iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** XII **Month of publication:** December 2021

DOI: https://doi.org/10.22214/ijraset.2021.39349

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue XII Dec 2021- Available at www.ijraset.com

Understanding Deep Learning Architecture to Various Problems of Cyber Security

Dr. Diwakar Ramanuj Tripathi
Information Technology & Legal Consultant, Nagpur, Maharashtra (India)

Abstract: Traditional machine learning has evolved into deep learning. It's capable of extracting the best feature representation from raw input samples. Intrusion detection, malware classification, Android malware detection, spam and phishing detection, and binary analysis are just a few examples of how this has been used in cyber security. Deep auto encoders, limited Boltzmann machines, recurrent neural networks, generative adversarial networks, and other DL methods are all described in this study in a brief tutorial-style method. After that, we'll go over how each of the DL methods is employed in security applications.
Keywords: Machine, Cyber, Security, Architecture, Technology.

I. INTRODUCTION

The creation of defence techniques that protect computing resources, networks, programmes, and data from illegal access, change, or destruction is known as cybersecurity. New cybersecurity dangers are emerging and evolving swiftly as a result of tremendous improvements in information and communication technology. Cybercriminals are employing new and sophisticated tactics to speed up and scale their attacks. As a result, more flexible, adaptable, and strong cyber defence systems that can identify a wide range of threats in real time are required.

The set of technologies and practises meant to protect computers, networks, programmes, and data from attack, illegal access, change, or destruction is known as cyber security. These systems are made up of network security and host security systems, each of which includes a firewall, antivirus software, and an intrusion detection system at a minimum (IDS). The relevance of cyber security employing deep learning techniques is summarised in this survey (DL). In recent years, researchers have used deep learning techniques. Deep learning can be used in conjunction with existing automation methods such as rule and heuristic-based methods, as well as machine learning approaches.

This research demonstrates the value of deep learning algorithms in classifying and correlating harmful activity detected from various sources such as DNS, email, and URLs. Deep learning algorithms, unlike older machine learning methods, do not use feature engineering and have visualisation methods. They will select the finest options on their own. Still, further domain-level alternatives for deep learning methods in information science activities must be outlined. Texts surround the cyber security events considered during this investigation. Several linguistic communication processes and text mining methods, as well as deep learning, are used to convert text to real-valued vectors.

Cyber security solution development has remained a difficult task. The majority of existing solutions rely on signature-based detection. A signature-based detection system necessitates human supervision and updating of the signature on a regular basis. Because signature-based systems rely solely on a signature database, they fail to deal with new variants of malware or cyber threats, as well as wholly new malware or cyber threats. To solve the difficulties of traditional cyber security measures, researchers are looking towards artificial intelligence and, more specifically, machine learning. Machine learning is a method for teaching a computer to discriminate between benign and harmful files. A machine must first be educated with a set of features extracted from both benign and malicious samples in order to do so. Machine learning has a sub-module called deep learning. Deep neural networks is another name for it (DNNs).

Deep learning architectures have excelled at a variety of supervised and unsupervised long-standing artificial intelligence problems, including natural language processing (NLP), picture processing, speech recognition, and many more. Large-scale data may now be trained thanks to recent advances in optimization and parallel and distributed computing technology. Deep learning is based on how the brain functions. When faced with a massive volume of data, deep learning systems can understand the meaning of the data and tune it whenever new data comes. As a result, it does not require domain expert knowledge to comprehend the significance of new information. Deep learning has the advantage of learning hierarchical feature representation by sending data to multiple hidden layers.

II. DEEP LEARNING'S IMPACT ON CYBER SECURITY

To improve the rate of cyber-attack and virus detection, deep learning architectures must be applied to cyber security. In comparison to traditional machine learning methods, deep learning architectures offer the extra benefit of being able to examine large amounts of security artefact data. Because both traditional machine learning algorithms and Deep learning architectures are parameterized, the best parameters determine the best performance. In recent days, finding suitable parameters in deep learning has remained a significant task. Despite the fact that there are now enough attack detection systems accessible, the constant increase in the number of attacks and the advancement in hacking abilities necessitate the creation of new detection methods. Although existing machine learning algorithms have had a lot of success in recent decades, they have a lot of trouble identifying cyberattacks in big distributed networks, and their scalability over a wide network is limited. Traditional machine learning methods have the disadvantage of using handmade features for recognition. However, it is preferable if the machine discovered and organised the features for attack detection on its own. Deep learning is one of the most active study areas in artificial intelligence right now, and it offers a lot of potential for overcoming the limitations of classic machine learning methods. Humans extract the features in typical machine learning methods. Feature engineering is a unique research direction. However, in feature extraction, deep neural networks outperform humans in huge data processing.

Because of its sophistication and capacity to self-learn, DL enables more accurate and faster processing. The success of deep learning in numerous fields, as well as the limitations of traditional cybersecurity approaches, necessitates further research into the use of deep learning in security domains. Cybersecurity areas, such as cyberattack detection, can benefit from DL.

Although deep learning methods have been successful in image, audio, and object identification, they are being used sparingly in cyberattack detection. The inability of existing cybersecurity solutions to cope with the growing dynamics of cyberattacks, failure to detect new threats, difficulties in the analysis process of complex events, and limitations of effective scalability as the volume of data and attack grows, are the main challenges that new cybersecurity solutions will face in the coming years. The use of deep learning methods to solve these issues is the main strategy that researchers are interested in. DDoS attack detection, behavioural abnormalities detection, malware and protocol detection, CAPTCHA code detection, botnet detection, and voice identification are only a few of the capabilities of DL methods for successful application in cybersecurity challenges.

III. ANALYSIS OF DIFFERENT DEEP LEARNING METHODS USED IN CYBER SECURITY

The many DL methods used in cyber security are described in this section. For each procedure, citations to key methodology publications are supplied.

A. Deep Belief Networks

Hinton introduced Deep Belief Networks in a seminal publication (DBNs). They're a type of DNN that's made up of numerous layers of hidden units with connections between them but not between the units within each layer. Unsupervised training is given to DBNs. To reconstruct the inputs, they are usually trained by altering weights in each hidden layer individually.

1) *Deep Autoencoders:* Autoencoders are a type of unsupervised neural network that takes a vector as input and attempts to match the output to that vector. One can generate a higher or lower multidimensional representation of the data by taking the input, altering the dimensionality, and reconstructing the input. Because they learn compressed data encoding in an unsupervised manner, these neural networks are extremely adaptable. They can also be trained one layer at a time, decreasing the computational resources needed to create a useful model. The network is used to encode data when the hidden levels have a lower dimensionality than the input and output layers (Figure 1). (i.e., feature compression). By training an autoencoder to rebuild the input from a noisy version of the input (Figure 2), a denoising autoencoder can be developed to eliminate noise and be more resilient. Compared to traditional autoencoders, this approach has been proved to be more generalizable and robust.

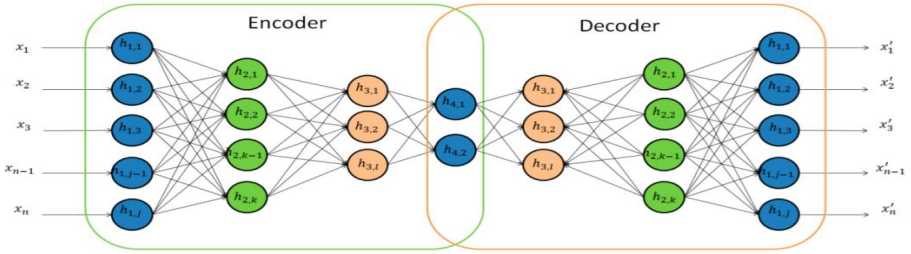


Figure 1. Deep autoencoder.

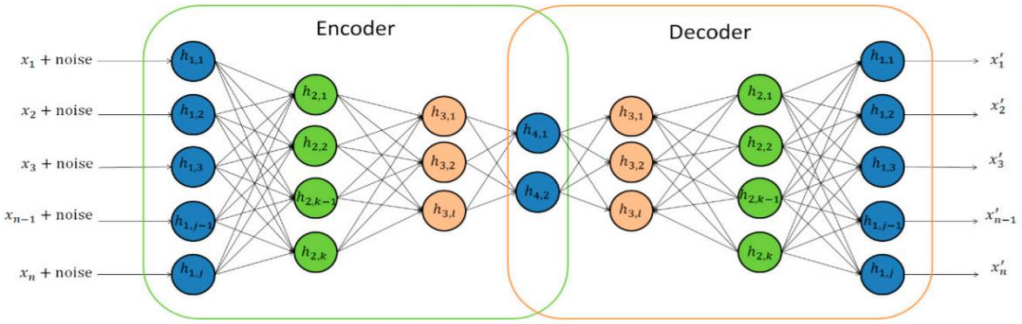


Figure 2. Denoising autoencoder.

Stacked autoencoders use numerous layers of autoencoders that are trained in order to gradually compress the data more and more (Figure 3). The full stacked autoencoder with a classification layer is shown in Figure 5a. Figure 3b shows how to make an autoencoder. The outputs of Figure 3b are then used as inputs for the autoencoder Figure 3c. After they've been trained, they're combined and a classification layer is added. Denoising autoencoders can be layered in the same way that ordinary autoencoders can.

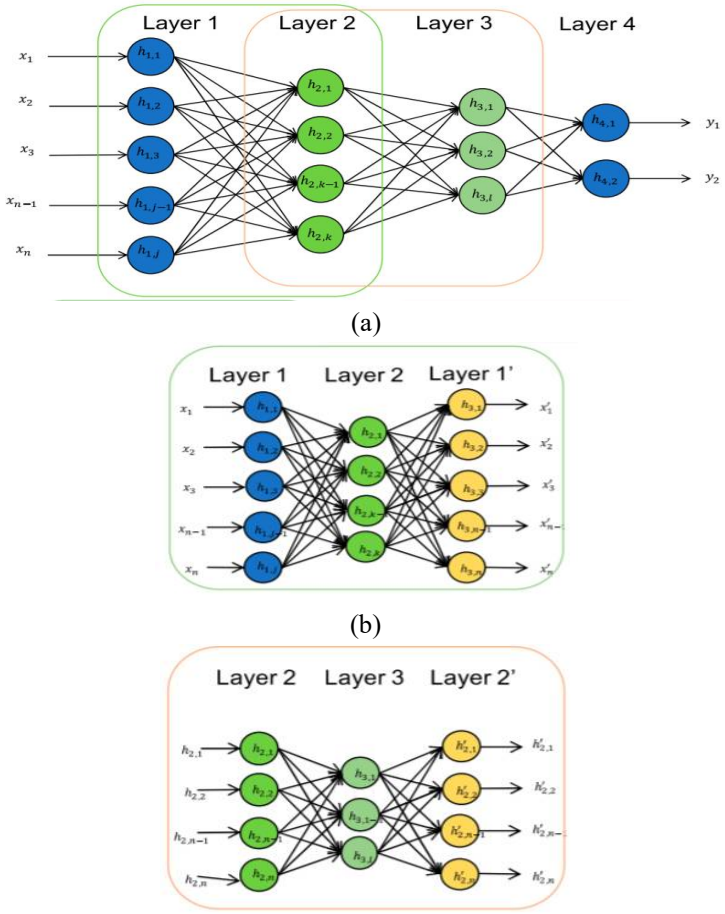


Figure 3. Stacked autoencoder with a classification layer. (a) Stacked autoenoder; (b) autoencoder for layer 2; (c) autoencoder for layer 3

A sparse autoencoder is a sort of encoder in which the number of hidden nodes is more than the number of input and output layers, but only a fraction of the hidden units is engaged at any given moment. This is compensated for by imposing a penalty for activating additional nodes.

2) *Restricted Boltzmann Machines:* The building blocks of DBNs are restricted Boltzmann machines (RBMs), which are two-layer, bipartite, undirected graphical models (data can flow in both directions, rather than just one). RBMs are unsupervised, like autoencoders, and can be trained one layer at a time. The input layer is the first, and the concealed layer is the second (Figure 4). There are no connections between nodes in the same layer, yet every node in the input layer is connected to every node in the hidden layer.(i.e., full connectivity).

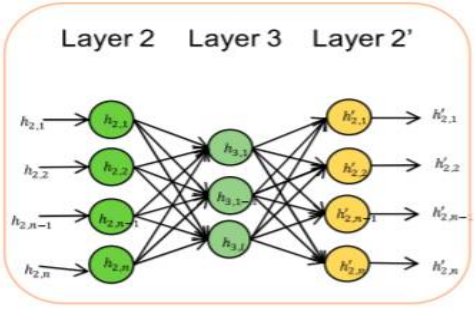


Figure 4. Restricted Boltzmann machine

The units in the input and hidden layers are usually limited to binary. The network is trained to minimise the "energy," a function that assesses the model's compatibility, using statistical mechanics for much of the math. The goal of training the model is to discover the functions, and hence the hidden state, that minimises the system's energy consumption. RBMs are also probabilistic, meaning they assign probabilities rather than exact values. The output, on the other hand, can be used as features in another model. By sending binary input data forward through the model, the model is trained. The incoming data is then sent backwards through the model to rebuild it. The system's energy is then estimated and used to adjust the weights. This procedure is repeated until the model achieves convergence. RBMs, like autoencoders, can be stacked to construct numerous layers in order to make a more complex neural network. Stack RBMs are what they're called.

3) *DBNs or RBMs or Deep Autoencoders Coupled with Classification Layers:* To accomplish a classification using a fully linked layer or layers, both RBMs and autoencoders can be paired with a classification layer (Figure 4). The feature extractors are the layers that have been taught using unsupervised learning, and they are inputs into the fully connected layers that have been trained using back propagation. These layers, unlike the RBM and autoencoder layers, require labels to train. Acoustic modelling, speech recognition, and image recognition are just a few of the applications for these sorts of networks.

B. Recurrent Neural Networks

Figure 6 shows how a recurrent neural network (RNN) extends the capabilities of a typical neural network, which can only handle fixed-length data inputs, to accommodate variable-length input sequences. The RNN processes inputs one by one, using the hidden units' output as additional input for the following element. As a result, RNNs may deal with speech and language issues as well as time series issues.

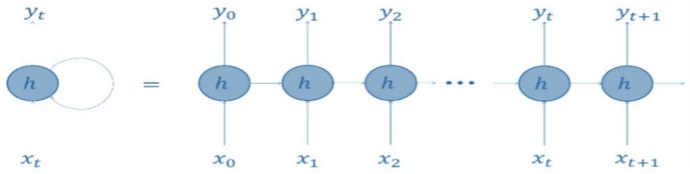


Figure 6. Recurrent neural network.

RNNs are more challenging to train than other types of neural networks because gradients can simply vanish or explode. However, advances in training and construction have resulted in a range of easier-to-train RNNs. As a result, RNNs have demonstrated their ability to anticipate the next word in a sentence, speech recognition, image captioning, language translation, and other time-series prediction tasks. An RNN's hidden units can keep track of a "state vector" that holds a memory of previous events in the sequence. Depending on the type of RNN node utilised, the length of this "memory" can be changed. The longer the memory, the longer the RNN can learn long-term dependencies.

C. Convolutional Neural Networks

A convolutional neural network (CNN) is a type of neural network that processes data in arrays. A colour or grayscale image, which is a two-dimensional (2D) array of pixels, is an example input. CNNs are frequently used to process 2D image arrays or audio spectrograms. They're also commonly utilised in three-dimensional (3D) arrays (videos and volumetric images). Their use to one-dimensional (1D) arrays (signals) is becoming more common. CNNs are utilised everywhere there is spatial or temporal ordering, regardless of dimensionality. Convolution layers, pooling layers, and the classification layer are the three types of layers that make up the architecture of a CNN (Figure 7). The CNN's core is made up of convolution layers. The weights define the receptive field, which is a convolution kernel applied to the original input, one small window at a time. The outcome of applying these filters to the full input is called a feature map, and it is then run through a non-linearity, usually a ReLU. These convolution kernels, called after the mathematical convolution procedure, allow for the accounting of close physical or temporal links within the data and assist save memory usage by using the same kernel over the entire image.

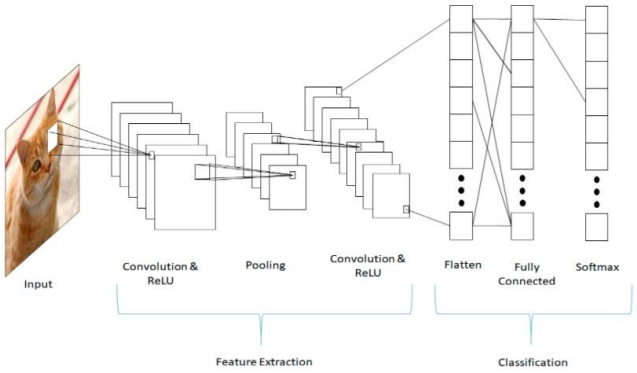


Figure 7. Convolutional neural network.

CNNs are used in a wide variety of ways. Computer vision tasks such as scene and object detection and object identification have had the most success. From biology to facial recognition, there are a variety of applications. The best demonstration of CNN success was in 2012 at the ImageNet competition, when a CNN outperformed other methods, and then in 2015 with the use of GPUs, ReLUs, dropout, and the production of new images, when a CNN outperformed human accuracy. CNNs have also been effectively utilised in language models for phoneme detection, letter recognition, speech recognition, and language model construction.

D. Generative Adversarial Networks

In unsupervised machine learning, generative adversarial networks (GANs) are a sort of neural network design in which two neural networks compete against each other in a zero-sum game to outsmart each other. One network function as a generator, while the other acts as a discriminator, according to Goodfellow et al. The generator accepts input data and produces output data that is identical to real data. The discriminator compares real data to data generated by the generator to determine whether the input is genuine or not. When the training is complete, the generator can produce fresh data that is indistinguishable from genuine data.

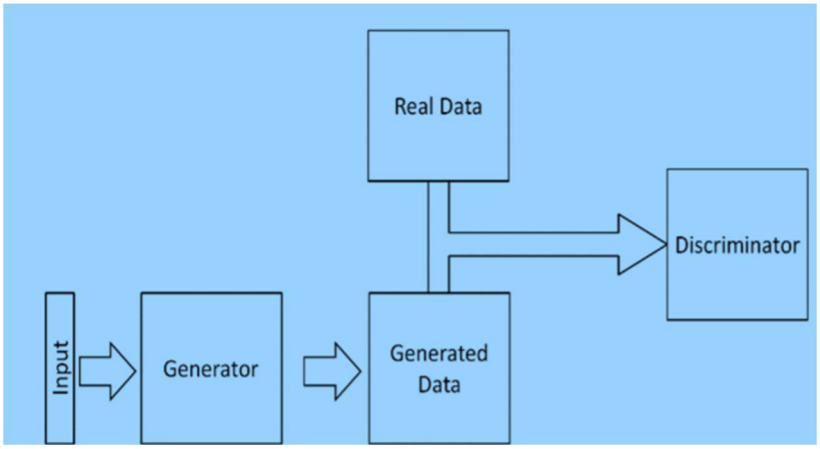


Figure 8 Generative adversarial network

E. Recursive Neural Networks

Recursive neural networks (Figure 9) are neural networks that apply a set of weights to a series of inputs recursively. The output of a node is utilised as the input for the following stage in these networks. The first two inputs are fed into the model jointly at initially. The output of that step is then used as an input for the next phase. This model has been utilised for picture segmentation and natural language processing problems.

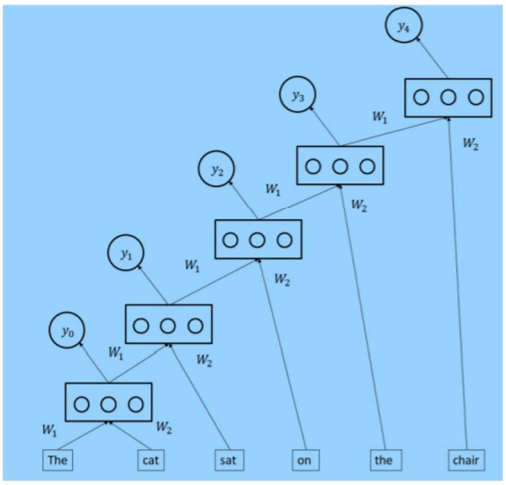


Figure 9. Recursive neural network.

IV. CHALLEGES FACED BY DL-BASED SECURITY TECHNOLOGIES

Adoption of DL–based security technologies face a number of challenges. The accuracy of these models is a key stumbling block. Because DL tools are fundamentally black boxes, there is a common sense of risk aversion when adopting any new tool. As a result, when errors occur, diagnosing the source is challenging, and unlike DL applications for, say, the marketing business, cyber security failures come with larger costs and hazards. It's possible that a cyber security analyst will waste time triaging false alarms, or that automated reactions to DL intrusion detections will wrongly limit access to important services. Furthermore, a DL tool may completely overlook a cyber-attack. Another impediment to adoption is that many of the current systems are focused on a single danger, such as malware detection. Researchers should examine how to generalise or integrate different DL techniques to address a broader range of attack vectors for a more comprehensive solution. Multiple DL detection algorithms are required in concurrently, and they may benefit from knowledge gained through various methods in order to increase their performance locally. For example, if the number of DGA domains detected increases, it may be beneficial to notify the malware detectors. In contrast, a decrease in detected attacks from a given adversary could indicate that they have transitioned to a new attack that evades detectors, necessitating new action. There is very little study on active learning in the cyber security arena, thus this last scenario in particular needs to be investigated.

Finally, when developing DL solutions for cyber security, the adversary must be considered. Susceptibility to data poisoning will be a useful indicator to consider while evaluating a method. Researchers should think about how an attacker could utilise deep learning to get around deep-learning-based detection systems. Bahnsen et al., for example, looked at how an attacker may utilise DNNs to improve the effectiveness of phishing attempts and get around machine-learning-based phishing detection systems. This falls under the category of adversarial examples, a new study topic that looks into the flaws and vulnerabilities of machine learning models. Hardening systems against zero-day assaults by extremely adept attackers will require this.

V. CONCLUSION

This study aims to give a comprehensive assessment of recent research on the use of Deep Learning techniques to address computer security issues. Deep learning is a popular method used in a variety of cyber security applications. Deep learning algorithms are regarded a reliable solution to tackle problems when compared to traditional methods and machine learning methods. It is obvious from this research that most deep learning algorithms have a higher accuracy rate, which will be useful in developing a real-time application for evaluating dangerous network activity. According to our views of the examined works, the literature on employing Deep Learning approaches to solve computer security concerns is still in its infancy.

REFERENCES

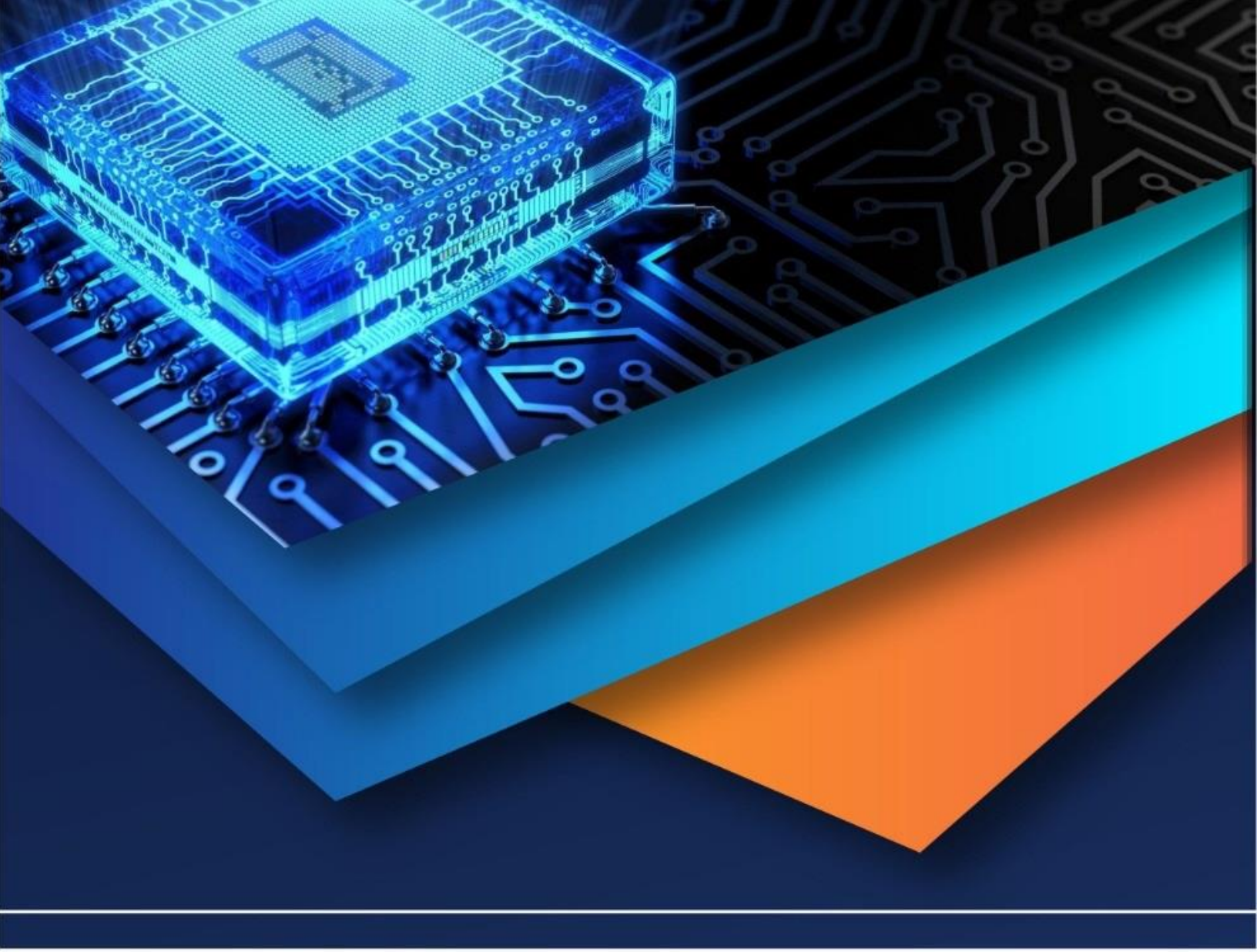
[1] Imamverdiyev, Yadigar& Abdullayeva, Fargana. (2021). Deep Learning in Cybersecurity: Challenges and Approaches. 10.4018/978-1-7998-7705-9.ch095.
[2] Dlshad, Kosrat& Askar, Shavan. (2021). Deep Learning Models for Cyber Security in IoT Networks: A Review. 10.5281/zenodo.4497017.
[3] Choi, Yoon-Ho & Liu, Peng & Shang, Zitong & Wang, Haizhou& Wang, Zhilong& Zhang, Lan & Zhou, Junwei & Zou, Qingtian. (2020). Using deep learning to solve computer security challenges: a survey. Cybersecurity. 3. 15. 10.1186/s42400-020-00055-5.
[4] Ravi, Vinayakumar&Kp, Soman & Poornachandran, Prabaharan & Soman, Akarsh. (2019). Application of Deep Learning Architectures for Cyber Security. 10.1007/978-3-030-16837-7_7.
[5] Ferrag, Mohamed Amine & Maglaras, Leandros &Moschoyiannis, Sotiris & Janicke, Helge. (2019). Deep Learning for Cyber Security Intrusion Detection: Approaches, Datasets, and Comparative Study. Journal of Information Security and Applications. 50. 10.1016/j.jisa.2019.102419.
[6] Mahdavifar, Samaneh & Ghorbani, Ali. (2019). Application of Deep Learning to Cybersecurity: A Survey. Neurocomputing. 347. 10.1016/j.neucom.2019.02.056.
[7] Chen, L, Sultana S, Sahita R (2018) Henet: A Deep Learning Approach on Intel Ⓡ Processor Trace for Effective Exploit Detection In: 2018 IEEE Security and Privacy Workshops (SPW).. IEEE. https://doi.org/10.1109/spw.2018.00025.
[8] Apruzzese, Giovanni &Colajanni, Michele & Ferretti, Luca & Guido, Alessandro & Marchetti, Mirco. (2018). On the effectiveness of machine and deep learning for cyber security. 371-390. 10.23919/CYCON.2018.8405026.

AUTHOR PROFILE

Dr. Diwakar Ramanuj Tripathi

Received the graduation (B.Sc.) degree in Computer Science, Master degree (MCA) in computer Application and Doctor of Philosophy (Ph.D.) in Computer Science. He is a Microsoft Certified I.T. professional (MCITP), Microsoft Certified Technology Specialist (MCTS) and Microsoft Certified Trainer (MCT) with 12 + years' experience in Computer Science. He has awarded the Life Time Achievement Award & Outstanding Scientist Award in Computer Science. He has pro-actively associated with various professional bodies.

IEI; IACSIT, Singapore; CSI; ISTE; IAENG, Hong Kong; IEEE; ASDF UK; CSTA; ACM, SDIWC, USA; IFERP; AIMA; ISCA; He is currently working as an Information Technology & Legal Consultant at Nagpur.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY