International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-6, March 2020

Design of Secure Blockchain Convolution Neural Network Architecture for Detection Malware Attacks

Sharifa Nawroozi, RA. K. SaravanaGuru

Abstract: ***Nowadays, Cyberattack continues to target the applications and networks more than past with different and advance ways like programming complex format of malware that it executes unauthorized action on the targeted system, so it is needed to develop and deploy advance method to these kind of attacks for detecting correctly with a trusted and a better accuracy. Therefore, the recent solutions to detect malware attacks focuses on new advance technologies like Deep learning and Machine learning concepts. In this paper we have developed secure blockchain convolution (SBC) Algorithm that provides a better way of analyzing malware data with effectiveness and accuracy. The deep learning concept does not involve in a method to identify the trust while the process is led to extraction of the features as it can be infected by the intervention of human or a trained system. Therefore, According to research which is done towards blockchain, it features as authentication function, immutable property, information privacy and safety helps in deployment of Convolution Neural Network method with better detection. Blockchain has a decentralized structure which is able to record the data between various parties and it helps in preventing the manipulation when the deep learning concept is applied and the higher detection accuracy is received in the limited time.***

Keywords: Deep learning, Convolution Neural Network, Malwares, Block-chain. Secure Blockchain Convolution (SBC)

I. INTRODUCTION

Malware stands for malicious software, the software programs designed to access the personal program or system without the permission, intercepting computer operations and gathering important and sensitive data. Malicious software have many types such as Adware, Virus, Worm, Trojan, Backdoor, Ransomware and Rootkit [15].

In previous times the industries and researches applied many types of techniques for detecting the malware such as heuristic and signature-based methods. Signature-based method is the simplest method of detection because it considers and compares the traffic network or malware with the known signature for possible attacks. Signature based method is used mostly for antivirus software from many years to identify a specific type of virus. There is a similarity between the virus families in behavior that makes it easy to detect it but on other hand the malware authors always try to be a step ahead from the antivirus (AV) by writing the metamorphic and polymorphic malware to bypass the virus signatures. This method has a drawback and it is not efficient in detection of unknown malware or threats, therefore the vendors of antivirus also rely in heuristic methods. This is based on rules that experts determined and that rely on static and dynamic analysis methods.

In contrast, the heuristic method for analyzing the malware before writing the signature it is needed to analyze that either it may be based on the behavior or by testing the code in a safe environment so the methods analyze the malware is based on the following two methods [9]:

- **Static Analysis:** Analyzing the malware without executing it. Here during analysis the pattern will detect including opcodes or byte-sequence, string signature, byte-sequence n-gram or opcodes n-grams, etc.
- **Dynamic Analysis:** It analysis the behavior of a malware program while running on a controlled environment like a sandbox or virtual machine. The behavior of malware will be monitored by using tools such as Wireshark, Process Explorer, and Capture BAT. Here the function, the network and the flow of data are monitored and this analysis is more effective but it needs more time and consumes more resources than the static analysis.

These methods are able to detect unknown malware but the drawback is, it generates more amount of false positive than signature based method. [12] And therefore in this case some AV vendors use hybrid analysis method which includes both the methods of heuristic and signature based for better detection of unknown malware. Recently Machine learning and deep learning are the concepts used and implemented for detection malware. Therefore because of a broad range of use towards these techniques in this field, Deep learning methods such as Convolutional Neural Networks (CNN) can attribute much of this success [16]. CNNs consists layers that refers to as either a convolutional layer, pooling and non-linear layers. The first layer that includes an input layer moves the input samples to CNN's first block, thus passing data through the Network to the last layer makes the choice.

Manuscript received on February 10, 2020.
Revised Manuscript received on February 20, 2020.
Manuscript published on March 30, 2020.
* Correspondence Author
Sharifa Nawroozi*, Department of Computer Science and Engineering, Information Security Specialization, Vellore Institute of Technology, Vellore, India. Email: sharifa.nawroozi2018@vitstudent.ac.in
Dr. RA. K. SaravanaGuru, Department of Information Security, Vellore Institute of Technology, Vellore, India. Email: saravanank@vit.ac.in

For the systems to use correctly and securely Artificial Intelligent systems, each block must be authenticated faultlessly. [5] In the other words, the CNN model will miss the accountability for each block therefore blockchain can be useful. Blockchain can assist secure implementation of AI systems in the public domain with its data privacy, transparency, safety, and authentication function.

The security element can be considered as a guard who checks whether the network architecture has been manipulated or not. On the other hand, it works on an Artificial Intelligent system. The decision property which is made by a specific AI model block would require validation of other blocks connected to the block in concern is called authentication. [13].

With the proper deployment of block chain technology, it is possible to avoid the attack in the applying method for detection level and classification. It is no longer possible to manipulate any layer in convolutional neural network, for example feature extraction and matching using cryptography and transitive hash will help it and modification in any layer will make alarm.

Any operation if performed at a specific block is malicious and at the previous checkpoint of the system can be restored. On the other hand, decentralization attribute, guarantees that not all controls are in a single entity's hands. Just as an unscrupulous chief executive of a business can present an inflated version of the assets of the business to attract the attention of potential shareholders, an unethical model proprietor can use unfair means to boast about the results of the model.

These above-mentioned characteristics are needed to provide a secure model of the Deep Neural Network (DNN) and making block chain a suitable candidate for the job. We have suggested an architecture in this study that combines CNN architecture with blockchain technology characteristics. The model can detect malware attack that is performed at the level of the parameter or at the level of feature extraction each block for instance the attack on the network level. Tampering vulnerability exists if CNN models are used without blockchain. While the inclusion of blockchain in CNN can effectively remove network level attack on CNN .The remaining of this paper is as follows:

The second section describes literature survey on the detection of malware methods as static, dynamic, machine learning and deep learning. The section III is discussed about the proposed methods, algorithm and methodology which include the structure of CNN and Blockchain. Section IV explains the experiment result and setup. The last section is the conclusion of this paper.

II. LITERATURE SURVEY

Malware classification can refer to classifying of malware and benign file. Hassen et al., (2017) [1] The authors consider many machine learning methods to extract malware samples and classify malware binaries into known malware families based on static analysis. A new feature was presented for comparing accuracy into the opcode n-gram feature and also held results in shorter training time. Su et al., (2018) [2] in this paper, they suggested a light-weight novel method for detection DDos malware in IoT environment. Frist, they extracted one-channel where gray-scale image is converted from binaries then used a light-weight convolution neural network to classify IoT malware families. According to their experiment results they gained it is 94.0% accuracy for the classification of the DDos malware. It shows significant result.

Prasse al.et. (2017) [3] In this study, they created a method that allows them to gather network flows of benign application and known malware as training data and then they applied a method for detection of malware which it is based on a neural language method and long short-term memory network (LSTM). The approached method can detect new malware. Paola al.et. (2018) [4] The author proposed a novel method based on the deep networks. First, they run malware in the sandbox environment and after this they will convert the log file of sandbox to a long binary bit-string file. It is fed to a deep neural network with 8 layered that produced 30 values in the output layer. These values as signature produced by the DBN which is very successful for detecting of malware. And the advantage of this algorithm is that it can be used for the supervised malware classification.

Kolosnjaji, al et, (2016) [8] In this study, a method was featured and was implemented based on the CNN and a current network layer, which came out to be one of the best for malware image detection. A full convolution of n-grams was combined as a sequential model in extraction of the model. The average accuracy was from 85.6% to 89.4%.

De Paola et al., (2018) [4] In this paper, the proposed method is the cloud-based malware detection system. This method is able to analysis big data which produced on the network. This system provides a fast classification that is based on the static analysis that used deep networks. And when the detection reaches uncertainty exceed a given threshold then it will use dynamic analysis and the result of dynamic analysis is exploited to refine the deep network in the continuous learning loop. And the advantage of this system is that it will be up to date that will detect new malware versions.

Abdelsalam et al. (2018) [10] In this work, they introduced a malware detection approach for virtual machines based on two dimensional convolution neural networks by utilized performance metrics. The result from the testing dataset showed that they gain accuracy of 79% and they also used 3D CNN model to improve the detection performance which used samples over a time-windows, and after applying 3D dimension to the 2D input matrix the achieved result was above 90% that is a significant output result.

Graf at el. (2018) [18] The researcher had suggested a method to manage and classify reports that happened by incident and developed a cyber situational awareness based on auto-encoder neural network and a smart contracts which is a component of blockchain technology. Both technologies are used for classification and incident management. The mentioned method would help in analyzing of cyber threat by not allowing and protecting it from critical infrastructures. The purpose of this system is to provide a solution in real time which is not need it for human to analyze cyber incident job and provide a facilitated way for cyber incident classification and will remove the irrelevant data.

And another advantage of this system is to develop an automated trusted system for incident management which allowed automatic classification, archiving and disposal based on smart contract technique.

Goel at el. (2019) [17] In this research, the authors represented a model which combined from two technology of deep neural network and blockchain technology and the name of this model is DeepRing.

The purpose of this model is to prevent the threat of any white-box adversarial attack. The tampering in any block changes the hash in other blocks as the properties of the blockchain has accountability towards the security as they stay transparent between the entire works that is categorized.

III. METHODOLOGY

A. System Description

The process of detection and classification of malware based on SBC algorithm is described in Fig 1. It starts with the input dataset which includes malimg and benign dataset. The dataset will preprocess and label as malware or benign. The processed data will forward as input for the convolution neural network then the algorithm would classify to the mentioned classes.

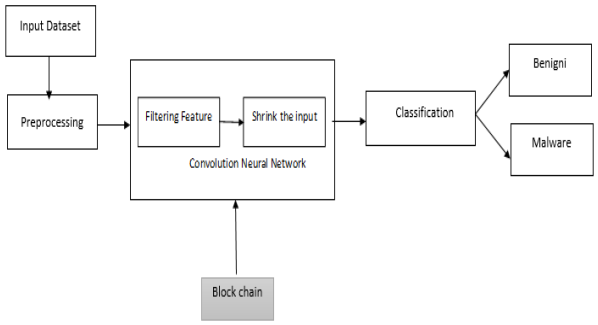

Fig 1. SBC Algorithm System

As shown in the above diagram, the vulnerability exists in CNN method during filtering the features and shrinking the input that the attacker can easily modify it and it affects the result of detection. Therefore, the blockchain technology is applied to avoid it. Each layer of CNN stored in each block and each block would have its own hash value and the pervious hash value of block. Using CNN method each gray scale image of malware will analyze one by one based on the train and test model.

B. Dataset

The Malimg dataset [6] used in this work consists of image malware along with the benign image. The binary malware is changed to the grayscale image and there is python script which converts binary malware into the grayscale image using Numpy library. In this work, the gray scale image has used directly as input to CNN model to train the data and to classify it.

C. Secure Blockchain Convolution Algorithm

Architecture (SBC)

As it is shown in the Fig 2, it is the architecture of designed algorithm which the input phase is explained already in Fig 1. And after preprocessing the dataset into train and test data. . The next phase is make up of two fold process that it is Blockchian and Convolution Neural Network. Firstly, the blockchain is created and each layer of the CNN is stored as data in blockchain.

Each layer of CNN would have same function with different values and a hash value, then the next step is the validation of the hash value which will check if it is valid. If it is invalid there are some changes in the system that would not apply CNN algorithm and it shows the massage which is invalid. On the other hand if it is valid the CNN method for analyzing and classifying the input is applied. The blockchain technology is explained in the upcoming content with CNN algorithm in detail.

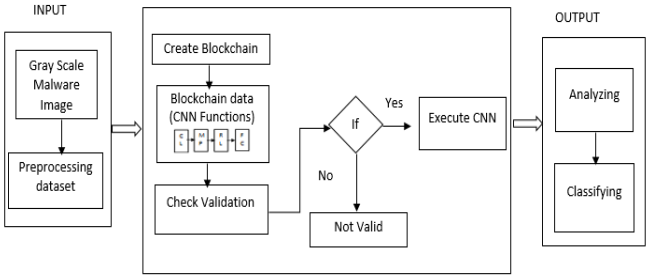

Fig 2. SBC Algorithm Architecture

D. Blockchain

Is a distributed model which stores the data between blocks and according to this project each function of CNN stored as data in blocks. The stored data is immutable and permanent that can be easily verified. The blockchain is mostly used in crypto-currencies and basically built from blocks; therefore it is not related directly to CNN in prior. Recently there are many researches in this part of different fields such as health care, smart energy and grids that shows blockchain having good potential and significant output.

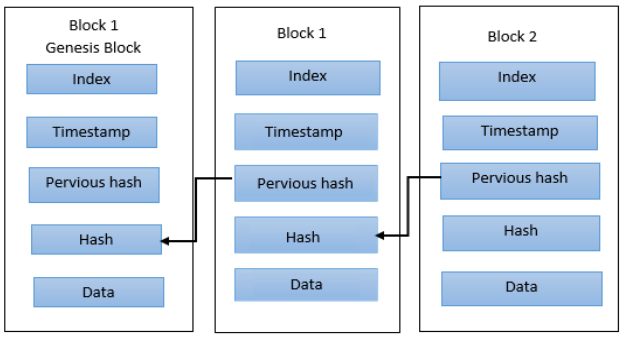

Fig 3. Blockchain Structure

The blockchain structure determined in Fig 3 is described as follows [11]:

- **Data**: The stored data in blockchain depends on the application. In this model, the stored data in each block is the Layer of convolution neural network components such as convolution and max-pooling function.

- **Hash**: A hash function takes any length of input and generates the output with fixed length and unique. The output would be different if a single value of input is modified and no matter the change is big or small, for instance if someone modified a single character of the convolution neural network layer which is hashed in the block then the modified block would have different hash values completely. This increased and improved the trust of data saved in blockchain.
- **Pervious Hash**: this is the hash value of the previous block which is stored in the current block to make sure the validation of block is correct. The same process would continue up to the end of blockchain and each of the pervious hash value will combine with the current hash value of block.
- **Timestamp**: It is used to record the time of creating of the block. This is a method to track the modification or creation time of the block in a secure way.

E. Convolution Neural Network

- **The convolutional layer:** This layer is the main part of a CNN. It is extracting the features from the input image and sending it to the next level, then the extracted features values will multiply with the original pixel values in the filter part. Here, we used fifth convolution filters of size 32,64,128,64,32 and the vector size is 5 for each convolution layer.

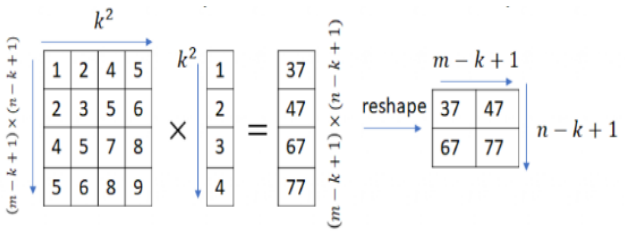

Fig 5. Convolution layer

As shown in Fig 5, this modifies how the convolution layer is working. And in this step, the function will move to each possible position feature on the image and filter it and then line up the feature of image, multiply each image pixel by the corresponding feature pixel and sum it up together and divide by the total number of pixels in the feature and in the end it will create a map to put the value of the filter. After convolving a kernel size of N over the image of M with the stride of S the output size will be:

$$output = \frac{M-N}{S} + 1$$

- **Rectified linear unit (ReLU) layer:** In this layer, all the negative values will be removed from the filtered image and will replace it with zero. It will be done to avoid the values form summing up to zero. Transformed function is activated only when a node if the input is above a certain quantity, while the input is below the zero then the value will be zero.
- **Pooling layer:** Pooling is a non-linear method of down-sampling. For implementing the pooling layer there are many non-linear functions like the minimum, maximum and the average but the maximum is the most common one. In the maximum pooling function the image will partition into a group of non-overlapping rectangles and the maximum value is the output of each sub-region and in this algorithm for reducing the dimensionality of the data, the factor value is 5.
- **Fully-Connected layer:** The responsibility of this layer is to classify the image into a label by using the output from the pooling process layer. The filter of shrunk image would put into a single list. To identify the most accurate weights, the fully connected layer goes through its own back propagation process. To prioritize the most appropriate label, it is according to each neuron weights received. The classification will be done accordingly towards the end of the process. The fully connected layer is a classic multi-layer resultant in the output layer with a softmax activation function and after this we used dropout method to prevent overfitting.

IV. SECURE BLOCKCHAIN CONVOLUTION (SBC) ALGORITHM

- **Data:** Gray scale Malware image input (**N1**..**Na**), **T** target label, $\mathbf{w_i}$, $\mathbf{b_i}$, $\mathbf{act_i}$ is the weight, bias, and activation function of the $\mathbf{i^{th}}$ layer of CNN. **Bi** is the number of blockchain that each **layeri** of convolution will store in the block.
- **Result:** Trained and Tested CNN method to detect the malware image and store each layer of CNN in blocks of blockchain to protect the method from human intervention.

Secure Blockchain Convolution Algorithm:

$layer_i$ = conv_2d(w_i, b_i, act_i), max pooling(w_i, b_i) + $hash_i$
if ($layer_i$ == $Hash_i$) then
 return applyCNN()
else
 return "here is some unauthorized change"

Function applyCNN{
 For i=1 to apoch_size **do**
  While (training malware image number) **do**
   - Compute the **i** hidden activation matrices $\mathbf{W_1}$ ……..$\mathbf{W_i}$ using the weight of (32,64,128)
   - Down sample the **i** hidden activation matrices $\mathbf{b_1}$…….$\mathbf{b_i}$ by a factor of 5.
   - Compute Relu and softmax activation vector.

   If (output_model == 1) **then**
    Return Benign
   Else
    Return Malware

  End
 End
}

SBC Algorithm Description: The algorithm has two parts. The first part is to create the blockchain and check the validation of each hash value of the block.

If it is valid then it will execute the next step which is CNN algorithm.

The second part of the algorithm is execution of the CNN algorithm that will analysis the malware image and classify it according to the prediction output and each steps of CNN algorithm explained already.

V. IMPLEMENTATION AND RESULT

In this section, the experiment result of the robustness and validity of the purposed algorithm is discussed. Here the experiment of this project is deployed in python3.7. We had performed 30 iterations. In every layer, different filter values are used and the rectified linear unit (ReLU) is used as activation function. This algorithm takes less time for the calculation process of training and the accuracy is higher.

```
Training Step: 25  | total loss: 0.01943 | time: 1.288s
| Adam | epoch: 025 | loss: 0.01943 - acc: 0.9974 | val_loss: 0.00036 - val_acc: 1.0000 -- iter: 46/46
--
Training Step: 26  | total loss: 0.01429 | time: 1.401s
| Adam | epoch: 026 | loss: 0.01429 - acc: 0.9981 | val_loss: 0.00071 - val_acc: 1.0000 -- iter: 46/46
--
Training Step: 27  | total loss: 0.01062 | time: 1.332s
| Adam | epoch: 027 | loss: 0.01062 - acc: 0.9986 | val_loss: 0.00158 - val_acc: 1.0000 -- iter: 46/46
--
Training Step: 28  | total loss: 0.00796 | time: 1.471s
| Adam | epoch: 028 | loss: 0.00796 - acc: 0.9989 | val_loss: 0.00372 - val_acc: 1.0000 -- iter: 46/46
--
Training Step: 29  | total loss: 0.00603 | time: 1.297s
| Adam | epoch: 029 | loss: 0.00603 - acc: 0.9992 | val_loss: 0.00881 - val_acc: 1.0000 -- iter: 46/46
--
Training Step: 30  | total loss: 0.00460 | time: 1.510s
| Adam | epoch: 030 | loss: 0.00460 - acc: 0.9994 | val_loss: 0.01938 - val_acc: 0.9836 -- iter: 46/46
```

Fig 6. Loss and Accuracy of the output Algorithm

According to the Fig 6, the experiment done has been achieved a significant output in comparison to the previous methods.

Table 1 Accuracy and Loss of SBC Algorithm

Accuracy	0.99
Loss	0.00460

The accuracy is increased in each approach and the final accuracy is 0.99 as shown in the above table and the loss is 0.00460 in the last iteration.

Fig 7. Malware and Benign image Result

Fig 7. Here, it selects few images after getting the target result to show how it was accurate by the mentioned algorithm. It is predicted to be accurate and positively there are no false depicts of any results.

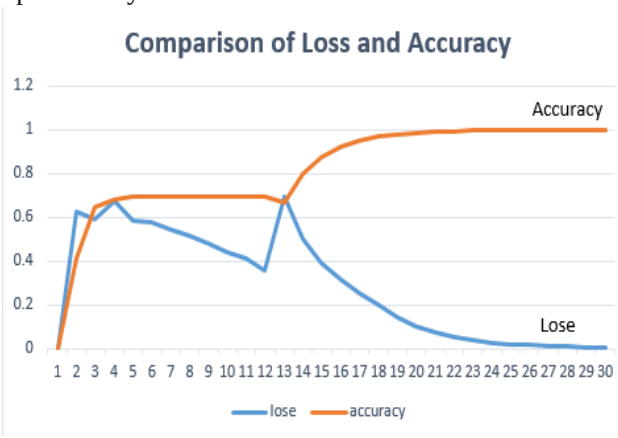

Fig 8 Loss and Accuracy Result Graph

Fig 8. In the above graph it is representing the loss and accuracy of the output result in the form of graph. It shows how accuracy is changed in each epoch and achieved the target result that is 0.99 and loss is 0.0046.

VI. CONCLUSION

In this paper, an approach is presented to detect and classify the malware image in a secure way and less time using convolution neural network method for detection and blockchain technology for preventing from human intervention. According to the experiment that has been achieved, it shows a significant output than the other methods as it is represented above. The accuracy is increased in each approach and the final accuracy is 0.99 as shown in the result, it is predicted to be accurate and positively there are no false depicts of any results mentioned. On the other hand the blockchain technology is also applied in this approach which increases the security. If any interception occurs during the calculation in any block then all the hash values would change and method would return a false value.

REFRENCES

1. M. Hassen, M. M. Carvalho and P. K. Chan, "Malware classification using static analysis based features," 2017 IEEE Symposium Series on Computational Intelligence (SSCI), Honolulu, HI, 2017, pp. 1-7.
2. J. Su, D. V. Vasconcellos, S. Prasad, D. Sgandurra, Y. Feng and K. Sakurai, "Lightweight Classification of IoT Malware Based on Image Recognition," 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC), Tokyo, 2018, pp. 664-669.
3. P. Prasse, L. Machlica, T. Pevný, J. Havelka and T. Scheffer, "Malware Detection by Analysing Network Traffic with Neural Networks," 2017 IEEE Security and Privacy Workshops (SPW), San Jose, CA, 2017, pp. 205-210.
4. A. De Paola, S. Gaglio, G. L. Re and M. Morana, "A hybrid system for malware detection on big data," IEEE INFOCOM 2018 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Honolulu, HI, 2018, pp. 45-50.
5. J. Gu, B. Sun, X. Du, J. Wang, Y. Zhuang and Z. Wang, "Consortium Blockchain-Based Malware Detection in Mobile Devices," in IEEE Access, vol. 6, pp. 12118-12128, 2018.
6. Sarvamblog, 2014, MiltiFamilyMalwareDataset, Aug2014 <https://sarvamblog.blogspot.com/2014/08/supervised-classification-with-k-fold.html>
7. D.Gibert," Convolutional neural networks for malware classification". University Rovira i Virgili, Tarragona, Spain.2016

8. Kolosnjaji, B., Zarras, A., Webster, G. and Eckert, C.," Deep learning for classification of malware system call sequences" 2016, December,Advances in Artificial Intelligence Lecture Notes in Computer Science (pp. 137-149). Springer, Cham.
9. M. Ijaz, M. H. Durad and M. Ismail, "Static and Dynamic Malware Analysis Using Machine Learning," 2019 16th International Bhurban Conference on Applied Sciences and Technology (IBCAST), Islamabad, Pakistan, 2019, pp. 687-691.
10. M. Abdelsalam, R. Krishnan, Y. Huang and R. Sandhu, "Malware Detection in Cloud Infrastructures Using Convolutional Neural Networks," 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), San Francisco, CA, 2018, pp. 162-169.
11. T. T. Huynh, T. D. Nguyen and H. Tan, "A Survey on Security and Privacy Issues of Blockchain Technology," 2019 International Conference on System Science and Engineering (ICSSE), Dong Hoi, Vietnam, 2019, pp. 362-367.
12. S.Saad, W.Briguglio, H.Elmiligi,"The curious case of machine learning in malware detection," Proceedings of the 5th International Conference on Information Systems Security and Privacy, arXiv preprint arXiv: 1905.07573, May 2019.
13. Y.Ye, T.Li, D.Adjeroh,and S.S.Iyengar, "A survey on malware detection using data mining techniques," ACM Computing Surveys (CSUR), 50(3), pp.1-40,June 2017.
14. D.S .Berman, A.L.Buczak, J.S.Chavis and C.L.Corbett, "A survey of deep learning methods for cyber security," Information, 10(4), p.122.April 2019
15. E.Gandotra, D.Bansal and S.Sofat," Malware analysis and classification:A survey," Journal of Information Security, 2014.
16. G. Apruzzese, M. Colajanni, L. Ferretti, A. Guido and M. Marchetti, "On the effectiveness of machine and deep learning for cyber security," 2018 10th International Conference on Cyber Conflict (CyCon), Tallinn, 2018, pp. 371-390.
17. A.Goel, A.Agarwal, M.Vatsa, R.Singh and N.Ratha," Deepring: Protecting deep neural network with blockchain,"In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops (pp. 0-0).2019
18. R. Graf and R. King, "Neural network and blockchain based technique for cyber threat intelligence and situational awareness," 2018 10th International Conference on Cyber Conflict (CyCon), Tallinn, 2018, pp. 409-426.
19. R. Kumar, X. Zhang, W. Wang, R. U. Khan, J. Kumar and A. Sharif, "A Multimodal Malware Detection Technique for Android IoT Devices Using Various Features," in IEEE Access, vol. 7, pp. 64411-64430, 2019.

AUTHORS PROFILE

Sharifa Nawroozi, is a post-graduate student at the department of Information Security, School of Computer Science and Engineering, Vellore Institute of Technology (VIT), Vellore, India. Her research interests include Deep learning, Cyber security, Blockchain Technology and Penetration Testing.

Dr. RA. K. SaravanaGuru, He has been associated with Vellore Institute of Technology (VIT), Vellore since June 2004 and presently working as Associate Professor in School of Computer Science and Engineering (SCOPE) and Assistant Dean Academics. He has sixteen years of teaching experience. He completed his Ph.D. in Computer Science and Engineering in the field of context aware middleware for vehicular adhoc network. His area of interest include context aware systems, middleware, web services, VANET and data science.