking, and automotive industries. There is a growing range of cyber-threats to cybersecurity of safety-critical systems. Cybersecurity goals of critical systems are the highest levels of cybersecurity requirements and determined based on the results of threat analysis and risk assessment, as well as what to be avoided. Therefore, the human behavior is the most important aspect to ensure cybersecurity of safety-critical systems [5]. In above of that, cybersecurity is also important to protect data in the big data area. The detection of cybersecurity threats in big data technology is necessary, where there are a lot of users and transactions on cyber space. The researchers contributed in this area by building strong and smart models to creating a security detection system in big data to discover threats. In [12], the authors construct a collaborative detection system of cybersecurity in big data by designing a new model that consists of Apache Flume system, Kafka system, and Esper engine. The results of constructing the new model described that the model was high efficient, reliable, accurate, and low cost. Also, cybersecurity systems appear in cloud computing for disaster recovery to ensure business continuity. The cloud-based disaster recovery enables backup and recovery of remote machine. The clouds can be private, public, community or hybrid. [20,21].

3. **Literature Review.** With the growing usage of technologies and the advancements in the fields of smart devices and networks, security is sure to be a key risk factor that faces different challenges. These challenges may lead to new types of network security problems that threaten our lives. Therefore, we need a strong cybersecurity system to protect information and devices. Using ML algorithms in cybersecurity is a smart choice to build strong security system. Several studies have applied AI and ML algorithms in cybersecurity for protecting data. For example, the authors in [10] used machine and deep learning algorithms to address three cybersecurity problems: intrusion detection, malware analysis, and spam and phishing detection. They first discussed the use of ML techniques to highlight the pros and cons of those techniques in cybersecurity. In their study, they have used the Domain Generation Algorithms (DGA), network intrusion detection, and two ML algorithms: Random Forest (shallow learning) and Feedforward Fully Connected Deep Neural Network on labelled training datasets. The results showed that the Random Forest algorithm is better than the Feedforward Fully Connected Deep Neural Network algorithm in cybersecurity, although the deep learning algorithms are known to be the best in many other fields. They concluded that ML algorithms provide superior performance for specific threats not for general threats. Their experimental results also showed that the detection rate of adversarial attacks is low, and all approaches need retraining, such that there are different results achieved by the same ML algorithms in different environments.

In [18], the authors concentrated on different application of ML for cyber analytics for discovering intrusion and email filtering. They also discussed different ML algorithms in cybersecurity in three main domains: Instruction Detection Systems (IDS), anomaly detection module, and misuse detection. A set of recommendations was proposed, for example, the clustering algorithms perform the best results for anomaly detection.

Chromosomes of genetic algorithms and branch feature of decision trees achieve the best results for misuse detection. In their article, four different ML algorithms are applied to classifying different attacks using MODBUS data from gas pipeline. The four algorithms are: Naïve Bayes, Random Forest, OneR, and J48. The authors compared the efficiency of those algorithms on a dataset of ICS network with more than 35 attacks. The authors performed a pre-processing for the dataset using Weka tool. The experiments showed that J48 was the best algorithm and achieved the most optimized results in all classifications to detect cyber-attacks. J48 has achieved an accuracy of 0.992. The results also showed the Random Forest algorithm was the second algorithm that gave a good result and achieved an accuracy of 0.988. However, this study also showed that more analysis needs to be performed to determine the performance of the algorithms because the performance of algorithms depends upon the applied dataset.

In [6], the authors proposed a deep learning technique to detect malware relying on malicious behavior. They used process name, process path, and runtime duration to identify the malicious behaviors because attackers want to hide their existence. The authors combined Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN) which includes a Long Short-Term Memory (LSTM) architecture to build an automated system. This system has the ability to determine if a sample is malicious or not. They used a training dataset which is made by the normal log event to test model. They also used a distributed analysis system to run the analysis simultaneously especially for a large number of samples. The proposed system performed very well in training and validation, where it achieved a high accuracy rate of 0.9875 to detect malware. Moreover, the authors tried another improvement to their system by using Gated Recurrent Units (GRU) instead of LSTM which achieved a better performance and accuracy that reached to 1.0. However, this study also showed that the model achieved high accuracy while having poor prediction, so it cannot be used in practical application.

In [13], the author analyzes Distributed Denial of Service (DDoS) attacks using two supervised ML algorithms, Long Short Term Memory Recurrent Neural Network (LSTM RNN) and Basic Neural Network (BNN). The author applied three different scenarios for the experiments using CAIDA dataset, DARPA dataset, and recent datasets. The study considered different environments with different hyperparamter values to examine the effects of learning former traffic on sequential traffic. Furthermore, the study focused on how different preprocessing methods and different values of hyperparameter affect the performance of ML techniques. Two optimizers were compared to detect DDoS attacks using TensorFlow. The results showed that LSTM RNN was better in some measures than BNN, but it needs a longer time than BNN for attack detection. Furthermore, the accuracy of BNN and LSTM reached to 1 for CAIDA and DARPA datasets, and achieved 0.90 for the other dataset. DDoS can be detected fast with high accuracy when learning algorithms and rate are selected suitably. The results also showed that DDoS attacks detection was better when using neural network, preprocessing methods, hyperparameter, and optimizers.

In [19], the author developed a model of keyed learning, which is an ML with a secret key. This key is used as an additional input to an adversarial learning system. The goal of this key is to prevent an adversary from simulating the learning process and finding a learned classifier. The key has two components: a data selection key to select some available examples and a learning key to prevent adversary from predicting the output. The developed model is specialized in an implementation-oriented framework, which is suitable for anomaly detection applications. Also, this model includes: network intrusion detection, attack, malware analysis, and user authentication. The framework can affect any form of learning and use any kind of secret information. Moreover, it is integrated with SIEM software to generate alarms to avoid adversarial actions. The author defined three adversarial models and explained how the information was used: Passive Observer,

Active Data Selector, and Active Data Modifier. However, this study also showed that the random choice of key may be to be a bad choice and will influence the learning. Also sometimes keyed learning does not work. Moreover, keyed learning in some cases will prevent a simulation of learning phase by the adversary.

In [7], the authors explained the security incidents and malwares that attack mobile devices and gather private information about users. So, this article proposed an ML technique to detect application layer cyber-attacks using a graph-based segmentation technique and dynamic programing. Also, it consists of patterns in form of Peral Compatibale Regular Expressions (PCRE). The proposed technique built a set of expressions for HTTP requests which are sent by client to the web application. It also examined many kinds of log files and textual data. This technique used Needleman-Wunsch algorithm to estimate the dissimilarities between two components. The CSIC'10 dataset was used for experimentations, since it has thousands of HTTP protocol requests dump. After the authors compared two approaches in their experiments, the proposed model showed that it was achieved better results for detection ratio of cyber-attacks with a lower number of false positives, especially when the learning was performed separately for each URL. The proposed method has achieved detection rate of 94.46%. However, this study also showed that the proposed approach operates poorly when it generalizes the whole traffic using the single model.

In [9], the authors proposed a new Dark Web (DW) attack detection and prediction. In general, the resources of DW are not always visible to search engines, since they need some technical challenges. The Dark Web or "Hidden" Web was called for many reasons such as the threats that face Web. Therefore, the authors applied in their study AI techniques, which analyze big data, to identifying DW attack groups and tracing their actions. Some of the attacks have exposed a large e-Government data. The proposed model is based on attack detection using the prediction of adversarial behavior in cyber clusters. They presented P2P forecasting model that divided cyber space into clusters according to set of parameters. Then, they formalized factors about adversarial behavior, where these factors can predict affiliations and activities between adversarial groups and possible attacks. This model is more accurate in predicting P2P attacks. However, this study does not attempt to differentiate between different types of P2P communicative acts within or across shared DW Communities.

In [14], the authors experimented various deep learning architectures such as Recurrent Neural Network (RNN), Long Short-Term Memory (LSTM), Identity-Recurrent Neural Network (IRNN), Convolution Neural Network (CNN), and CNN-LSTM. These architectures were used to identify the nature of website as either benign or malicious URL's. Feature engineering in ML models is able to generalize well for unknown malicious URL. Phishing and malware are two types of malicious that the authors tested for two datasets. They explained the experiments for a dataset 1 (URL from Alexa and DMOZ directory and malicious URL's from MalwareURL, MalwareDomains, and MalwareDaominList.) and a dataset 2 (URL from Alexa and DMOZ directory, Phishing from Phishtank and OpenPhish) and a merging from these two datasets. As a result, the LSTM model and hybrid CNN with LSTM have attained the highest accuracy and performed well in detecting and classifying the URL either benign or malicious. The model has achieved an accuracy of 0.9996. However, this study clarified the characteristics of malicious threats are growing in nature. At the same time the URL's also change across time. So a large study should be done. Also, in real-time scenario, getting an acceptable labeled training data is often considered as a difficult task.

In [8], the authors introduced a strong algorithm for encryption, decryption, and generation of a strong key. They applied DNA Deep Learning Cryptography to transmitting and protecting a message among sender and receiver safely. They also proposed a genetic algorithm with Neddlemen-Wunsch (NW) algorithm to generate a unique key. Plain text

was encoded into long sequences of DNA nucleotide bases and then encrypted. In addition, a random number of key generators were used to generate an initial population of chromosomes, and a fitness function was also used to calculate the randomness of chromosomes. There are a number of sequences of data that is based on a number of runs. NW algorithm was adopted to compare the similarity of sequences for non-repeating. The proposed algorithm adds another security layer and reduces the complexity of mathematical equations, as well as it protects data from hackers. However, this research also showed that there is still a lot needed to be done with regards to the cost and time effectiveness. The research study is done conceptually; it requires actually implement.

All of the above mentioned studies, which applied ML algorithms in the cybersecurity domain, are summarized in Table 1. Table 1 also shows the advantages and the disadvantages of using ML and deep learning in cybersecurity.

TABLE 1. A summary of some studies that applied ML in cybersecurity

Author	Usage	Algorithms and their classification	Results	Advantages and disadvantages
[10] 2018	Addressing three cybersecurity problems: intrusion detection, malware analysis, and spam and phishing detection	1- Random Forest. (ML) 2- Feedforward Fully Connected Deep Neural Network. (deep learning)	- The Random Forest algorithm is better than the Feedforward Fully Connected Deep Neural Network algorithm in cybersecurity. - The ML algorithms provide superior performance for specific threats not for general threats.	**Advantage** - provide better performance for specific threats. **Disadvantages** - the detection rate of adversarial attacks is low. - different results are achieved by the same ML algorithms in different environments, so retraining is needed.
[18] 2017	Cyber analytics for discovering intrusion and email filtering.	1- OneR. (ML) 2- Naïve Bayes. (ML classification) 3- Random Forest. 4- J48. (ML classification)	J48 was the best algorithm and achieved the most optimized results in all classifications to detect cyberattacks.	**Advantage** - detect many different cyberattacks. **Disadvantage** - more analysis needs to be performed to determine the performance of the algorithms.
[6] 2018	Detecting malware relying on malicious behavior.	Deep Learning System using CNN and RNN which includes LSTM or GRU. (deep learning)	The proposed system has low overhead and high accuracy to detect malware that reached to 1.	**Advantages** - ability to determine if a sample is malicious or not. - ability to detect malware. **Disadvantage** - model has poor prediction, so it cannot be used in practical application.
[13] 2019	Analyzing Distributed Denial of Service (DDoS) attacks.	1- Long Short Term Memory Recurrent Neural Network (LSTM RNN). (deep learning) 2- Basic Neural Network (BNN). (deep learning)	- LSTM RNN was better in some measures than BNN, but it needs longer time than BNN for attack detection. - DDoS can be detected fast with high accuracy when learning algorithms and rate are selected suitably.	**Advantages** - DDoS can be detected fast using neural network. - abnormal behavior and several types of attacks can be detected. **Disadvantage** - some algorithms need longer time for detection.

(continued)

[19] 2019	Adversarial learning system for network intrusion detection, attack, malware analysis, and user authentication	Model of keyed learning which is an ML with an secret key. (ML)	- This model is suitable for anomaly detection applications. - It includes: network intrusion detection, attack, malware analysis, and user authentication. - It can generate alarms to avoid adversarial actions.	**Advantages** - it can detect attack and malware. - generate alarms to avoid adversarial actions. **Disadvantages** - random choice of key may be to be a bad choice. - sometimes keyed learning does not work. - keyed learning in some cases will prevent a simulation of learning phase by the adversary.
[7] 2015	Detecting application layer cyber-attacks	1- Algorithim for graph segmentation. 2- Dynamic programming 3- Needleman-Wunsch (ML)	- The proposed model showed that it achieved better results for detection ratio of cyber-attacks with a lower number of false positive.	**Advantage** - it can detect cyber-attacks. **Disadvantage** - the proposed approach operates poorly when it generalizes the whole traffic.
[9] 2014	Attack detection and prediction in Dark Web that includes a cyber-warfare among terrorist groups, organized crime, extremists, and civil society	- AI techniques, which analyze big data. - Attack detection using the prediction of adversarial behavior in cyber clusters.	- The model can predict affiliations and activities between adversarial groups and possible attacks. - It is more accurate in predicting P2P attacks.	**Advantage** - it can predict adversarial groups and attacks. **Disadvantage** - it does not differentiate between different types of P2P.
[14] 2018	Identifying the nature of website as either benign or malicious URL's	Deep learning approaches. RNN, LSTM GRU, CNN, I-RNN, and CNN-LSTM for text encoding. (deep learning)	The LSTM model and hybrid CNN with LSTM have attained the highest accuracy and performed well in detecting and classifying the URL either benign or malicious.	**Advantage** - it can classify the website either benign or malicious. **Disadvantages** - characteristics of malicious threats are growing in nature, and the URL's also change across time. - it is hard to get a suitable labeled training data.
[8] 2017	Encryption, decryption, and generation of a strong key to protect a message among sender and receiver safely	1- DNA Deep Learning Cryptography for encryption and decryption. 2- Genetic Algorithm with NW to generate a key. (ML)	- The proposed algorithm adds another security layer and reduces the complexity of mathematical equations. - It protects data from hackers.	**Advantage** - it can protect data, and adds another security layer. **Disadvantages** - it does not contain the cost and time effectiveness. - it requires implement.

4. **Discussion and Results.** The conducted review made in this comprehensive study has shown the significance of applying ML methods in the cybersecurity domain, since these methods are suitable and effective to detect cyber-attacks and threads. Furthermore, it has been noticed that deep learning methods also play a vital role in detecting

the other types of threats especially if there is a large volume of data. In general, ML methods have proven their efficiency in classifying the malicious threats, adding security layers, protecting data from hackers, and limiting the attacks that gather private information about users. The study has also demonstrated that some ML methods can predict activities between adversarial groups, detect possible attacks, and generate alarms to avoid adversarial actions. However, the current cybersecurity systems, which are based on ML, may suffer from some shortcomings that may reduce their efficiency for cybersecurity and decrease the level of detecting and identifying different cyber threats. As a result, more studies must be conducted based on AI and ML methods to build the most effective systems for cybersecurity. Moreover, smart approaches can be applied in cloud to taking all advantages of cloud services. Improvements in AI, however, have led to the creation of much smarter security systems. By applying machine learning, many of these systems can learn from themselves without the need for human involvement.

5. **Conclusions.** This paper provided an inclusive literature review of different AI algorithms and models that have been applied for cybersecurity. Some of them focus on using ML, while others use deep learning. Datasets are also very important for training, validation, and testing the algorithms. Machine and deep learning methods played an important role in cybersecurity and intrusion detection, but unfortunately, the most effective methods have not been developed yet. Hence, this area of research is very rich to find new and effective models for cybersecurity and has a lot of challenges for big data. Anyway, ML, deep learning, and data mining techniques have proven that they can support security activities and achieve effective results for cybersecurity, as well as they are all useful in intrusion detection. We encourage researchers of this field to focus more on enhancing the current and existing ML and deep models used for cybersecurity. Moreover, the directions of future works for these researchers should be based on improving the performance of these models by carrying out more experiments and increasing the size of the used datasets or using different datasets. Thus, researchers in the cybersecurity domain should pay attention to all of these ideas in order to resolve many issues and increase the accuracy results of the used ML models as well as build more effective ML systems for cybersecurity and intrusion detection.

Acknowledgment. We would like to express our special thanks to Al Zaytoonah University of Jordan for the effort that it provides to us for supporting this research paper.

REFERENCES

[1] M. Usman, M. A. Jan, X. He and J. Chen, A survey on representation learning efforts in cybersecurity domain, *ACM Computing Surveys*, vol.52, no.6, 2019.

[2] P. W. Singer and A. Friedman, *Cybersecurity and Cyberwar What Everyone Needs to Know*, Oxford University Press, New York, USA, 2014.

[3] Y. Xin, L. Kong, Z, Liu, Y. Chen, H. Zhu, M. Gao and C. Wang, Machine learning and deep learning methods for cybersecurity, *IEEE Access*, vol.6, pp.35365-35381, 2018.

[4] J. Bell, *Machine Learning Hands-on for Developers and Technical Professional*, Wiley&Sons, Inc., Canada, 2015.

[5] A. Walker, Cybersecurity in safety-critical systems, *Journal of Software: Evolution & Process*, vol.30, no.5, 2018.

[6] Q. T. Hai and S. O. Hwang, An efficient classification of malware behavior using deep neural network, *Journal of Intelligent & Fuzzy Systems*, vol.35, no.6, pp.5801-5814, 2018.

[7] M. Choras and R. Kozik, Machine learning techniques applied to detect cyber-attacks on web applications, *Logic Journal of the IGPL*, vol.23, no.1 pp.45-56, 2015.

[8] S. Kalsi, H. Kaur and V. Chang, DNA cryptography and deep learning using genetic algorithm with NW algorithm for key generation, *Journal of Medical Systems*, vol.42, pp.1-12, 2017.

[9] G. Epiphaniou, T. French and C. Maple, The DarkWeb: Cyber-security intelligence gathering opportunities, risks and rewards, *Journal of Computing & Information Technology*, vol.22, pp.21-30, 2014.

[10] G. Apruzzese, M. Colajanni, L. Ferretti, A. Guido and M. Marchetti, On the effectiveness of machine and deep learning for cyber security, *The 10th International Conference on Cyber Conflict*, NATO CCD COE, Tallinn, pp.371-389, 2018.

[11] A. L. Buczak and E. Guven, A survey of data mining and machine learning methods for cyber security intrusion detection, *IEEE Communications Surveys & Tutorials*, vol.18, no.2, pp.1153-1175, 2016.

[12] J. Zhang, Y. Guo and Y. Chen, Collaborative detection of cyber security threats in big data, *International Arab Journal of Information Technology (IAJIT)*, vol.16, no.2, pp.186-193, 2019.

[13] M. Kim, Supervised learning-based DDoS attacks detection: Tuning hyperparameters, *ETRI Journal*, vol.41, no.5, pp.560-573, 2019.

[14] R. Vinayakumar, K. P. Soman and P. Poornachandran, Evaluating deep learning approaches to characterize and classify malicious URL's, *Journal of Intelligent & Fuzzy Systems*, vol.34, no.3, pp.1333-1343, 2018.

[15] L. Wang and R. Jones, Big data analytics for network intrusion detection: A survey, *International Journal of Networks and Communications*, vol.7, no.1, pp.24-31, 2017.

[16] *What is Cyber-Security*, https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security, Accessed on Jan. 17, 2020.

[17] S. Dua and X. Du, *Data Mining and Machine Learning in Cybersecurity*, Taylor and Francis Group, LLC, USA, 2011.

[18] R. Das and Th. H. Morris, Machine learning and cyber security, *International Conference on Computer, Electrical & Communication Engineering (ICCECE)*, Techno India University, 2017.

[19] F. Bergadano, Keyed learning: An adversarial learning framework formalization, challenges, and anomaly detection applications, *ETRI Journal*, vol.41, no.5, pp.608-618, 2019.

[20] S. Hamadah and D. Aqel, A proposed virtual private cloud-based disaster recovery strategy, *2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT)*, Jordan, 2019.

[21] S. Hamadah, Cloud-based disaster recovery and planning models: An overview, *ICIC Express Letters*, vol.13, no.7, pp.593-599, 2019.

[22] M. Murata, K. Orikane and R. Akae, Automatic selection and analysis of verb and adjective synonyms from Japanese sentences using machine learning, *International Journal of Innovative Computing, Information and Control*, vol.15, no.6, pp.2135-2147, 2019.

[23] D. Aqel and B. Hawashin, Arabic relative clauses parsing based on inductive logic programming, *Recent Patents on Computer Science*, vol.11, no.2, pp.121-133, 2018.

[24] D. Aqel, S. AlZu'bi and S. Hamadah, Comparative study for recent technologies in Arabic language parsing, *The 6th International Conference on Software Defined Systems (SDS)*, Rome, Italy, pp.209-212, 2019.

[25] S. S. Chouhan, A. Kaul, U. P. Singh and S. Jain, Bacterial foraging optimization based radial basis function neural network (BRBFNN) for identification and classification of plant leaf diseases: An automatic approach towards plant pathology, *IEEE Access*, vol.6, pp.8852-8863, 2018.