# A TECHNICAL REVIEW ON DEEP LEARNING ALGORITHMS FOR CYBER ATTACKS DETECTION

**Dr.R.K.Dhuware[1], Ms.Rubina Kureshi[2]**

*1.Head, Department of Computer Science, Dhote Bandhu Science College, Gondia*

*2.Research Scholar,Department of Electronics and Computer Science,RTM Nagpur University,Nagpur*

*Abstract:With exponential rise in systems having Internet-connection, risk of attacks increasing day by day. Attackers deploy zero-day activities where attack takes places as soon as weakness in system is detected. although various existing cyber safety tools are still continuously active to classify safety breaches and stop attacks. Such attacks have no previous record and can damage the computer system before problem is solved. There are emerging trends of deep learning in information-security. Deep Learning techniques like Deep Belief Networks, Recurrent Neural Network and lots of additional may be applied to completely different information security areas to predict Cyber security attacks It discusses the challenges of cyber security for electronic devices and explains how deep learning can address these challenges. The paper also highlights some recent research efforts in this area and discusses their limitations. Finally, the paper concludes with some suggestions for future research in this area..*

*Keywords: Deep Learning techniques (DLT), Cyber security, Attacks Prediction*

## 1.INTRODUCTION:

In this era of IoT(internet of things),Cybersecurity is the whole suite of all methods and tools that accountable for shielding networks, software, and data from attacks [1, 2]. The mechanism of cyber protection is available at the network, data level, host and application. Selected cybersafety tools like firewalls, the system of intrusion detection, the system of intrusion protection etc., are continuously active at every end to classify safety breaches and stop attacks [3, 4]. However, with the growing number of systems having Internet-connection, the risk of attacks is increasing day by day. With the insight of Internet of things (IoT) networks, cybersecurity is becoming more essential than ever. Computer networks including IoT are susceptible to numerous security threats. Certain attacks are of known pattern can be easily managed. However, attackers deploying zero-day activities, where the attack takes places as soon as a weakness in the system is detected. Such an attack has no previous record and the attack can damage the computer system before the problem is solved. Furthermore, the system must be protected not only from outside threats but also need to be defend from insider threats, like abuse the authorized access, which can be an individual or mean to be a part of the organization.

The main challenge is to discover the compromising system's indicators from the attack's lifecycle, which may have meaningful signs of a forthcoming attack. However, this could be a difficult job because of enormous numbers of data-generating constantly from loads of cyber-enabled devices.

In order to improve cybersecurity, data science uses the vast array of data produced by the cyber defense system, including the security information and event management (SIEM) scheme. At times, this overloads the security specialist with event warnings, patterns, and related events, as well as the detection of abnormal behavior.

Hybrid detection in security amalgamates anomaly and misuse detection. The primary goals of this system are to improve the rate of recognized intrusion detection and reduce the false-positive value rate of anonymous attacks. Hybrid techniques are used in maximum DL approaches [5, 6].Prior reviews, such as those found in [7-9], have demonstrated how machine learning (ML) can be applied to solve cyber-related issues; however, those evaluations did not specifically address deep learning (DL) techniques. A few publications demonstrate deep learning techniques for cybersecurity. There are certain restrictions with these methods when it comes to cybersecurity applications [10, 11].

## 2. Related Work:

DL models have shown significant improvements over traditional ML-based solutions, signature-based methods and rule-based methods in order to address cyber security problems. From the review, it can be seen that most researchers have focused on malware classification and detection of various types of intrusion in the network. Cyber physical autonomous systems which is not only sensor-based but also communication-enabled (e.g., automotive systems), biometrics behavioral (i.e., signature dynamics) are considered as increasing areas for DL applications of security. *Podder,P ,Bharati S and Hossain R.M*[9] said for malware and intrusion detection, RBMs were the most often utilized DL technique. RNNs were another popular solution for tackling the largest range of cyber security challenges feasible (i.e., network intrusions, cyber-physical intrusions, malware, host intrusions and names of malicious domain). The large use of RBMs and autoencoders, around 50%, is most likely owing to a scarcity of labeled data, and unlabeled data is pre-trained and fine-tuned using a little quantity of labeled data. Since many cyber security tasks or data sets can be viewed as time series problems, RNNs are probably often used.[9].

Certain tendencies, however, are remarkable. Berman*, D.S.; Buczak, A.L.; Chavis, J.S.; Corbett, C.L*[13] said performance of various areas of the security business varied greatly. Domains constructed employing a variety of techniques seem to have the most consistent

DGA-produced hazardous domains. *Podder,P ,Bharati S and Hossain R.M*[9] said that with TPRs ranging from 1% to 1.5 % and accuracy values ranging from 0.9959 to 0.9969, equivalent to 96.01 to 99.86%. Network intrusion detection techniques, on the other hand, have a performance range of 92.33 to 100 percent with a TPR of 1.58 to 2.3 percent and an accuracy range of 44 to 99 percent. A high classification accuracy of 99.72% is reported for RBM when applied to a custom dataset , while accuracy of 99.80% is achieved by LSTM for KDD Cup 99 dataset . Historically, the capacity to detect network intrusions has significantly been reliant on the kind and quantity of attacks carried out. *Bharati, S.; Podder, P.; Mondal, M.; Robel, M. and Alam, R* [9] said that authentication systems are described by which vehicular networks can be protected from fake messages and malicious nodes. Different direct vehicle communication methods, such as on-board diagnostics and universal serial bus, and various remote vehicle communication methods, such as radio frequency identification, WiFi, WiMAX, Zigbee, Bluetooth, and cellular schemes, are discussed along with security threats and countermeasures.Another crucial component influencing overall performance was the training set's relationship between benign and dangerous data. This quandary stems from the difficulties of getting legally harmful materials. Because authentic data might be difficult to get, data is often generated using viral simulations and reverse engineering.

Virtualization plays a vital role in the construction of cloud computing. However, various vulnerabilities are existing in current virtualization implementations, and thus there are various security challenges at virtualization layer. In this paper, we investigate different vulnerabilities and attacks at virtualization layer of cloud computing. We examine the proposals of cloud intrusion detection system (IDS) and intrusion detection and prevention system frameworks. We recommend the cloud IDS requirements and research scope to achieve desired level of security at virtualization layer of cloud computing.

When employing DL-driven security technology, some difficulties may arise. *Podder,P ,Bharati S and Hossain R.M*[9] said that model's accuracy can be viewed as a significant impediment. The use of any new tool, especially DL tools, is universally frowned upon because they are ultimately black boxes. As a result, when errors occur, determining the cause is impossible, and unlike DL applications such as

the marketing sector, larger costs and hazards are associated with cybersecurity missteps. A cybersecurity analyst may waste time analyzing false alarms, or an automated response to intrusion detection may erroneously restrict access to critical services.

A cyberattack can also be totally disregarded by a DL tool.. Another barrier to adoption is that many of the currently available systems focus on a specific hazard, such as virus detection. Researchers should investigate methods for generalizing or combining multiple DL approaches in order to cover a broader range of attack vectors and provide a more comprehensive solution. Multiple DL detection techniques must be used concurrently, and information gathered by various techniques may also be used to improve local performance.

Cyber security has become an important issue for IoT since IoT can contribute to managing pandemics, particularly the novel coronavirus disease (COVID-19). One example of the use of IoT for COVID-19 is to mitigate the causative virus from being spreading. This can be done by the screening of temperature, tracing the contacts, and several other ways. Detecting early cases of the infection, tracing, and then isolating the suspected patients can be done with IoT. Note that IoT-driven healthcare systems and IoT-driven COVID-19 diagnosis systems are emerging techniques that can be useful to patients and doctors. Another example is facilitating the new lifestyle during COVID-19, including home-office, distant learning, fitness training at home, etc[9].

*Al-Garadi, M.A.; Mohamed, A.; Al-Ali, A.; Du, X.; Guizani,* [10] said that activities enable the running of businesses, educational institutions, government offices without risking the people's health. Another use case of IoT is to resolve machinery issues for controlling medical inventory, tracking tagged nebulizers, oxygen cylinders, and other medical equipment. For tackling a pandemic, IoT can be used along with other techniques such as near field communication, radio frequency identification, WiFi, light fidelity, sensor networks, etc.

These technologies require small portable devices that have low computation power and low battery life. As a result, ensuring cybersecurity for small IoT devices is a more challenging task compared to traditional computers, server, smartphones and laptops. Cyber attacks evolve rapidly, so it is difficult to incorporate security measures in IoT devices quickly. Unless the cyber attacks are mitigated, IoT cannot be effectively used in controlling pandemics. Security threats such as phishing, spamming, ransomware,

Distributed DoS may affect the reliability of IoT-driven healthcare and COVID-19 diagnosis systems. Hence, understanding the possible security threats and finding appropriate mitigation techniques is essential in the context of IoT and other networking scenarios.

## 3. DEEP LEARNING ALGORITHMS FOR CYBER ATTACK DETECTION

The Deep Learning architecture is of three types: unsupervised, hybrid and supervised as shown in the figure 1.

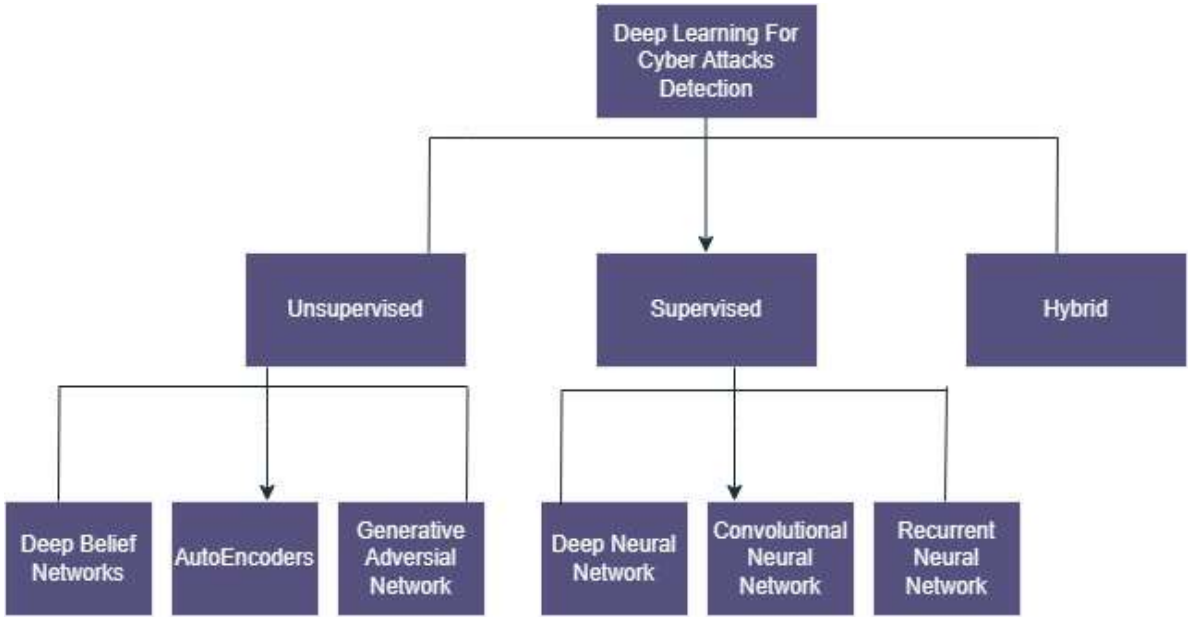


**Figure 1: Categorization of Current Deep Learning Algorithms for Cyber Attacks Detection**

To properly perceive the utilization of Deep Learning within these information security areas, it's necessary to grasp the threats and vulnerabilities that arise in the systems.

### 3.1. Deep Belief Networks

Deep Belief Networks (DBNs) is brought in a seminal paper by Geoffrey Hinton. Among Deep Neural Networks (DNNs) is a class called DBNs. The hidden casual variables that make up a DBN are layered. Furthermore, no links exist between any unit inside a layer, although connections do exist between the layers [12]. In conjunction with machine learning and neural networks, it combines probability and statistics.. Figure 2 shows different types of DBN.

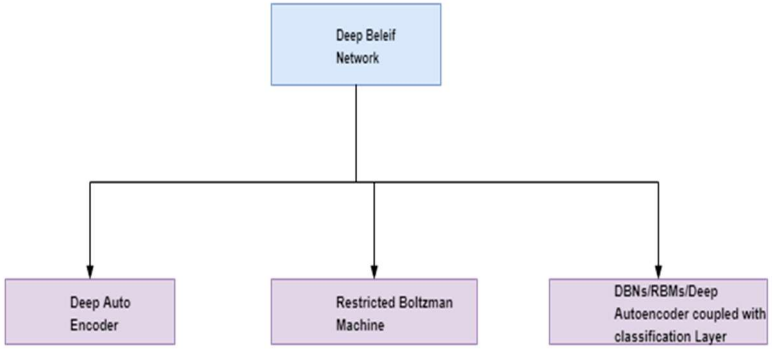


**Figure 2. Classification of DBN**

### 3.2. Auto encoder

An auto encoder using vector input is an example of an unsupervised technique. The network attempts to match the input vector and the output, which are identical.By obtaining the input and altering the dimensionality of the input throughout its recreation, one may produce an illustration of the data with a lower or higher dimensionality. The process of data encoding, also known as feature compression, is carried out in a network with a limited number of hidden layers. To remove the noise and recreate the original input from the noisy input, a denoising autoencoder might be a useful tool. Figure 2 shows an example of a simple auto encoder.

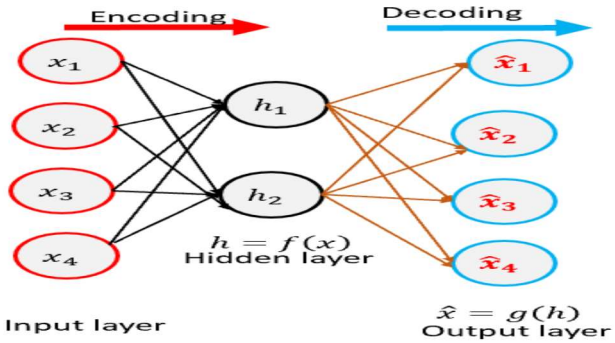


**Figure 3. Auto encoder**

### 3.3. Generative Adversarial Networks

GANs are used in unsupervised machine learning (ML), where two neural networks compete with one another in a zero-sum game to defeat the other. The introduction is provided by Goodfellow's work. The GAN's block diagram is displayed in Figure 4. Using input data, the generator generates output data with properties comparable to real-time data. Next, the discriminator examines the actual data to determine if the input is authentic or fraudulent.GAN systems have several uses, such as optical flow estimates, caption creation, picture enhancement, and DCGAN for Facebook.

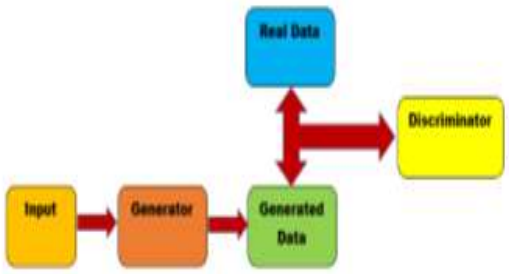


**Figure 4. Generative Adversarial Networks**

### 3.4. Deep Neural Network

In Figure 5, a deep neural network is shown. Between the input and output layers are several levels; the input layer is regarded as lower level and the output layer as higher level. Higher-level ideas are defined from the lower-level notions. Even if the few first layers of the DL network can be used for feature extraction.

Between the input and output layers of an ANN, a deep neural network (DNN) has several hidden layers. DNNs have the same ability to represent complicated non-linear interactions as shallow ANNs. Neural networks are primarily used to tackle real-world issues like categorization by taking a collection of inputs, processing them via more sophisticated computations, and producing an output. Our scope is limited to feed forward neural networks.In a deep network, we have a flow of sequential data, an input, and an output.

Artificial Intelligence (AI) has become more prevalent in our daily life with the introduction of deep neural networks (DNNs). These networks are used in self-driving cars, smartphones, games, drones, and other gadgets. Most of the time, DNNs were accelerated by servers equipped with multiple processing engines, including GPUs. However, as many modern applications now operate on mobile computing nodes, new technology advances have made it necessary to accelerate DNNs in an energy-efficient way. Neural Processing Unit (NPU) architectures were therefore necessary for energy-efficient DNN acceleration. Numerous research have shown that, even though the DNN training phase requires precise number representations, lower bit-precision is sufficient for inference with minimal power consumption.

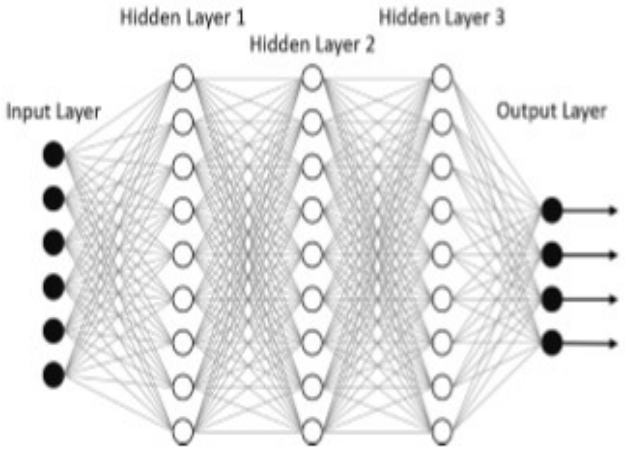


**Figure 5. Deep Neural Networks**

### 3.5. Convolutional Neural Network :

Part of the deep neural network (NN) that processes and analyzes visual imagery input is the convolutional neural network (CNN). An input picture, whether it be grayscale or colorful, will be saved as a 2D array of pixels. Moreover, audio spectrograms with 2D arrays are managed by CNNs use. Convolution, pooling, and classifying layers are the three types of layers included in the CNN model [15]. Figure 6 displays an example of CNN.

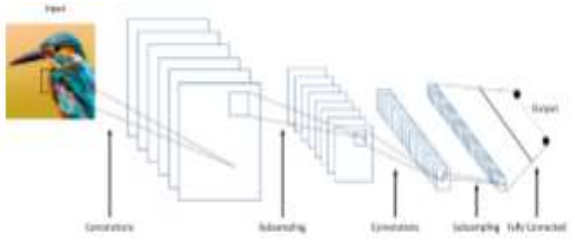

**Figure 6. Convolutional Neural Network**

### 3.6. Recurrent Neural Network

By forming loops in the network, they process arbitrary input sequences using their internal memory, allowing the signal to flow both forward and backward [13–15]. Because of the gradients' removal, training RNNs is usually more difficult. But numerous RNNs have been established via advancements in training and architecture.

As seen in Figure 3, a directed graph composed of nodes is a subset of neural networks called recurrent neural networks (RNNs). The network is now in its internal state as a result. It allows for the display of dynamic sequential behavior. They interpret random input sequences using their internal memory, and the signal flows both forward and backward through the network's creation of loops [13–15]. Because the gradients vanish, training RNNs is often more difficult. But different RNNs have been created thanks to advancements in training and design. Training this model is easier. In 1997, Hochreiter and Schmidhuber introduced the long short-term memory (LSTM), an enhanced RNN system [14].

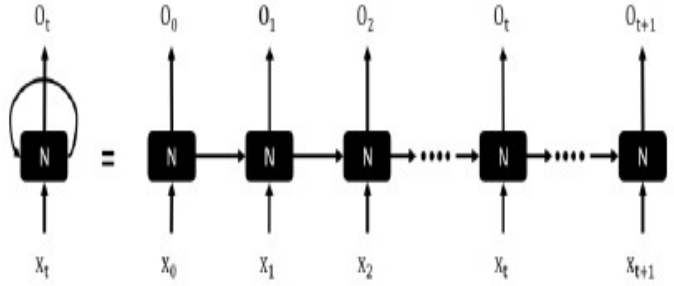

**Figure 7. Recurrent Neural Network**

In several voice applications, LSTM is setting a groundbreaking record for some classic models and drastically altering the field of speech recognition. It is presented as a solution to the short-term memory issue with RNNs. The following time step is where LSTM units make a connection to the scenario. A memory cell is the arrangement of the information-accumulating components.

## 4. Review of use of Deep Learning for Cyber Attacks Detection

### 4.1 Comparison and Analysis:

To carry out flow-based anomaly detection, Tang et al. [16] suggest a DNN model. Their initial attempt to use DNN for network security yielded a rather basic DNN with three hidden levels, one output layer, and one input layer. A few tests are conducted using the NSL-KDD dataset, demonstrating that the suggested DNN model outperforms the other machine learning techniques in terms of behavior and is able to identify zero-day attacks. The fact that harmful assaults happen often and in big quantities creates challenges that call for scalable solutions.

In response to this problem, Vinayakumar et al. [8] offer a scalable and hybrid DNN framework that can actively warn of potential network assaults by monitoring host level events and network traffic in real-time. To analyze large amounts of data, their suggested system specifically uses scalable computing architecture, text representation techniques, and DNNs. DNNs may also assist their model perform better by enhancing its nonlinear activation functions. Maintaining the network system and computer in a secure and regular operating state and preventing the incursion of malevolent network hackers are critical tasks for network administrators.

### 4.2 Public Datasets:

Many public datasets are popular to prove and compare efficiency and effectiveness among different attack detection methods. Among them, we list two famous benchmark datasets, that is, KDDCup 99 and NSLKDD, which are widely used in the academic research to evaluate the ability to detect attacks.

Table 1: Category of 22 different attacks contained by KDDCup 99.

| Class label | Attack name |
|---|---|
| DoS | back, land, neptune, pod, smurf, teardrop. |
| Probe | ipsweep, nmap, portsweep, satan. |
| R2L | ftp_write, guess_passwd, imap, multihop, phf, spy, warezclient, warezmaster. |
| U2R | buffer_overflow, loadmodule, perl, rootkit. |

**4.3Performance metrics for the problem:-**

• To assess how successfully a model has classified the data points that correspond to each of the 23 classes, we will utilize the Confusion Matrix.

• To identify the optimal model, we will compute precision, recall, and weighted f1-score in addition to the confusion matrix.

**4.4Another important metric:**

Our goal with this task is to have the lowest possible FPR. This is due to the fact that the loss of a "Normal" connection due to it being mistakenly identified as a "Bad" connection is not as serious as the potential security danger posed by a "Bad" connection being mistakenly identified as a "Normal" connection.

The TPR and FPR for this Intrusion Detection issue may be explained as follows:

- For this Intrusion Detection System problem, the TPR and FPR can be described as below:-

$$\text{TPR (True Positive Rate)} :- \frac{\text{Total no. of points correctly classified as "Normal" or "Good" connection points}}{\text{Total no. of points actually belonging to "Normal" or "Good" connections}}$$

$$\text{FPR (False Positive Rate)} :- \frac{\text{Total no. of points INCORRECTLY classified as "Normal" or "Good" connection points}}{\text{Total no. of points belonging to "Intrusion" or "Bad" connections}}$$

## 5.Conclusion and Future Works:

Deep learning achieves notable outcomes in the areas of unsupervised feature learning and pattern recognition by processing data using cascaded layers in a hierarchical framework. Motivated by the effectiveness of deep learning techniques, we think deep learning is critical to the field of network security, leading us to examine the state-of-the-art deep learning techniques for attack detection. We examine current approaches, categorize them based on various deep learning methodologies, and condense the effectiveness of the most exemplary approaches .The study of using deep learning techniques to attack detection has advanced significantly in the last several years. However, there are still a lot of issues.

First of all, deep learning techniques are difficult to adapt and use as real-time classifiers for attack detection. The majority of earlier studies just reduced feature dimension to lower computing costs during the feature extraction phase. Second, the majority of deep learning methods are suitable for image and pattern recognition analysis. Based on the aforementioned study, we believe that this overview will be helpful to anyone who have suggestions on how to enhance attack detection's accuracy; it will also offer direction and ideas for future research in this area.

## REFERENCES:-

[1] Buczak, L.; Guven, E. A Survey of Data Mining and Machine Learning Methods for Cyber Security. IEEE Commun. Surv. Tutor. 2016, 18, 1153–1176.

[2] A. Milenkoski, M. Vieira, S. Kounev, A. Avritzer, and B. D. Payne. Evaluating computer intrusion detection systems: A survey of common practices. ACM Comput. Surv., vol. 48, no. 1, pp. 1-41, 2015.

[3] C. N. Modi and K. Acha. Virtualization layer security challenges and intrusion detection/prevention systems in cloud computing: A comprehensive review. J. Supercomput., vol. 73, no. 3, pp. 1192-1234, 2017.

[4] Nguyen, T.T.T.; Armitage, G. A survey of techniques for internet traffic classification using machine learning. IEEE Commun. Surv. Tutor. 2008, 10, 56–76.

[5] E. Viegas, A. O. Santin, A. França, R. Jasinski, V. A. Pedroni, and L. S. Oliveira. Towards an energy-efficient anomaly-based intrusion detection engine for embedded systems," IEEE Trans. Comput., vol. 66, no. 1, pp. 163-177, Jan. 2017.

[6] A. Patcha and J.-M. Park, ``An overview of anomaly detection techniques: Existing solutions and latest technological trends," Comput. Netw., vol. 51, no. 12, pp. 34483470, Aug. 2007.

[7] Sperotto, A.; Schaffrath, G.; Sadre, R.; Morariu, C.; Pras, A.; Stiller, B. An overview of IP flow-based intrusion detection. IEEE Commun. Surv. Tutor. 2010, 12, 343–356.

[8] Wu, S.X.; Banzhaf, W. The use of computational intelligence in intrusion detection systems: A review. Appl. Soft Comput. 2010, 10, 1–35. [CrossRef]

[9] Bharati, S.; Podder, P.; Mondal, M.; Robel, M. and Alam, R.; Threats and countermeasures of cyber security in direct and remote vehicle communication systems. Journal of Information Assurance & Security. 2020, 15(4), 153-164. 2020.

[10] Al-Garadi, M.A.; Mohamed, A.; Al-Ali, A.; Du, X.; Guizani, M. A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security. arXiv 2018, arXiv:1807.11023.

[11] El Hihi, S.; Bengio, Y. Hierarchical recurrent neural networks for long-term dependencies. In Advances in Neural Information Processing Systems; MIT Press: Cambridge, MA, USA, 1996; pp. 493–499.

[12] Sutskever, I.; Vinyals, O.; Le, Q.V. Sequence to sequence learning with neural networks. In Advances in Neural Information Processing Systems; MIT Press: Cambridge, MA, USA, 2014; pp. 3104–3112.

[13] 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.

[14] Hochreiter, S.; Schmidhuber, J. Long short-term memory. Neural Comput. 1997, 9, 1735–1780. Artificial Neural Network for Cybersecurity: A Comprehensive Review

[15]R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat, and S. Venkatraman, “Deep learning approach for intelligent intrusion detection system,” IEEE Access, vol. 7, pp. 41525–41550, 2019

[16] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi and M. Ghogho, "Deep learning approach for Network Intrusion Detection in Software Defined Networking," 2016 International Conference on Wireless Networks and Mobile Communications (WINCOM), Fez, Morocco, 2016, pp. 258-263