A Review Paper on Cyber Security System Based on CNN and RNN

Pankaj Saraswat

SOEIT, Sanskriti University, Mathura, Uttar Pradesh, India

Email Id- pankajsaraswat.cse@sanskriti.edu.in

ABSTRACT: The government, military, business, financial, and medical organizations acquire procedures and store enormous amounts of data on PCs and other devices, cybersecurity is becoming increasingly important in a variety of areas, including government, military, and so on. A large portion of the data might be sensitive data, such as scholarly, financial, or personal data, or other types of data for which unauthorized access or introduction could have severe consequences. Using deep learning methods, the author can uncover attack types using this methodology. Work area application that detects a web application assault and delivers a notification to the webserver system. It is possible to get many comparable results with less preparatory time by using Gated Recurrent Units instead of traditional LSTM systems. Improved irregularity IDS is achieved by combining stacked CNNs with GRUs. Interruption detection relies on a language model built on regular call arrangements from the ADFA Data set of system call traces to determine the chance of a certain call grouping occurring.

KEYWORDS: Convolutional Neural Network (CNN), Cyber-attack, Deep learning, Neural Networks, Recurrent Neural Network (RNN).

1. INTRODUCTION

Because of the increased degree of assaults on association networks and systems, cybersecurity has become a major concern as technology advances. In such cases, Intrusion Detection Systems (IDS) are a must-have for protecting an association's electronic assets. Host-based Intrusion Detection Systems (HIDS) and Network-based Intrusion Detection Systems (NIDS) are the two types of interruption detection systems (NIDS). To protect a system against network-based threats, system-based interruption detection systems filter and analyse organized traffic[1]–[3].

The system-based IDS focuses on obtaining data from the bundle itself and examining the content of individual parcels with the goal of detecting malignant movement in traffic organizations. Host-based interruption detection systems are a system security innovation that were originally designed to identify vulnerability abuses against a target application or PC system. A HIDS is designed to collect information about events or system calls/signs on a given system.

In earlier approaches, a huge and delegated collection of information was necessary, which was lately organized by a human master or by other ways. The final techniques do not need a pre-marked dataset for preparation. Deep Neural Networks (DNNs) are large neural networks with several layers that are capable of self-representation learning. DNNs are used in all Deep Learning computations. Fully associated Feed forward Deep Neural Networks with Directed DL computations FNN is a variant of DNN in which each neuron is linked to all of the neurons in the previous layer. To the drawback of high processing costs, FNN makes no assumptions about the data and provides an adaptive and universally usable solution for order[4], [5].

1.1 Convolutional feed forward Deep Neural Networks (CNN):

CNN is a variant of DNN in which each neuron obtains its information from a subset of neurons in the previous layer. CNN's trademark makes them attractive when it comes to breaking down spatial data, but when it comes to non-data, they fall short. CNN's calculating cost is cheaper than FNN's. Deep Neural Networks with Intermittent Activity (RNN). A kind of DNN in which neurons can communicate their output to previous levels in addition to the current layer; this structure makes them more difficult to prepare than FNN.

Mark-based and oddity-based HIDS are the two most common types. The mark-based methodology operates in the same way as an infection scanner, seeking for personalities or markings of known interruption events, whereas the peculiarity-based methodology establishes a gauge of common cases. Oddity-based IDS allows for the detection of hidden assaults, but at the cost of increased false alarm rates. However, when coupled with signature detection, it may provide a formidable barrier[6]–[9].

This approach establishes a fundamental interface between a process and the operating system. Forrest was the first to suggest that a series of system calls might be used to capture routine behaviour in a computer system. Currently, the Defense Force Academy Linux Dataset (ADFA-LD), which was recently released system call, has 833 standard preparation arrangements, 746 attacks, and 4372 approval groups, and has been used to evaluate a system call based HIDS. The system call following consists of full number call sequences. It is difficult to distinguish between normal and irregular behaviour due to the diverse and dynamic environment of system call architectures[10].

Inspired by these Deep Neural Networks applications, the author proposes an architecture with two major commitments. To begin, sequence to succession realization is a combination of a multilayer CNN and an RNN made up of Gated Recurrent Units, in which the CNN layer extracts neighboring highlights in the data groups and contributes to the GRU layer. A soft layer that is entirely associated with the GRU layer and yields a likelihood appropriation over system call, resulting in a design, handles the yield from the GRU layer. Furthermore, because of the shorter preparation periods, the author was able to successfully replace LSTM with GRU and obtain a large number of almost similar results.

1.2 Cyber Attack:

Any attempt to discover, alter, change, impair, empower, decimate, take, or add unauthorized access to or use information in PCs and PC systems is considered an assault. A cyber-attack is a form of cyber that targets computer data systems, foundations, systems, or devices. The attackers are individuals or procedures that attempt to get access to information, capacity, or other restricted areas of the system without permission, perhaps for nefarious purposes. Cyber-attacks can be classified as cyber warring or cyber fear-based oppression, depending on the situation. A cyber-attack should be conceivable for sovereign governments, individuals, groups, societies, or organisations, and it might come from an unknown source. Figure 1 shows the cyber-attacks.

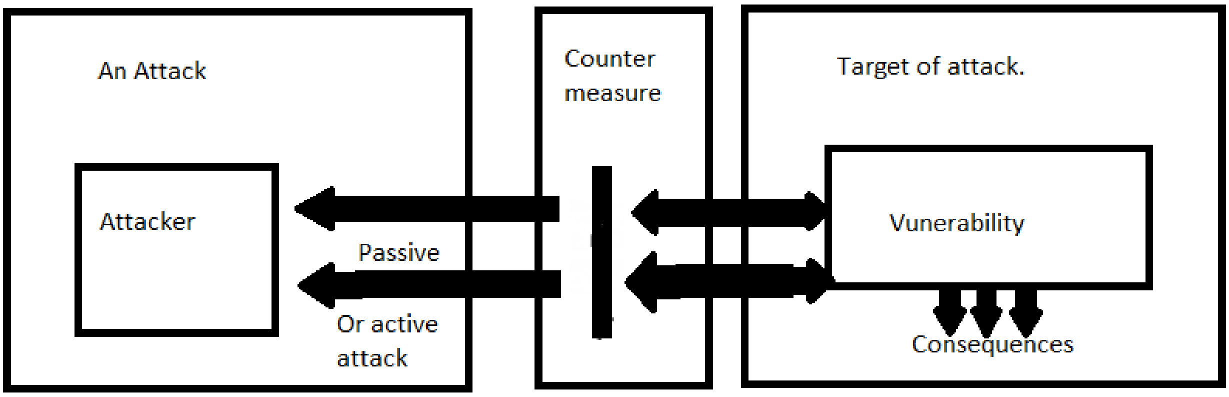

Figure 1: The above figure shows the cyber-attacks [appsealing].

1.3 RNN (Recurrent Neural Network):

A recurrent neural network (RNN), as shown in Figure 2, extends the capabilities of a traditional neural network, which can only accept fixed-length information inputs, to handle variable-length input sequences. The RNN forms inputs for each component one by one, using the yield of the shrouded units as a bonus contribution for the component after that. As a result, RNNs can deal with both discourse and language difficulties as well as time sequence concerns.

An RNN's hidden units are suitable for maintaining a "state vector" that holds a recollection of previous events in the grouping. Depending on the type of RNN hub used, the length of this "memory" can be adjusted. The longer the memory, the more long-term situations the RNN is capable of learning.

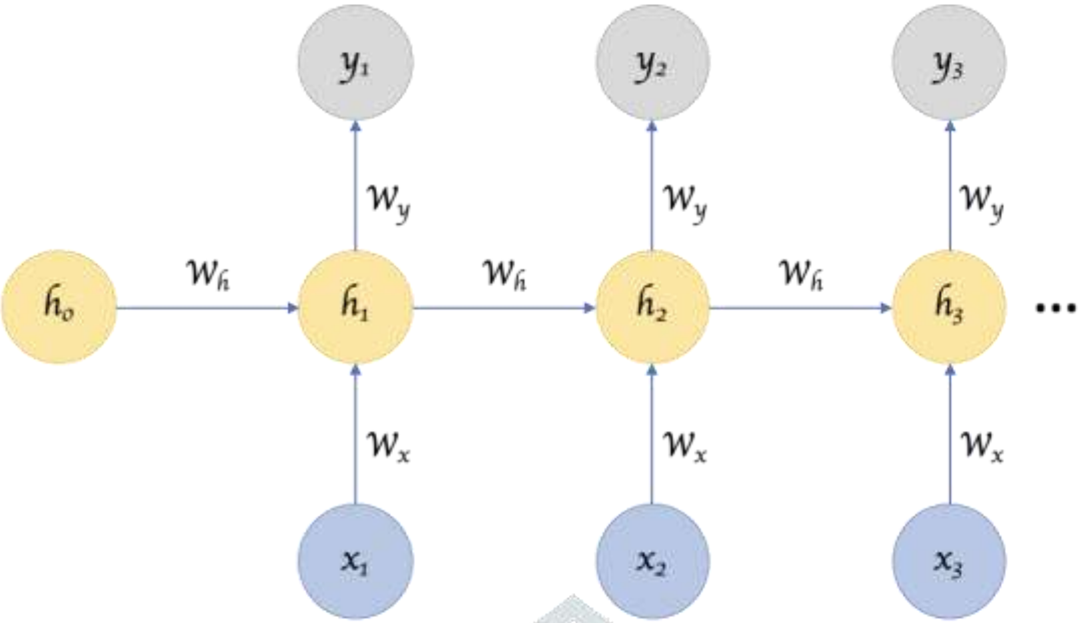

Figure 2: The above figure shows the Recurrent Neural Network [gotensor].

Long short memory (LSTM) units are familiar with enabling RNNs to manage situations that require long memories. LSTM units have a memory cell structure that collects data and correlates it with itself in the following phase. New data and an overlook doorway that loads more current and more seasoned data higher or lower depending on what is wanted enlarge the memory cell's estimates.

1.4 CNN (Convolution Neural Network):

A convolutional neural network (CNN) is a type of neural network that is designed to process input in clusters. A shade or grayscale image is a two-dimensional (2D) display of pixels that contains model information. CNNs are frequently used to create 2D versions of images or sound spectrograms. They are occasionally used for three-dimensional (3D) clusters as well (recordings and volumetric pictures). Their use of one-dimensional (1D) clusters (signals) is less frequent, but it is growing. CNNs are used if there is spatial or fleeting requesting, notwithstanding their dimensionality.

Convolution layers, pooling layers, and the sequence layer are the three types of layers that make up a CNN's design. The CNN's convolution layers are at its heart. The loads describe a convolution component that is applied to the initial data, a small window at a time, and is referred to as the responsive field. The result of applying these channels to the whole amount of data is a non-linearity, which is commonly referred to as a component map. By using a comparable bit across the aggregate of the image, these convolution parts, named after the numerical convolution activity, allow tight physical or worldly relationships inside the information to be portrayed and assist reduce memory use. Figure 3 shows the convolution Neural Network.

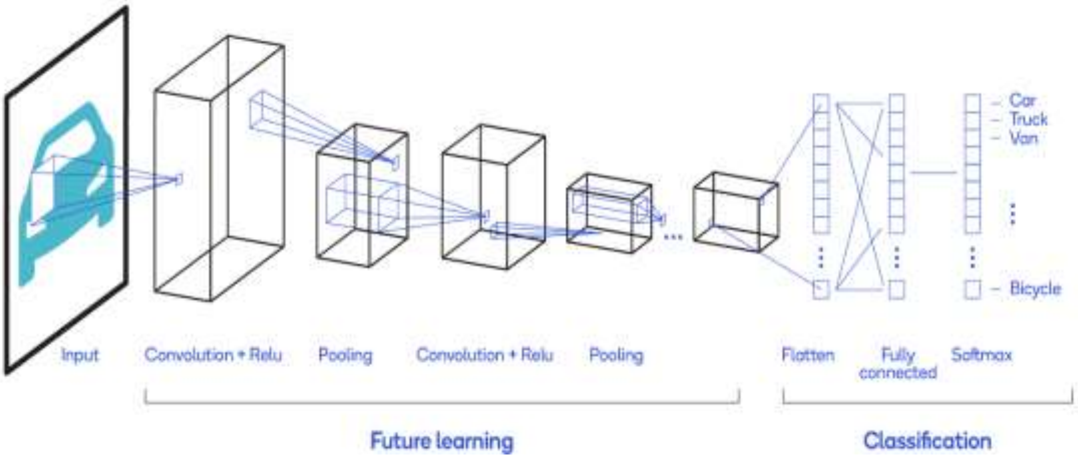

Figure 3: The above figure shows the Convolution Neural Network [qualcomm].

Additionally, CNNs can use regularization approaches to reduce overfitting. "Dropout" is one of the most effective techniques. When constructing a model-using dropout, a specified number of hubs in a particular layer, as well as their approaching and active associations, are arbitrarily evacuated during each preparation focus. Counting dropout enhances a model's precision and generalizability by increasing the likelihood that a hub will be useful. Figure 4 shows the layers of CNN.

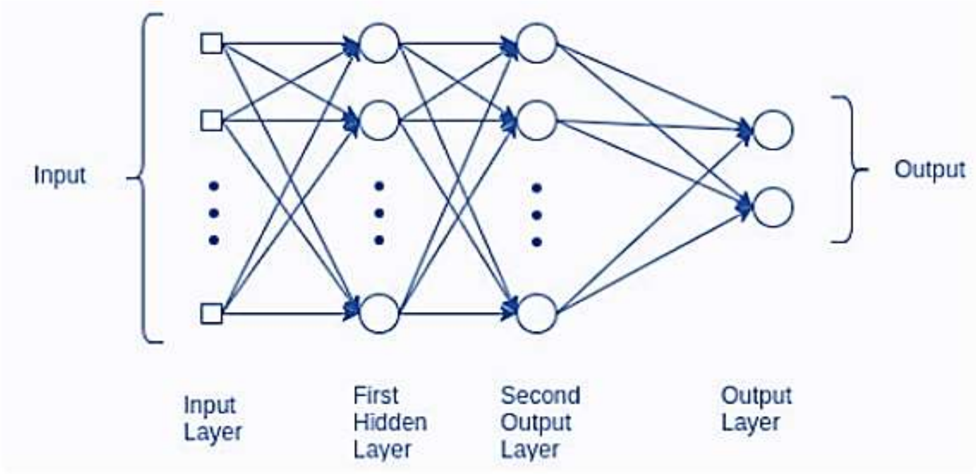

Figure 4: The above figure shows the Layers of CNN

CNN has a very different work environment. PC's apparition errand has excelled in areas like as scene and item identification, as well as evidence of identifiable things. The applications range from biology to facial recognition. The best example of CNN's success was in an ImageNet competition, when the CNN's outperformed prior results for different techniques and afterwards humanoid exactness in previous years utilising GPU, ReLU, dropouts, and decades of extra image data. Figure 5 shows the model architecture.

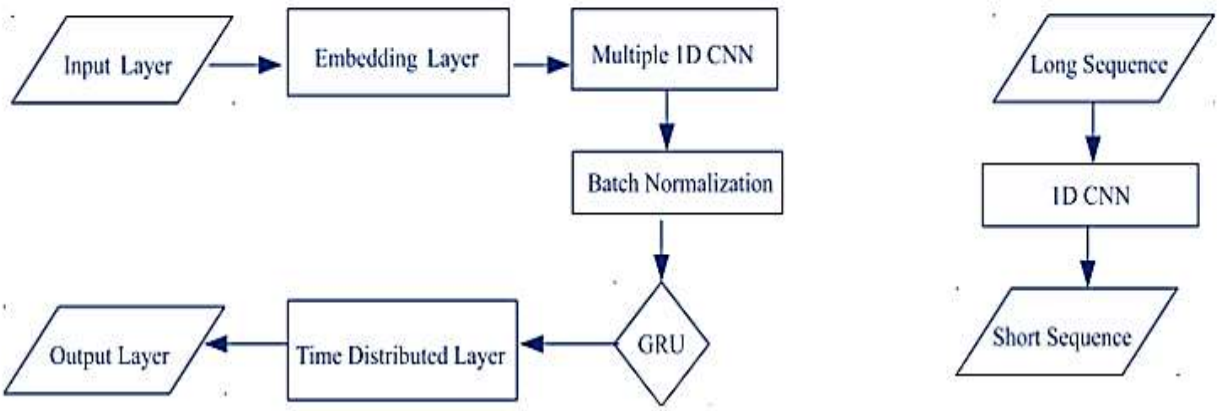

Figure 5: The above figure shows the Model Architecture.

As a result, the author devised five free models:

- Eight-layer 1D CNN using a 600 GRU unit.
- Seven-layer 1D CNN using a 500 GRU unit.
- One layer using a 200 GRU unit.
- One layer using a 200 LSTM unit
- Six-layer 1D CNN using a 200 GRU unit.

Every model was made up of 833.0 typical successions, which were divided into different lengths scaled-down groups, and each sequence into a smaller than predicted cluster was cushioned for lengths for the longest systems.

2. DISCUSSION

The author has discussed about the Cyber Security, which is based on the CNN and RNN. A large portion of the data might be sensitive data, such as scholarly, financial, or personal data, or other types of data for which unauthorized access or introduction could have severe consequences. Using deep learning methods, the author can uncover attack types using this methodology. Work area application that detects a web application assault and delivers a notification to the webserver system. It is possible to get many comparable results with less preparatory time by using Gated Recurrent Units instead of traditional LSTM systems. As seen above, a CNN's layer may capture neighborhood connections for structure into an arrangement and executes inside the same refining execution, but RNN's (GRU) layers can take in consecutive associations from these higher-level highlights. On typical named successions, models are created that estimate the likelihood of a subsequent whole number dispersion into the called sequences. The limit of characterizations is then browsed as a scope for detrimental logarithm probability esteems, and thus are used to predict the likelihood of a full sequence. Currently, the Defense Force Academy Linux Dataset (ADFA-LD), which was recently released system call, has 833 standard preparation arrangements, 746 attacks, and 4372 approval groups, and has been used to evaluate a system call based HIDS. The system call following consists of full number call sequences. It is difficult to distinguish between normal and irregular behaviour due to the diverse and dynamic environment of system call architectures. Any attempt to discover, alter, change, impair, empower, decimate, take, or add unauthorized access to or use information in PCs and PC systems is considered an assault. A cyber-attack is a form of cyber that targets computer data systems, foundations, systems, or devices. The attackers are individuals or procedures that attempt to get access to information, capacity, or other restricted areas of the system without permission, perhaps for nefarious purposes.

3. CONCLUSION

The author had concluded about the Cyber Security system, which is based on CNN and RNN. Attacks on cyber networks continue to advance at a rate that exceeds the ability of computer-generated safeguards to assemble and transmit new marks in order to detect new attacks. With advances in machine learning (ML) computation, there is a good probability that neural networks DLs will be used to detect new malware variants and zero-day attacks in the future. Currently, a late-released ADFA-LD interruption detection informative index suggests CNN-GRU languages models. As seen above, a CNN's layer may capture neighborhood connections for structure into an arrangement and executes inside the same refining execution, but RNN's (GRU) layers can take in consecutive associations from these higher-level highlights. On typical named successions, models are created that estimate the likelihood of a subsequent whole number dispersion into the called sequences. The limit of characterizations is then browsed as a scope for detrimental logarithm probability esteems, and thus are used to predict the likelihood of a full sequence. We must stay attentive to the state of workmanship execution of neural system models because to the considerable reduction in preparation time as compared to LSTM models.

REFERENCES

[1] L. Fichtner, "What kind of cyber security? Theorising cyber security and mapping approaches," *Internet Policy Rev.*, 2018, doi: 10.14763/2018.2.788.

[2] T. Limba, K. Agafonov, L. Paukštė, M. Damkus, and T. Plėta, "Peculiarities of cyber security management in the process of internet voting implementation," *Entrep. Sustain. Issues*, 2017, doi: 10.9770/jesi.2017.5.2(15).

[3] J. Kim, J. Kim, H. L. T. Thu, and H. Kim, "Long Short Term Memory Recurrent Neural Network Classifier for Intrusion Detection," in *2016 International Conference on Platform Technology and Service, PlatCon 2016 - Proceedings*, 2016, doi: 10.1109/PlatCon.2016.7456805.

[4] R. Von Solms and J. Van Niekerk, "From information security to cyber security," *Comput. Secur.*, 2013, doi: 10.1016/j.cose.2013.04.004.

[5] A. Fielder, E. Panaousis, P. Malacaria, C. Hankin, and F. Smeraldi, "Decision support approaches for cyber security investment," *Decis. Support Syst.*, 2016, doi: 10.1016/j.dss.2016.02.012.

[6] C. C. Sun, A. Hahn, and C. C. Liu, "Cyber security of a power grid: State-of-the-art," *International Journal of Electrical Power and Energy Systems*. 2018, doi: 10.1016/j.ijepes.2017.12.020.

[7] T. Limba, T. Plėta, K. Agafonov, and M. Damkus, "Cyber security management model for critical infrastructure," *Entrep. Sustain. Issues*, 2017, doi: 10.9770/jesi.2017.4.4(12).

[8] M. Sonntag, "Cyber security," in *IDIMT 2016 - Information Technology, Society and Economy Strategic Cross-Influences - 24th Interdisciplinary Information Management Talks*, 2016, doi: 10.2478/hjbpa-2019-0020.

[9] M. Gratian, S. Bandi, M. Cukier, J. Dykstra, and A. Ginther, "Correlating human traits and cyber security behavior intentions," *Comput. Secur.*, 2018, doi: 10.1016/j.cose.2017.11.015.

[10] R. Vinayakumar, K. P. Soman, and P. Poornachandrany, “Applying convolutional neural network for network intrusion detection,” in *2017 International Conference on Advances in Computing, Communications and Informatics, ICACCI 2017*, 2017, doi: 10.1109/ICACCI.2017.8126009.