Academic City University College – Accra Ghana
Society for Multidisciplinary & Advanced Research Techniques (SMART) Africa
Tony Blair Institute for Global Change
FAIR Forward – Artificial Intelligence for All - Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

Accra Bespoke Multidisciplinary Innovations Conference (ABMIC)

& The Africa AI Stakeholders' Summit 14th December, 2021

An Exploratory Study of Recurrent Neural Networks for Cybersecurity

Omotosho, Oluwabusayo I.
Department of Computer Science
Ladoke Akintola University of Technology
Ogbomoso, Nigeria
E-mail: bomotosho@gmail.com
Phone: +2348032989132

Baale Abimbola Adebisi
Department of Information Systems
Ladoke Akintola University of Technology
Ogbomoso, Nigeria
E-mail: aabaale@lautech.edu.ng
Phone: +2348035700116

Oladejo, Olajide Ademola.
Department of Computer Science
University of Ibadan
Ibadan, Nigeria
Email: programmerolajide@gmail.com
Phone: +2348020837226

Adelodun, Felicia Ojiyovwi.
Department of Computer Studies
The Polytechnic Ibadan
Ibadan, Nigeria
Email: adelodunfelicia@gmail.com
Phone: +2348020837226

Proceedings Citation Format

Omotosho, O.I. Baale, A.A. Oladejo, O.A. & Adelodun, F.O. (2021): An Exploratory Study of Recurrent Neural Networks for Cybersecurity. Proceedings of the Accra Bespoke Multidisciplinary Innovations Conference. University of Ghana/Academic City University College, Accra, Ghana. December 2021. Pp 197-204 www.isteams.net/ghanabespoke2021.
DOI https://doi.org/ 10.22624/AIMS/ABMIC2021P15

An Exploratory Study of Recurrent Neural Networks for Cybersecurity

Omotosho, O.I. Baale, A.A. Oladejo, O.A. & Adelodun, F.O

ABSTRACT

The consistent increase in the rate of cyber threats, cyber-attacks and malwares in recent times obviously demonstrates that current countermeasures don't seem to be enough to defend against it, as attackers are becoming sophisticated in their approach by cunningly developing systems that automatically rewrite and reorder their malware to avoid detection. And typical machine learning approaches, which learn a classifier based on a handcrafted feature vector are not sufficiently robust to such reordering. Hence, the need for an efficient automated cyber security solutions that leverage deep neural networks. This paper presents a study of Recurrent Neural Networks (RNNs) potency for combating cyber threats, cyber-attacks and new variants of malware. The experiment conducted shows that RNN with Long Short Term Memory (LSTM) performed very well more than the classical machine learning algorithms (SVM and Random Forest) at 99.70%, 98.55%, and 99.42% accuracy, respectively. This is possible because RNNs have in-built memory capability that can remember several prior states, and implicitly extract the salient features, hidden complex structure and complex sequential relationship in data which help in achieving better accuracy.

Keywords: Cybersecurity, Deep Learning, Recurrent Neural Networks (RNNs), LSTM, Machine Learning, Malware Detection, SVM, Random Forest.

1. INTRODUCTION

Attacks against cyber networks in recent times are increasing within the cyber space at a rate outpacing cyber defenders' ability to write and deploy new signatures to detect these new attacks, threats and malwares [6]. And as such advance security measures are needed to be taken to scale back or avoid the amount of cyber-attacks and threats [9]. Although, there are deluge of tools – like firewalls, antivirus software, intrusion detection systems (IDSs), and intrusion protection systems (IPSs) - that work in stacks to defend against attacks and detect security breaches [3]. However, attackers are still at vantage because they only need to find one loophole in the system needing protection. And as the number of systems connected to the internet increases, the attack surface also widens, leading to higher risk of attack [3] [9]. Additionally, attackers are becoming more sophisticated, by developing zero day techniques and malware variants that circumvent security measures, enabling them to linger for longer periods without notice [8].

Numerous attacks such as D-Dos attacks, Man in the middle, information escape, PROBE, User-To-Root, Remote-To-Local, etc. are utilized by hackers or adversaries to gain illegal/unapproved access to any websites, non-public networks, and information in our personal computers [9]. Therefore, intelligent and efficient cyber defense solution that will leverage machine/deep learning should be put in place to wade off threats and attacks that evolve in an ever threatening cyber landscape and safeguard the security of the same. Cyber security is the science of technologies, processes, and practices designed to shield networks, devices, programs, and information from attacks, damage, and or illegal access [9].

With advances in Machine Learning algorithm development, Neural Network based Deep Learning approaches could be applied to cyber security to detect new variants of malware and previously unknown zero-day attacks. Deep Learning is a sub module of machine learning, and it is also called Deep Neural Networks (DNNs) [1]. The adoption of deep learning in cyber security will definitely help in correlating events, identifying patterns, and detecting previously unknown attacks and anomalous behavior to fortify the security posture/outlook of any defense program and reduce the unknown attack rate.

Fortunately, today's deep learning showed stellar performance in numerous longstanding artificial intelligence (AI) problems such as natural language processing, computer vision, speech recognition [11]. And in recent times, deep learning approaches have been applied to diverse use cases of cyber security ranging from intrusion detection, traffic analysis, android malware and network malware analysis to mention but a few. It has the ability to detect cyber-attacks and threats by learning the complex salient structure, hidden sequential relationships and hierarchical feature representations from an extensive set of security data by passing the information to more than one hidden layers [6]. Hence, Cyber security is positioned to take advantage of machine leaning/deep learning to boost cyber-attacks/threats and malware detection rate, sorting events, acknowledge breaches and alert organizations to security challenges.

In this paper, an evaluation of RNNs would be carried out for one cybersecurity use case – malware domain detection (malwares generated from domain algorithm (DGA)) – and compared with classical machine learning algorithms. DGA is a subroutine that enables malware with new domains on demand or on the fly.

2. RECURRENT STRUCTURE

RNNs belong to a family of neural networks that work/run on sequential data [1] [3]. Classical neural network presumes that all inputs and outputs are not dependent of each other. Typically, it receives input from two sources; one is from present and the other from past. The preceding information is stored in the self-recurrent loop mostly called recurrent.

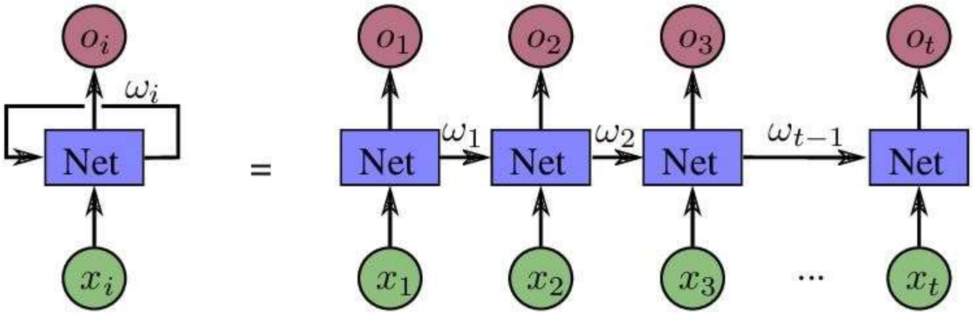

Figure 1: Recurrent Neural Network Structure.

The left is the classical RNN structure. The right part is the unfolding version where information from the past is transferred to the later time step. [10]

Given an input sequence $X = (x1, x2. \ . \ . \ xT)$, the transition function for RNN model can be mathematically expressed as follows:

$$ht = gn\ (wxhXt + whhht-1 + bh) \qquad (1)$$
$$ot = gn\ (wohht + bo) \qquad (2)$$

where *xt* denotes an input vector, *gn* denotes non-linear activation function, *ht* connotes hidden state vector, *ot* denotes output vector and terms of *w* and *b* implies weights and biases respectively.

RNN results in vanishing and error gradient when it is memorized to recall information for longer time steps [1] [3] [4]. To minimize the vanishing and gradient problem, gradient clipping was introduced [1]. Later, LSTM was proposed [1] [4] [5]. This has a memory block rather than the simple unit in RNN that helps to store information. The memory block consist of a memory cell contained by input, output and forget gates. Both the gates and cell state provides interactions. And the primary function of gate is to control the information of the memory cell. These gates help the LSTM network to retain and remember information for longer duration than the RNN.

Given an input sequence $X = (x1, x2. \ . \ . \ xT)$, the transition function for LSTM model can be mathematically defined as follows:

$$ft = \sigma\ (Wf\ .[ht-1, xt] + bf\ ) \qquad (3)$$
$$it = \sigma\ (Wi.[ht-1, xt] + bi) \qquad (4)$$
$$ct = \tanh\ (Wc.[ht-1, xt] + bc) \qquad (5)$$
$$ot = \sigma\ (Wo[ht-1, xt] + bo) \qquad (6)$$
$$ht = ot * \tanh\ (ct) \qquad (7)$$

where *xt* connotes an input vector, *ht* connotes hidden state vector, *ct* connotes cell state vector, *ot* connotes output vector, *it* connotes input vector and *ft* conotes forget state vector and terms of *w* and *b* connotes weights and biases respectively.

Typically, LSTM is a complex network. Recently, minimized version of LSTM called gated recurrent unit (GRU) was introduced [1]. GRU is similar to LSTM but more computationally efficient and easier to train than LSTM [3] because it has only two gates; update and reset gate. In GRU, both forget and input gates functionality found in LSTM are combined to form an update gate. The update gate indicates the amount of past memory to be kept in GRU. In recent past, RNN variant, identity RNN was proposed which initialize the appropriate RNNs weight matrix using an identity matrix or its scaled version, and use Rectified Linear Unit (*ReLU)* as non-linear activation function to counteract vanishing and exploding gradient problem [1].

3. MATERIALS AND METHODS

For domain malware classification, five different models (SVM, Random forest, RNN and RNN with layer and Batch normalization) were implemented for comparison sake. The data set was gotten from DGA-Domains-from-datadrivensecurity.info, with the total size of 1.6G. The experiment was run for 15 epoch and 10 fold cross validation was used. The dataset was splitted into 70/30 for training and testing respectively.

The data consist of 4 columns (host, domain, class, and subclass). For the purpose of this study, the host and class columns were used. The host contains all the domain including the top level domain like .com, .org, etc. so, the host was used instead of domain column which does not include the top level domain. The "class" columns is considered the target. It contains two classes "dga" and "legit". "dga" is the malware domain and "legit" is the legal domain and consists of 81261 and 52665 parameters respectively. Firstly, feature extraction from the host data was done for SVM and Random Forest models. For features extraction TF-IDF (Term Frequency – Inverse Document Frequency) was used. So, the SVM and Random Forest receive the extracted feature from the TF-IDF as input. The shape of the extracted feature from each sample is (39x1). Thus, the input of SVM and Random Forest is (39X1) and the output is binary (0 and 1). 1 for 'dga' or malware domain and 0 for "legal/legit" domain.

Different data preparation methods for the RNN models were used, with the input tokenized. The host data was padded for fix input for the model and was post padded should the character length be less than 55. The maximum length of each sequence was 55.
Layer, and batch normalization was used in between fully connected layers, and regularization to obviate and speed up the RNN model training and drop out (0.001) was adopted to avoid overfitting. The RNN models input is a sequence of shape (55 X 1), and the output of the RNN models is in range (0, 1) because the activation function is sigmoid. And to get the final classes, the results > 0.5 as 1, and < 0.5 as 0, was used.

4. EXPERIMENTS AND RESULTS

The model was trained, validated, and tested with the preprocessed dataset on ASUS TUF Gaming FX705GM with the following configurations: Graphics Processing Unit (GPU) 1xTesla K80, computer 3.7, 12GB (11.439GB Usable) GDDR5 VRAM, Intel Processors Core(TM) i7-8750H 8th Gen. CPU @2.20Ghz (No Turbo Boost), 45MB Cache, RAM 12.6 GB Available, Disk 320 GB Available. The model was implemented using Python programming language, Tensor Flow as the backend and Keras library in Python 3.7.

4.1. Evaluation Metric

Accuracy evaluation metric was used in order to evaluate the proposed model. It is the proportion of the total number of predictions that were correctly classified i.e. the ratio of observation correctly predicted to the total observation.

$$ACC = (TP + TN) / (FP + FN + TP + TN) \qquad (8)$$

Where True Positive rate (TP) and True Negative rate (TN) are correctly classified while False Positive (FP) and False Negative (FN) are correctly misclassified.

4.2. Experimental Results

The model under study (Recurrent Neural Networks) was evaluated against classical machine learning classifiers; SVM and Random Forest on domain generated algorithm's (DGAs) Cyber security use case. The three models were trained and tested on the same dataset (Domain malware). The detailed results and graphs of the proposed RNN and other machine learning models on the use case are displayed in the table 1 and figures below.

Table 1: Summary of Test Results

Algorithms	Task Name	Accuracy (%)	Precision	Recall	F- score
SVM	Domain malware classification	0.985	0.699	0.489	0.389
Random forest	Domain malware classification	0.994	0.761	0.992	0.95
RNN with LSTM	Domain malware classification	0.997	1.00	1.00	1.00
RNN (Layer Normalization)	Domain malware classification	0.994	0.98	0.88	0.99
RNN (Batch Normalization)	Domain malware classification	0.946	0.95	0.94	0.94

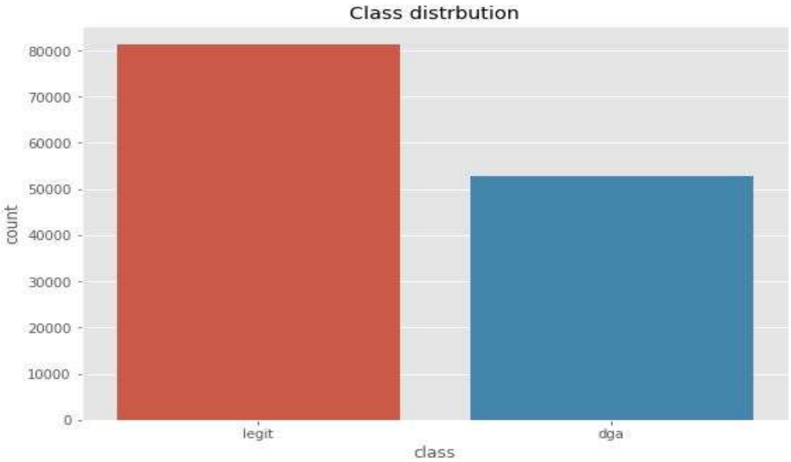

Figure 2: dataset class distribution

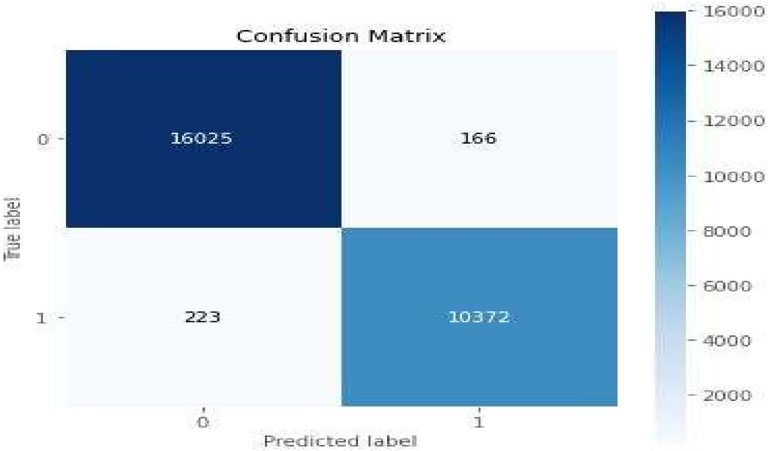

Figure 3: The confusion matrix of support vector machine (SVM)

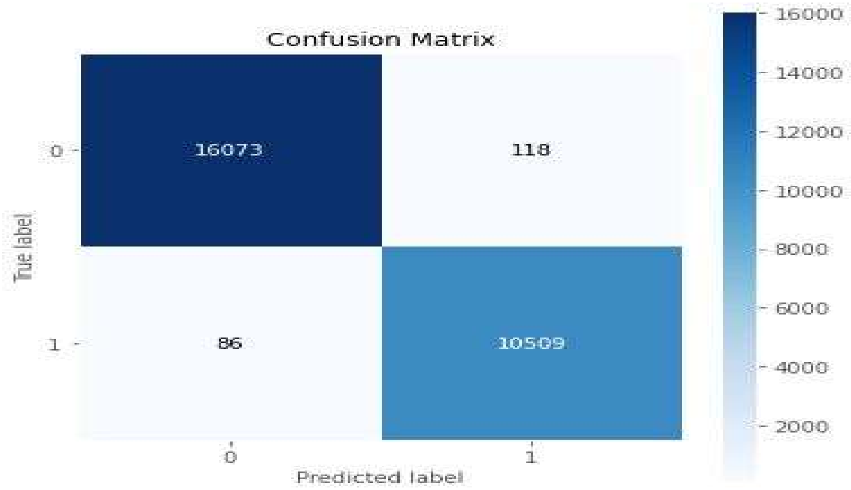

Figure 4: The confusion matrix of Random Forest

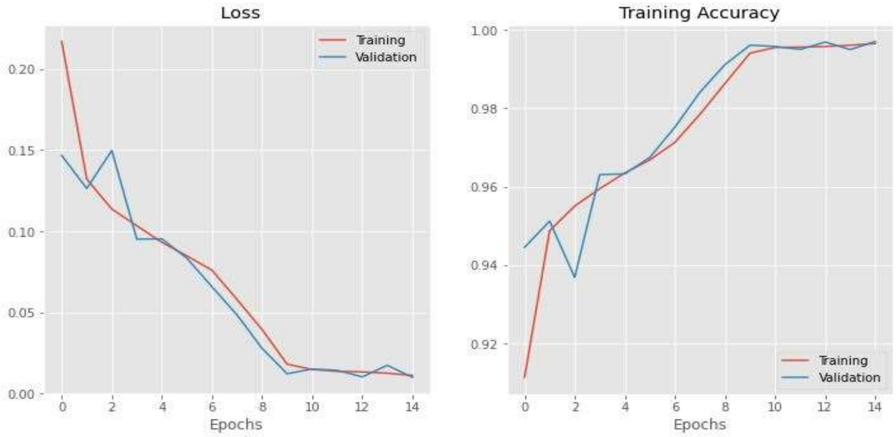

Figure 5: RNN training and validation accuracy

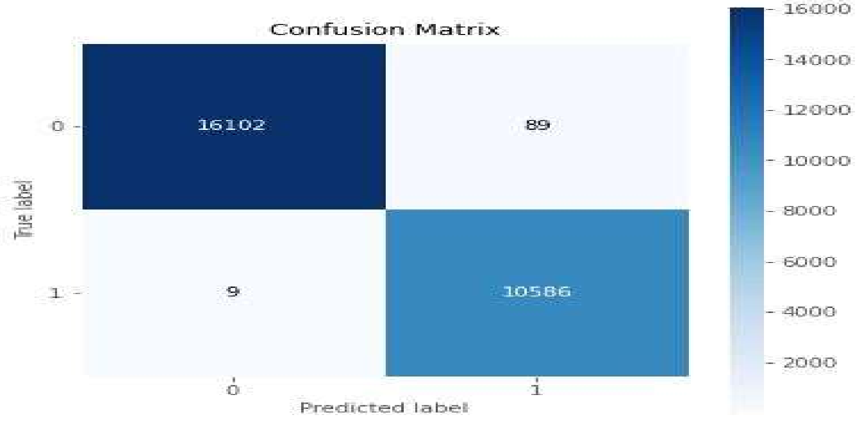

Figure 6: The confusion matric of RNNs

5. CONCLUSIONS

This paper presents a study of recurrent neural networks (RNN) model for Cybersecurity using domain malware detection as the application area. The performance of RNNs and other classical machine learning classifiers are studied and evaluated for domain malware classification cyber security use case and compared. From this study, it is seen that RNN came up with a better accuracy than the classical machine learning classifiers (SVM and Random forest). This is possible because RNNs have in-built memory capability that can retain and recall several prior states, and implicitly extract the salient features, hidden/underlying complex structure and complex sequential relationship in data which help in achieving better accuracy.

Thus, it will be helpful in building a real time application for analyzing malicious activities over the network.

REFERENCES

[1] Le Cun Y, Bengio Y, Hinton G (2015) Deep learning. Nature 521(7553):436

[2] Zhu N Y, Liu X, Liu Z Q, Hu K, Wang Y K, Tan J L, et al. Deep learning for smart agriculture: Concepts, tools, applications, and opportunities. Int J Agric & Biol Eng, 2018; 11(4): 32–44.

[3] Daniel S. Berman, Anna L. Buczak, Jeffrey S. Chavis and Cherita L. A Survey of Deep Learning Methods for Cyber Security Corbett Information 2019, 10, 122; doi:10.3390/info10040122

[4] Hochreiter, S.; Schmidhuber, J. Long short-term memory. Neural Comput. 1997, 9, 1735–1780. [CrossRef]

[5] Sak H, Senior A W. Processing acoustic sequences using long short-term memory (LSTM) neural networks that include recurrent projection layers. U.S. Patent No. 9,620,108. 11 Apr. 2017.

[6] R. Vinayakumar, K. P. Soman, Prabaharan Poornachandran and S. Akarsh Application of Deep Learning Architectures for Cyber Security, Advanced Sciences and Technologies for Security Applications, 2019 https://doi.org/10.1007/978-3-030-16837-7_7

[7] Razvan Pascanu, Jack W Stokest, Hennineh Sanossian, Mady Marinescu, Anil Thomas (2015), Malware Classification with Recurrent Networks 978-1-4673-6997-8/15/$3l.00 ©2015 IEEE

[8] Mohammed Harun Babu R, Vinayakumar R, Soman KP, RNNSecureNet: Recurrent neural networks for Cyber security use-cases.

[9] R. Devakunchari, Sourabh, Prakhar Malik, A Study of Cyber Security using Machine Learning Techniques, International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8, Issue-7C2, May 2019

[10] lei tai, Ming liu, Deep learning in Mobile Robotics- from perception to control systems: A Survey on Why and Why not. Journal of Latex Class File Vol., 14. NO. 8. August 2015

[11] Vinayakumar R, Soman KP, Prabaharan Poornachandran, A Comparative Analysis of Deep learning Approaches for Network Intrusion Detection Systems (N-IDSs), Article in International Journal of Digital Crime and Forensics, July 2019 *doi: 10.4018/ijdcf.2019070104*