10.48047/jocaaa.2024.32.02.47

SDN based Model to Enhance Security and Fault Tolerance in IoT Environments

Dr. ASHIMA MEHTA
Assistant Professor, Department of Computer Science and Engineering, Dronacharya College of Engineering, Gurugram, Haryana
ashima.mehta@ggnindia.dronacharya.info

Dr. HANSRAJ
Assistant Professor, Department of Computer Science & Engineering, Dronacharya Group of Institutions, Greater Noida, Uttar Pradesh
hansraj@ggnindia.dronacharya.info

Abstract

The Internet of Things (IoT) is increasingly used in various sectors, including education, healthcare, and smart cities, putting users' privacy and security at risk. IoT devices are vulnerable to resource exhaustion attacks due to limited memory, computing capability, and battery usage. These attacks impact the operational functionality and availability of IoT services. IoT devices make up 96% of devices involved in Distributed Denial of Service (DDoS) attacks, with home routers accounting for 3% and hacked Linux servers accounting for 1%. To ensure the healthy operation of IoT systems, it is crucial to develop Intrusion Detection and Prevention Systems for IoT networks that address new and existing vulnerabilities. Compliance with enhanced security methods with network architectures based on Software Defined Network (SDN) and SDN enabled benefits is required for quick detection and minimization of attacks. Machine Learning (ML)-based IDS systems perform better than conventional approaches, as they analyze network traffic features automatically, circumventing manual feature extraction issues and enhancing detection accuracy.

Keywords: Internet of Things (IoT), Distributed Denial of Service (DDoS) , Software Defined Network (SDN), Machine Learning (ML),Security.

Introduction

The Internet of Things (IoT) has revolutionized industries by providing interconnected devices for transmitting and receiving information. With a growing demand from 2 billion to 200 billion objects, IoT devices are used in various sectors, including logistics, green infrastructure, tourism, education, and financial management. However, IoT users' negligence can put them at risk, leading to cyberattacks and threats to the environment [1-5].

Fig.-1 DDoS Mitigation process

10.48047/jocaaa.2024.32.02.47

The Dyn cyberattack recruited connected smartphones into "botnets" using Mirai malware. IoT systems also face attacks against vectors, making it more complex and diverse. Therefore, much emphasis should be placed on analyzing these attacks, their detection, malicious prevention, and system retrieval [6-10].

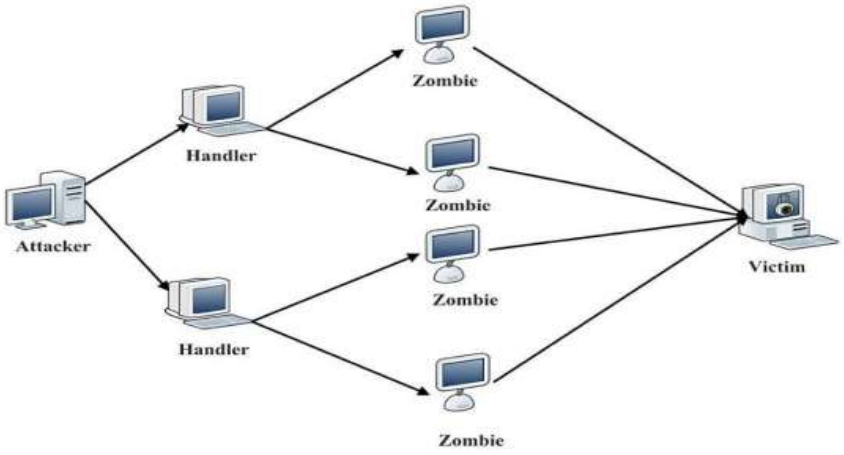

Fig.-2 Outline of DDoS Attack

IoT security is essential due to the differences between traditional networks and IoT. Traditional networks have more resources, while IoT systems have minimal security features that balance energy use and security. The IoT environment consists of hard-core parts, operational planning, and functional methods with data formats. However, no single architecture is required for IoT, and multiple researchers have proposed multiple architectures [11-15].

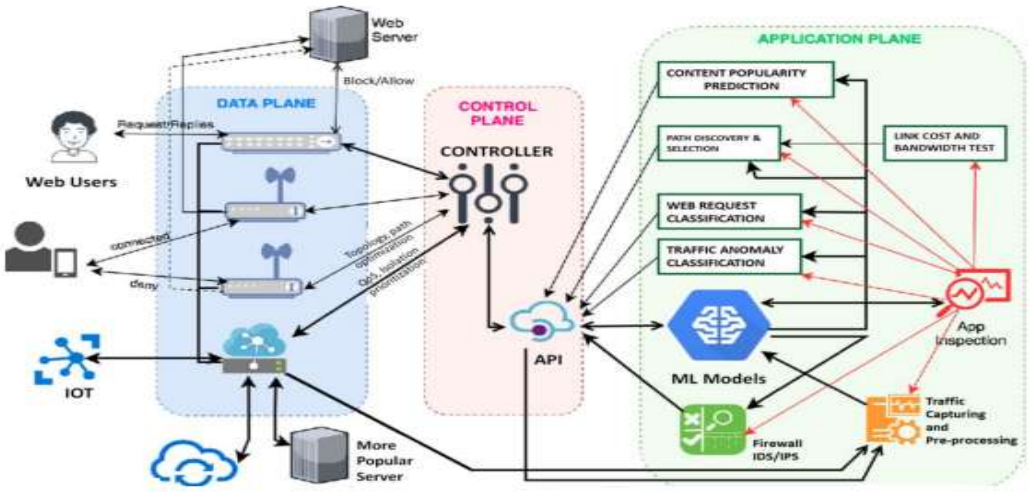

Fig.-3 SDN security solutions using machine learning

10.48047/jocaaa.2024.32.02.47

The Internet of Things (IoT) offers numerous benefits but also presents risks and security threats. Research shows that 90% of users do not guarantee security analysis in their internet devices, making security a critical requirement for privacy and reliability. To secure attached devices, networks, data, and IoT organizations, IoT security is more important. However, due to the design of IoT, traditional security systems cannot be directly implemented due to heterogeneity and scalability issues [16-20].

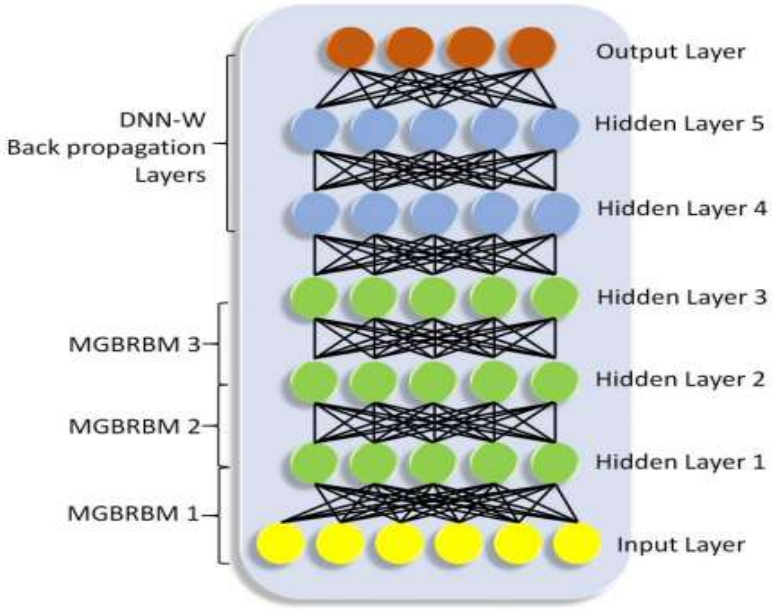

Fig.-3 Modified Hybrid Deep Belief Network with Weights Structure

To address these challenges, it is essential to implement security measures integrated with IoT, enabling trust and enabling high-security protocols for information exchange. Data security issues aim to achieve accessibility, reliability, and privacy, and security performance measures are used to solve security challenges. Traditional methods like signature, threshold, and statistical analysis are insufficient for large network data and require cybersecurity professionals' training [21-25].

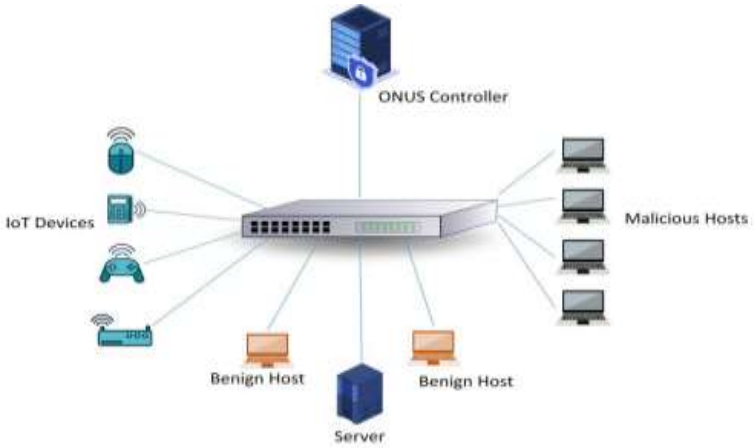

Fig.-4 Testbed Environment

10.48047/jocaaa.2024.32.02.47

Machine learning/deep learning techniques have been used to improve dynamic IDSs, and new techniques are being explored to counter malicious attack traffic in heterogeneous networks.

Methodology & Analysis

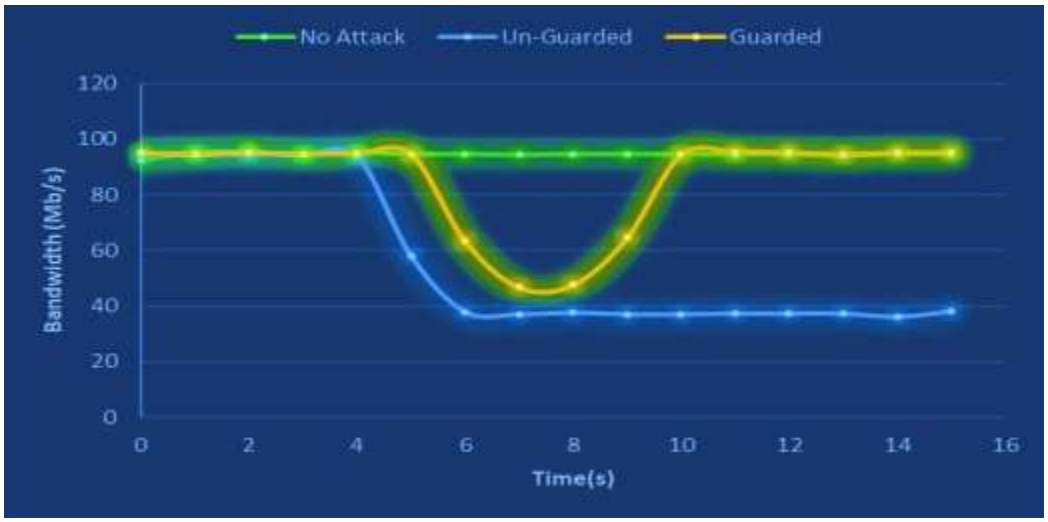

Fig.-5 SYN flood with spoofing: available bandwidth

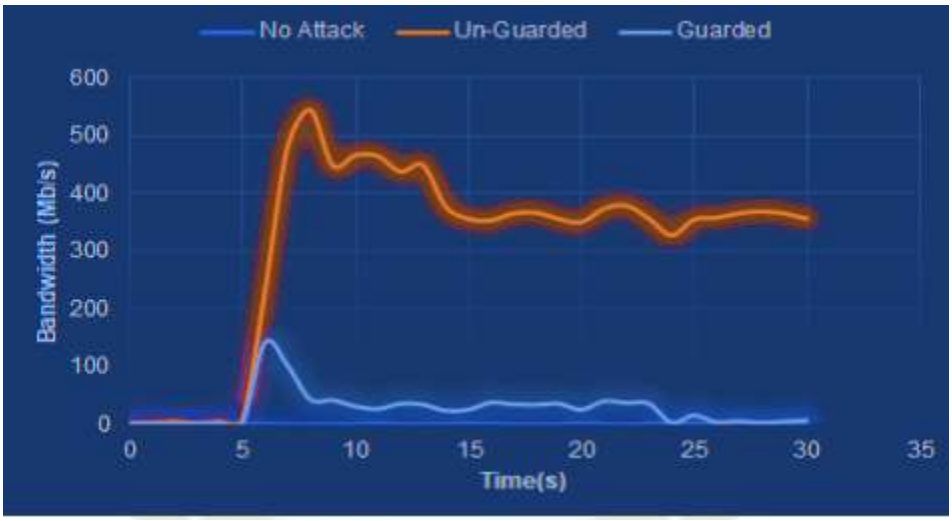

Fig.-6 Controller CPU utilization under SYN flood

The increasing number of connected devices and IoT use cases has led to an increase in data traffic and cyber-attacks in the managed IoT network. By the end of 2025, there are expected to be 5 billion IoT devices. To mitigate these threats, an enhanced device with proper security levels is needed. However, IoT devices manage sensitive information, making them vulnerable to malicious attacks like DoS and DDoS [26-30].

10.48047/jocaaa.2024.32.02.47

The SDN-IoT architecture consists of three layers: applications, control, and infrastructure (DP). The northbound API communicates with the controller for operations, while the southbound API uses the OpenFlow protocol for interaction between controller and switches. The controller maintains a global network view and inserts forwarding rules called "flow rules" into appropriate switches. Flow rules are compared to header fields of arriving packets, and the controller responds with a routing suggestion in the form of a PACKET OUT message [31].

Flow rule networks do not allow for the detection of the first packet that initiated the installation of a flow rule, which can lead to data loss in DoS and DDoS attacks. The increasing number of connected devices and IoT use cases has led to an increase in data traffic and cyber-attacks in the managed IoT network. By the end of 2025, there are expected to be 5 billion IoT devices. To mitigate these threats, an enhanced device with proper security levels is needed. However, IoT devices manage sensitive information, making them vulnerable to malicious attacks like DoS and DDoS [32].

The SDN-IoT architecture consists of three layers: applications, control, and infrastructure (DP). The northbound API communicates with the controller for operations, while the southbound API uses the OpenFlow protocol for interaction between controller and switches. The controller maintains a global network view and inserts forwarding rules called "flow rules" into appropriate switches. Flow rules are compared to header fields of arriving packets, and the controller responds with a routing suggestion in the form of a PACKET OUT message [33-34].

Flow rule networks do not allow for the detection of the first packet that initiated the installation of a flow rule, which can lead to data loss in DoS and DDoS attacks.

Conclusion

The Internet of Things (IoT) is a rapidly growing technology, with smart homes, buildings, and cities being a part of it. However, security concerns have also increased due to the growing popularity of IoT. The Smart Distributed Network (SDN) is a future trend for IoT security solutions, introducing an SDN controller to separate the Control Point (CP) of a network device. This paper presents three models of IDS that have proven more resilient and reliable in presenting threat models. The third paper addresses defending the IoT from malware and cyberattacks using an SDN-enabled hybrid DL architecture. The third paper presents a distributed SDN architecture for detecting and reacting to abnormalities in a large-scale network and a multi-SDN controller architecture to mitigate single point failure. The fifth paper presents "SHProIoT", a honeypot-based distributed SDN controller architecture for IoT to mitigate DDoS attacks and relieve stress on the SDN controller. The model employs "SOMEM-BT", a self-organizing map and ball tree-based learning model, to identify anomaly traffic.

Future Scopes

he work presents high detection rates and low FAR models, but faces flaws like difficulty in anomaly detection and difficulty determining unknown assaults. Future research will focus on using different deep learning classifiers and testing the models in real-world settings. Future studies will focus on continuous learning with a human-in-the-loop system for improved performance in various network configurations.

10.48047/jocaaa.2024.32.02.47

References

[1] Grau. “The Internet of Secure Things – What is Really Needed to Secure the Internet of Things? “| Icon Labs, March 2014.

[2] J. Ferlay *et al.*, “Estimating the global cancer incidence and mortality in 2018: GLOBOCAN sources and methods,” *Int. J. Cancer*, vol. 144, no. 8, pp. 1941–1953, 2019, doi: 10.1002/ijc.31937.

[3] F. Bray, J. Ferlay, I. Soerjomataram, R. L. Siegel, L. A. Torre, and A. Jemal, “Global cancer statistics 2018: GLOBOCAN estimates of incidence and mortality worldwide for 36 cancers in 185 countries,” *CA. Cancer J. Clin.*, vol. 68, no. 6, pp. 394–424, 2018, doi: 10.3322/caac.21492.

[4] Singh, G. Tripathi, and A. J. Jara. “A survey of Internet-of-Things: Future vision, architecture, challenges and services”. In 2014 IEEE World Forum on Internet of Things (WF-IoT), pages 287–292, March 2014.

[5] M. A. A. Hamid and N. A. Khan, “Investigation and Classification of MRI Brain Tumors Using Feature Extraction Technique,” *J. Med. Biol. Eng.*, vol. 40, no. 2, pp. 307–317, 2020, doi: 10.1007/s40846-020-00510-1.

[6] HPE Fortify and the Internet of Things, (2017). [Online]. Available: http://go.saas.hpe.com/fod/internet-of-things

[7] M. Hosseinzadeh, S. Salmani, and M. H. M. Ara, “Interferometric optical testing to discriminate benign and malignant brain tumors,” *J. Photochem. Photobiol. B Biol.*, vol. 199, no. August, p. 111590, 2019, doi: 10.1016/j.jphotobiol.2019.111590.

[8] S. S. Han, M. S. Kim, W. Lim, G. H. Park, I. Park, and S. E. Chang, “Classification of the Clinical Images for Benign and Malignant Cutaneous Tumors Using a Deep Learning Algorithm,” *J. Invest. Dermatol.*, vol. 138, no. 7, pp. 1529–1538, 2018, doi: 10.1016/j.jid.2018.01.028.

[9] S. E. Steck and E. A. Murphy, “Dietary patterns and cancer risk,” *Nat. Rev. Cancer*, vol. 20, no. 2, pp. 125–138, 2020, doi: 10.1038/s41568-019-0227-4.

[10] vinod k ramani, “Analysis of Bloodstream Infections and Their Antibiotic Sensitivity Pattern (Pre- and Post-COVID Lockdown in an Indian Cancer Hospital): A Record-Based Retrospective Cohort Study,” *Eurasian J. Med. Oncol.*, 2022, doi: 10.14744/ejmo.2022.18855.

[11] C. I. Owobu *et al.*, “Pattern of Cancer in Irrua Specialist Teaching Hospital,” *Int. J. Trop. Dis. Heal.*, vol. 42, no. December 2020, pp. 14–21, 2021, doi: 10.9734/ijtdh/2021/v42i730468.

[12] A. Myronenko, “3D MRI brain tumor segmentation using autoencoder regularization,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 11384 LNCS, pp. 311–320, 2019, doi: 10.1007/978-3-030-11726-9_28.

[13] Borgohain, U. Kumar, and S. Sanyal, “Survey of security and privacy issues of Internet of Things,” 2015

[14] S. Rathore *et al.*, “Brain Cancer imaging phenomics toolkit (brain-CaPTk): An interactive platform for quantitative analysis of glioblastoma,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 10670 LNCS, pp. 133–145, 2018, doi: 10.1007/978-3-319-75238-9_12.

10.48047/jocaaa.2024.32.02.47

[15] K. Iqtidar, A. Iqtidar, W. Ali, S. Aziz, and M. U. Khan, "Image Pattern Analysis towards Classification of Skin Cancer through Dermoscopic Images," *Proc. - 2020 1st Int. Conf. Smart Syst. Emerg. Technol. SMART-TECH 2020*, no. January 2021, pp. 208–213, 2020, doi: 10.1109/SMART-TECH49988.2020.00055.

[16] P. Tschandl, C. Rosendahl, and H. Kittler, "The HAM10000 dataset, a large collection of multi-source dermatoscopic images of common pigmented skin lesions," *Sci. Data*, vol. 5, no. 1, p. 180161, Dec. 2018, doi: 10.1038/sdata.2018.161.

[17] B. E. Bejnordi *et al.*, "Diagnostic Assessment of Deep Learning Algorithms for Detection of Lymph Node Metastases in Women With Breast Cancer," *JAMA*, vol. 318, no. 22, p. 2199, Dec. 2017, doi: 10.1001/jama.2017.14585.

[18] G. Yu *et al.*, "Accurate recognition of colorectal cancer with semi-supervised deep learning on pathological images," *Nat. Commun.*, vol. 12, no. 1, pp. 1–13, 2021, doi: 10.1038/s41467-021-26643-8.

[19] J. Noorbakhsh, S. Farahmand, M. Soltanieh-ha, S. Namburi, K. Zarringhalam, and J. H. Chuang, "Pan-cancer classifications of tumor histological images using deep learning," *bioRxiv*, vol. 64, p. 715656, 2019, [Online]. Available: https://www.biorxiv.org/content/10.1101/715656v1.full.

[20] L. A. D. Cooper, E. G. Demicco, J. H. Saltz, R. T. Powell, A. Rao, and A. J. Lazar, "PanCancer insights from The Cancer Genome Atlas: the pathologist's perspective," *J. Pathol.*, vol. 244, no. 5, pp. 512–524, 2018, doi: 10.1002/path.5028.

[21] M. Saric, M. Russo, M. Stella, and M. Sikora, "CNN-based Method for Lung Cancer Detection in Whole Slide Histopathology Images," *2019 4th Int. Conf. Smart Sustain. Technol. Split. 2019*, pp. 14–17, 2019, doi: 10.23919/SpliTech.2019.8783041.

[22] "Cancer Detection and Classification in Whole-slide Lung Histopathology," Accessed: May 29, 2022. [Online]. Available: https://acdc-lunghp.grand-challenge.org/.

[23] K.-H. Yu *et al.*, "Classifying non-small cell lung cancer types and transcriptomic subtypes using convolutional neural networks," *J. Am. Med. Informatics Assoc.*, vol. 27, no. 5, pp. 757–769, May 2020, doi: 10.1093/jamia/ocz230.

[24] T. T. Tang, J. A. Zawaski, K. N. Francis, A. A. Qutub, and M. W. Gaber, "Image-based Classification of Tumor Type and Growth Rate using Machine Learning: a preclinical study," *Sci. Rep.*, vol. 9, no. 1, pp. 1–10, 2019, doi: 10.1038/s41598-019-48738-5.

[25] Q. D. Vu *et al.*, "Methods for segmentation and classification of digital microscopy tissue images," *Front. Bioeng. Biotechnol.*, vol. 7, no. APR, 2019, doi: 10.3389/fbioe.2019.00053.

[26] C. Davatzikos *et al.*, "Cancer imaging phenomics toolkit: quantitative imaging analytics for precision diagnostics and predictive modeling of clinical outcome," *J. Med. Imaging*, vol. 5, no. 01, p. 1, 2018, doi: 10.1117/1.jmi.5.1.011018.

[27] A. Fathi Kazerooni *et al.*, "Cancer Imaging Phenomics via CaPTk: Multi-Institutional Prediction of Progression-Free Survival and Pattern of Recurrence in Glioblastoma," *JCO Clin. Cancer Informatics*, no. 4, pp. 234–244, 2020, doi: 10.1200/cci.19.00121.

[28] M. Hasan, S. Das Barman, S. Islam, and A. W. Reza, "Skin cancer detection using convolutional neural network," *ACM Int. Conf. Proceeding Ser.*, no. March 2020, pp. 254–258, 2019, doi:

10.48047/jocaaa.2024.32.02.47

10.1145/3330482.3330525.

[29] NEEMA M, A. S. NAIR, A. JOY, A. P. MENON, and A. HARIS, "SKIN LESION/CANCER DETECTION USING DEEP LEARNING," *Int. J. Appl. Eng. Res.*, vol. 15, no. 1, pp. 11–17, 2020.

[30] Virupakshappa and B. Amarapur, "Computer-aided diagnosis applied to MRI images of brain tumor using cognition based modified level set and optimized ANN classifier," *Multimed. Tools Appl.*, vol. 79, no. 5–6, pp. 3571–3599, Feb. 2020, doi: 10.1007/s11042-018-6176-1.

[31] S. R. Sannasi Chakravarthy and H. Rajaguru, "Automatic Detection and Classification of Mammograms Using Improved Extreme Learning Machine with Deep Learning," *IRBM*, vol. 43, no. 1, pp. 49–61, Feb. 2022, doi: 10.1016/j.irbm.2020.12.004.

[32] Haider, J. Hu, J. Slay, B. P. Turnbull, and Y. Xie. "Generating realistic intrusion detection system dataset based on fuzzy qualitative modeling". Journal of Network and Computer Applications, 87:185–192, June 2017.

[33] Zargar, S. T., Joshi, J., & Tipper, D. (2013). "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks". IEEE communications surveys & tutorials, 15(4), 2046-2069.

[34] Tripathi, S., et al. (2013). "Hadoop based defense solution to handle distributed denial of service (DDoS) attacks". Journal of Information Security. Vol. 4 No. 3 (2013), Article ID: 34629 , 15 pages DOI:10.4236/jis.2013.43018.