Open Journal of Physical Science (OJPS)
ISSN: 2734-2123
Article Details:
DOI: 10.52417/ojps.v2i2.237
Article Ref. No.: OJPS0202001-200
Volume: 2; Issue: 2, Pages: 01 - 09 (2021)
Accepted Date: 9th August, 2021
© 2021 George & Uppin

Open Journals Nigeria (OJN)
Open Access | Bi-annual | Peer-reviewed
www.openjournalsnigeria.org.ng
editorial@openjournalsnigeria.org.ng

Open Journal of Physical Science
Open Access | Peer reviewed | Biannual
ISSN: 2734-2123
2021 | Vol. 2; Iss. 2

RESEARCH ARTICLE **OJPS0202001-200**

A PROACTIVE APPROACH TO NETWORK FORENSICS INTRUSION (DENIAL OF SERVICE FLOOD ATTACK) USING DYNAMIC FEATURES, SELECTION AND CONVOLUTION NEURAL NETWORK

[*1]George, G. & [2]Uppin, C.

[1&2]*Department of Computer Science, Faculty of Computing and Applied Sciences, Baze University, Jabi Abuja, Nigeria*
[*]***Corresponding Author Email:*** *gilbert.george@bazeuniversity.edu.ng*, *cv.uppin@bazeuniversity.edu.ng*

ABSTRACT

Currently, the use of internet-connected applications for storage by different organizations have rapidly increased with the vast need to store data, cybercrimes are also increasing and have affected large organizations and countries as a whole with highly sensitive information, countries like the United States of America, United Kingdom and Nigeria. Organizations generate a lot of information with the help of digitalization, these highly classified information are now stored in databases via the use of computer networks. Thus, allowing for attacks by cybercriminals and state-sponsored agents. Therefore, these organizations and countries spend more resources analyzing cybercrimes instead of preventing and detecting cybercrimes. The use of network forensics plays an important role in investigating cybercrimes; this is because most cybercrimes are committed via computer networks. This paper proposes a new approach to analyzing digital evidence in Nigeria using a proactive method of forensics with the help of deep learning algorithms - Convolutional Neural Networks (CNN) to proactively classify malicious packets from genuine packets and log them as they occur.

Keywords: *Cybercrime, Deep-Learning, Digital Forensic, Denial of Service Attacks, Network-monitoring system, Network Forensics*

INTRODUCTION

Nowadays the increased usage of mobile devices and smart wares has dramatically increased the generation of data, usage of these devices has become our everyday lives. These smart devices hold valuable information that includes; bank records, private and commercial data which are transferred via computer (wired and wireless) networks and these networks are vulnerable to attacks such as ‘man in the middle attacks and spoofing attacks’ of which form a major part of criminal activities (Chowdhury et al., 2016). The number of digital crimes also increase with the introduction of new technologies, such criminals find new ways of attacking vulnerabilities in these applications.

Base on (*2020 Internet Crime Report*, n.d.) the top 20 countries with most cybercrime victims index, Nigeria ranked 16th with 443 crimes recorded, while countries like the United Kingdom and India were top of the list with an average crime of 216,633 crimes recorded in the UK and 5399 in Canada. Nigeria has a large population of over 150 million people and of that 104.4 million people use the internet, with the large amount of people on the internet, there is an opportunity of cyber criminals to take advantage of these amounts.(*Digital in Nigeria: All the Statistics You Need in 2021 — DataReportal – Global Digital Insights*, n.d.) Currently, cybercrime is committed by people ranging from as young as 10 years to as old as 60 years. From our study, we discovered that as much as 2.1 trillion dollars was lost to cyber theft in 2019 and it is estimated by the end of 2021 the rate will increase to as much as 6 trillion dollars. (Isacenkova *et al.*, 2013)

Cyber-attacks cost on average $123,00 per Organization in the United States of America, according to (BBC, n.d.) the report cost of solving a cyber-attack is about 5.6 million dollars in the United States of America, this is because the current methods of analyzing cybercrime are expensive, time-consuming, involves a lot of human resources and interventions. (Zamani & Movahedi, 2013).

AIM

The paper aims to propose the combination of a deep learning algorithm (Convolution Neural Network) and traditional Intrusion detection and network monitoring systems to create a proactive forensics framework for network analysis.

OBJECTIVES

To Propose a proactive digital forensic framework with the use of a deep learning technique for improved performance in digital networking forensics.

BACKGROUND OF LITERATURE

Network forensics can be classified into two approaches which are:

- Proactive network forensics
- Reactive network forensics

Proactive network forensic investigation is a new approach that involves live investigation and deals with the phases of network forensics during an ongoing attack. (Alharbi *et al.*, 2011). Reactive network forensics investigation as the name implies deals with the cyber-crime case after some time usually after the crime has been committed, it is the more traditional method of network forensics and involves the use of more resources including time.

(Ieong, 2006) the Digital Forensics Workshops (DFRWS) provided the first network forensic reactive method as a basic investigation framework that can be applied to network environments and most investigations. The framework comprises six phases of tasks, which are:(Alharbi *et al.*, 2011)

- Identification
- Preservation
- Collection
- Examination
- Analysis
- Presentation
- Decision making

As seen from figure1 below

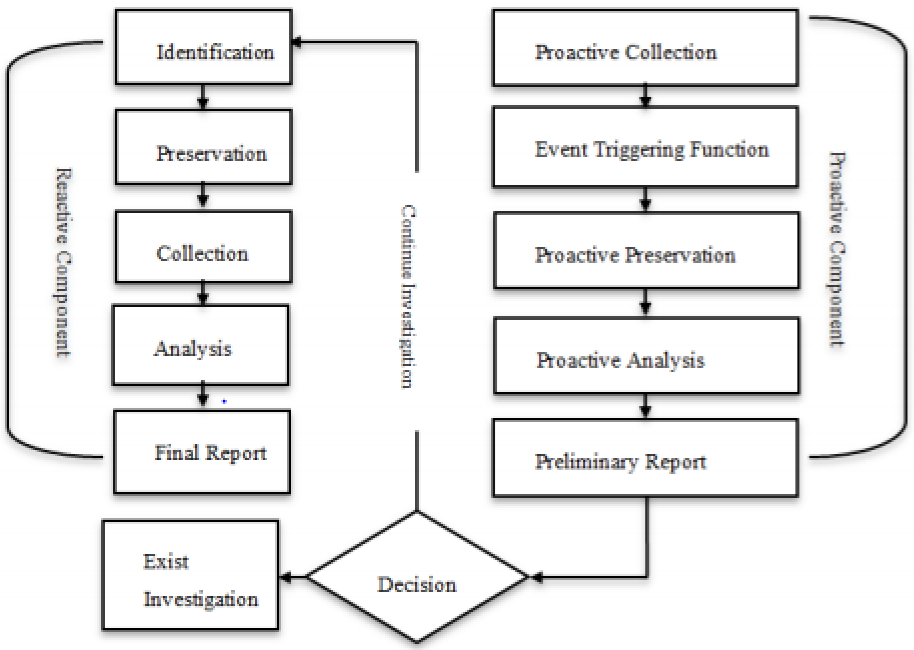


Figure 1: The functional process of proactive and reactive digital forensics investigation system
Source: *(Ieong, 2006)*

Saleem *et al.* in 2014 proposed a new framework/model called Abstract Digital Forensics. The model is made up of nine phases.

- Identification
- Preparation
- Approach strategy
- Preservation
- Collection
- Examination
- Analysis

- Presentation
- Returning evidence

As reported by Alharbi *et al.,* in 2011, proactive network forensics method reduces the resources, time and cost of the investigation by identifying potential evidence as the crime is committed. This is used in preliminary analysis of cybercrime and also it helps to speed up decision-making processes by the organization. According to the proactive network forensic concepts, as mentioned by the first five stages work proactively for the reason that they work during the time the crime is ongoing, the other four stages in the model work after the investigative phase and work as reactive processes (Alharbi *et al.,* 2011).

Convolutional Neural Networks (CNN) are variations of artificial neural networks which was developed to use the insight from locally connected features in the input. It has been widely used in the field of image classifications. CNN is one of the most successful applied algorithms in other research areas such as natural language processing, signal processing and audio classification. (He & Sun, 2014). CNN has recently gotten the attention of cybersecurity experts/researchers and network managers. The use of CNN has been used to detect and classify a diverse range of traffic seen in recent day networks. CNN has been seen to be promising in the field of cybersecurity and can perform both statistical analyses by interpreting traffic metadata features, finding patterns in packets and message contents in network traffic (Millar *et al.,* 2019).

ADVANTAGES OF APPLYING CNN

The first advantage is, the entire input does not have to be processed at once, this is important when working with huge amount of input size (network packets). The second advantage is when there is a transition or repetition of identifying features in the input. This is because where there is a repetition of patterns the algorithm detects it no matter where it may occur. Therefore, if a repeated pattern or local correlation is identified, there is no additional complexity this is known in Artificial Neural Network (ANN) as weight sharing, depending on the application weight sharing can greatly reduce the size of the network and increase its ability to generalize new data. (Millar *et al.,* 2019). The third advantage of CNN is that local receptive fields are more robust to localized noise. In many classification tasks, the input is likely to suffer from noise. CNN are simply neural networks that use local receptive fields. This is done using two specialized layers, which are:

- Convolutional layer
- Pooling layer

A lot of CNN is made up of these two stages. The first uses convolutional and pooling layers to identify local correlation with the input data and allow translation invariance. The first stage can be thought to be the learning and extracting features from the input While the second stage uses fully connected layers to combine the features found in stage one into the overall prediction of which class the input mostly belongs to.

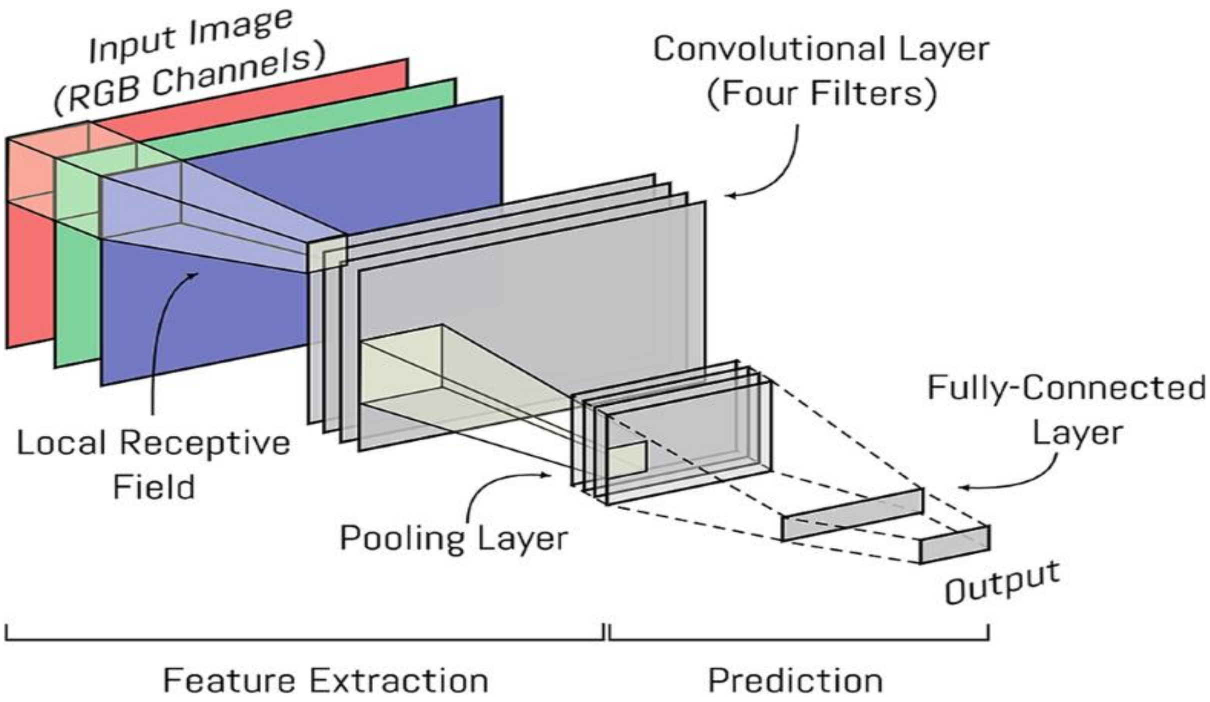


Figure 2: A typical CNN structure for image processing

Source: (Millar *et al.*, 2019)

RELATED WORKS

Network traffic classification characteristically falls into two categories;

- Statistical-based classification: this is where the traffic is classified based on a collection of metadata features, such as the number of packets sent.
- Payload-based classification: this is where the traffic is classified based on the distinct signatures found in the message content of the packet

Table 1: Related works in the application of CNN on Network Packets

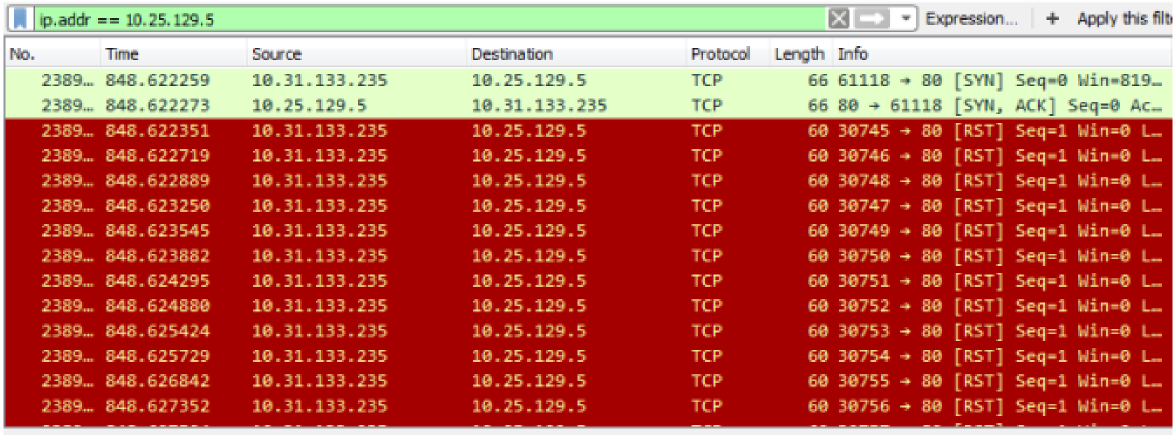
Authors	**Excerpt**
(Wang *et al.*, 2017)	The authors made of use of CNN for payload-based classification where a 28 × 28-pixel image was used to represent the first 784 bytes of the payload content of a traffic flow. Each byte was denoted by a greyscale pixel using the range from black represented using 0 to white which was represented using 255. This provided a one-to-one mapping with the 256-value range of a byte field. Wang *et al.* showed that a 1D-CNN achieved a better classification accuracy than a 2D-CNN on this input representation.
(Millar *et al.*, 2019)	The authors aim to examine convolutional neural network (CNN), and how its application can be adapted to detect and classify malicious network traffic.

GAP IN LITERATURE

Although significant efforts have been taken in the step of digital network forensics, there has not been a proactive methodology that combines DL methods for proactive digital forensic network investigation processes.

METHODOLOGY

The methodology being proposed is the use of deep learning algorithms (Convolutional Neural Networks) to analyze the incoming packets from a network interface in real-time.



ip.addr == 10.25.129.5

No.	Time	Source	Destination	Protocol	Length	Info
2389…	848.622259	10.31.133.235	10.25.129.5	TCP	66	61118 → 80 [SYN] Seq=0 Win=819…
2389…	848.622273	10.25.129.5	10.31.133.235	TCP	66	80 → 61118 [SYN, ACK] Seq=0 Ac…
2389…	848.622351	10.31.133.235	10.25.129.5	TCP	60	30745 → 80 [RST] Seq=1 Win=0 L…
2389…	848.622719	10.31.133.235	10.25.129.5	TCP	60	30746 → 80 [RST] Seq=1 Win=0 L…
2389…	848.622889	10.31.133.235	10.25.129.5	TCP	60	30748 → 80 [RST] Seq=1 Win=0 L…
2389…	848.623250	10.31.133.235	10.25.129.5	TCP	60	30747 → 80 [RST] Seq=1 Win=0 L…
2389…	848.623545	10.31.133.235	10.25.129.5	TCP	60	30749 → 80 [RST] Seq=1 Win=0 L…
2389…	848.623882	10.31.133.235	10.25.129.5	TCP	60	30750 → 80 [RST] Seq=1 Win=0 L…
2389…	848.624295	10.31.133.235	10.25.129.5	TCP	60	30751 → 80 [RST] Seq=1 Win=0 L…
2389…	848.624880	10.31.133.235	10.25.129.5	TCP	60	30752 → 80 [RST] Seq=1 Win=0 L…
2389…	848.625424	10.31.133.235	10.25.129.5	TCP	60	30753 → 80 [RST] Seq=1 Win=0 L…
2389…	848.625729	10.31.133.235	10.25.129.5	TCP	60	30754 → 80 [RST] Seq=1 Win=0 L…
2389…	848.626842	10.31.133.235	10.25.129.5	TCP	60	30755 → 80 [RST] Seq=1 Win=0 L…
2389…	848.627352	10.31.133.235	10.25.129.5	TCP	60	30756 → 80 [RST] Seq=1 Win=0 L…

Figure 3: Showing a DDOS flooding attack in Wireshark

Source: (Sahi *et al.*, 2017)

THE BENEFIT OF OUR MODEL TO NETWORK FORENSICS

1) Efficient on a larger input size: Network traffic is normally characterized by large volumes of traffic. Packets spanning the maximum transmission unit (MTU) of 1500 bytes and network traffic flows using hundreds or thousands of packets are commonly seen in networks interfaces. It is, therefore, necessary to consider how to efficiently evaluate such large input sizes when using neural networks in particular using CNN. Millar *et al.*, 2019)

2) The trainable parameters of a neural network are the parameters that are adjusted while training to reduce its error on the desired output. The most important trainable parameter is the weight of the connections between nodes. Every connection in the neural network has an associated weight. The value of this weight is adjusted during training to determine the significance of the connection to the overall classification. A CNN can considerably reduce the number of trainable parameters of a neural network by using weight-sharing. Weight-sharing allows a trained weight value to be shared between multiple connections in the same layer. (Khan *et al.*, 2021)

3) The computational requirements of maintaining such a large number of trainable parameters for each of these connections would rule out many hardware implementations and could lead to overfitting if there are not enough samples to train on. The reduction in trainable weight parameters as a result of weight-sharing allows a CNN to be much more computationally efficient than other types of neural networks when dealing with larger input sizes. (Millar *et al.,* 2019).

4) In the process of scanning for discrete, local patterns enables a CNN to locate features regardless of where they appear in the input. The benefit of this approach has been shown in speech recognition tasks where the varying speed, tone, and inflexion of a speaker can change the positioning of these identifying features [16]. Malicious network traffic has been shown to exploit similar properties in the size, sequencing, and timing of packets to obfuscate the identifying features of malicious intent. In allowing for variations in the input, a CNN can be robust to certain evasion techniques. CNN could reuse the same patterns it has found in its lower levels of abstraction to quickly generalize to new variants. (He & Sun, 2014)

5) Weight-sharing allows a CNN to identify repetition in the input without adding any additional complexity to the neural network. From a network traffic perspective, similar syntax structures and duplicated packets make repeated patterns in data and communication traffic highly prevalent. (Millar *et al.,* 2019)

OUR PROPOSED MODEL INCLUDES THE STEPS INCLUDED THE MODEL ARE

1) Intrusion detection systems get triggered
2) Wireshark framework dynamically captures the screen and send the images to the CNN model to classify
3) the CNN model classifies if the images are malicious or not and then triggers the following stages of the
    - Stage 1: stores the packets concurrently every second and stores them in a folder
    - Stage2: implements read-only functions on the files to avoid tamper (preservation)
    - Stage 3: conduct a test and logs the report in a text file.
    - Stage 4: human interpretation of the report and decision decision-making

The proposed methodology uses a proactive investigation process. The prepossessing phase uses the concept of machine learning (classification) and pattern making/learning using the CNN model. The alert is provided by a pattern of malicious packets which is already known by the system (in the knowledge base). The pre-processed data is passed to the examination and analysis stage and a detailed preliminary report is created, based on this report a decision is taken. An intrusion detection system will be triggered if there is an abnormality in-network, then the Wireshark network monitoring system begins to capture live packets and then takes screenshots of the packets. The screenshots are then passed to the CNN model to classify if they are malicious, the application store PCAP file them in a file as read-only to avoid tapering by the operating system and then creates a log file and stores important data in it which is in turn, read by a human and then a comprehensive decision making is followed.

EXPECTED HYPOTHETICAL RESULTS

The efficiency and effectiveness of this method is to minimize the cost and time taken during an investigation process and to improve the quality and time of decision-making using artificial intelligence and deep learning. The quality conduct of the approach will resolve criminal cyberattacks and the organizational cases of misconduct using the network forensics stages with a minimum time and low cost. The time and cost fall under managerial issues and most management want to cut down cost and time, in this research, we propose to find an effective and efficient route that could reduce the time and cost. In general, to identify the critical route, our method can be used, which uses a one-time estimate to identify the duration of each stage to complete its activity. The critical route is a path in which a staged activity is accomplished without any delay. The delay of any stage will automatically affect the resolution of the criminal/organizational case. Accordingly, the critical route can be used when the management level is sure about the duration of each phase which our suggested model brings to the table.

CONCLUSION

Most of the existing models in network forensics serve as a guideline in the investigation of cybercrimes, not of them are actually proactive in nature, most without enough information or details on how to analyze the evidence. Therefore, the ambiguity of each stage procedure is an issue that exists in network forensic. This issue exists because investigators have trouble understanding how the stages work and how the outcomes for each stage are accomplished. Substantial time is spent on trying to understand the stages, as the investigators focus on the number and order of stages instead of the main actions inside these stages.

Cyber-crimes committed via networks yield large amount of evidence, using network monitoring and capturing tools this evidence is stored. However, a significant quantity of time is required to discover the real perpetrator. By means of deep learning the time can be considerably minimized in real-time. The current network forensic investigation approach used in practice are reactive in nature, time consuming, costly, and disposed to error as it requires much effort to analyze the overwhelming amount of evidence presented in each case. Furthermore, gathering useful evidence through the reactive approaches is difficult since the evidence is collected right after the detection of the cyber-crime and that take a long time. Therefore, a new approach is needed to analyse evidence and enhance the investigation process. In our proposed model, we employ the use of proactive processes and artificial intelligence to resolve cyber-crime in network forensics. From this, the result of the proposed approach should outperform the generic methods and should be more efficient and effective in terms of time and cost as well as prevention and detection.

FUNDING

This study was sponsored by the monetary contributions of the authors.

CONFLICT OF INTEREST

There is no conflict of interest.

REFERENCES

Alharbi, S., Weber-jahnke, J., & Traore, I. (2011). *The Proactive and Reactive Digital Forensics Investigation Process : A Systematic The Proactive and Reactive Digital Forensics Investigation Process : A Systematic Literature Review*. *August*. https://doi.org/10.1007/978-3-642-23141-4

BBC. (2021, March 12). *Cyber-attack: Europol says it was unprecedented in scale*. Https://Www.Bbc.Com/News/World-Europe-39907965. https://www.bbc.com/news/world-europe-39907965

Digital in Nigeria: All the Statistics You Need in 2021 — DataReportal – Global Digital Insights. (n.d.). Retrieved July 16, 2021, from https://datareportal.com/reports/digital-2021-nigeria

Federal Bureau of Investigation. (2020). *2020 internet crime Report.* https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

He, K. & Sun, J. (2014). Convolutional Neural Networks at Constrained Time Cost. *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, *07-12-June-2015*, 5353–5360. http://arxiv.org/abs/1412.1710

Isacenkova, J., Thonnard, O., Costin, A., Balzarotti, D., & Francillon, A. (2013). Inside the SCAM Jungle: A closer look at 419 scam email operations. *Proceedings - IEEE CS Security and Privacy Workshops, SPW 2013*, 143–150. https://doi.org/10.1109/SPW.2013.15

Ieong, R. S. C. (2006). FORZA – Digital forensics investigation framework that incorporate legal issues. *Digital Investigation*, *3*(SUPPL.), 29–36. https://doi.org/10.1016/J.DIIN.2006.06.004

Khan H, Hanif S, Muhammad B (2021) A survey of machine learning applications in digital forensics. Trends Computer Sci Inf Technol 6(1): 020-024. DOI: 10.17352/tcsit.000034.

Millar, K., Cheng, A., Chew, H. G., & Lim, C.-C. (2019). Using Convolutional Neural Networks for Classifying Malicious Network Traffic. *Advanced Sciences and Technologies for Security Applications*, 103–126. https://doi.org/10.1007/978-3-030-13057-2_5

Sahi, A., Lai, D., Li, Y. A. N., & Diykh, M. (2017). An Efficient DDoS TCP Flood Attack Detection and Prevention System in a Cloud Environment. *IEEE Access*, *5*, 6036–6048. https://doi.org/10.1109/ACCESS.2017.2688460

Saleem, S., Popov, O., & Bagilli, I. (2014). ScienceDirect Extended abstract digital forensics model with preservation and protection as umbrella principles Peer-review under responsibility of KES International. *Procedia Computer Science*, *35*, 812–821. https://doi.org/10.1016/j.procs.2014.08.246

Wang, W., Zhu, M., Wang, J., Zeng, X., & Yang, Z. (2017). End-to-end encrypted traffic classification with one-dimensional convolution neural networks. *2017 IEEE International Conference on Intelligence and Security Informatics: Security and Big Data, ISI 2017*, 43–48. https://doi.org/10.1109/ISI.2017.8004872

Zamani, M., & Movahedi, M. (2013). *Machine Learning Techniques for Intrusion Detection*. http://arxiv.org/abs/1312.2177