EAI Endorsed Transactions
on Smart Cities

Research Article EAI.EU

Detection of Cyber Attacks using Machine Learning based Intrusion Detection System for IoT Based Smart Cities

Maria Nawaz Chohan[1], Usman Haider[2,*], Muhammad Yaseen Ayub[3], Hina Shoukat[3], Tarandeep Kaur Bhatia[4] and Muhammad Furqan Ul Hassan[3]

[1]National Defence University, Islamabad, Pakistan
[2]Department of Electrical Engineering, National University of Computer & Emerging Sciences, Peshawar, Pakistan
[3]Department of Computer science, COMSATS University Islamabad, Attock, Pakistan
[4]University of Petroleum and Energy Studies, Dehradun, India

Abstract

The world's dynamics is evolving with artificial intelligence (AI) and the results are smart products. A smart city has smart city is collection of smart innovations powered with AI and internet of things (IoTs). Along with the ease and comfort that the concept of a smart city pointed at, many security concerns are being raised that hinders the path of its flourishment. An Intrusion Detection System (IDS) monitors the whole network traffic and alerts in case of any anomaly. A Machine Learning-based IDS intelligently senses the network threats, takes decisions about data packet legibility and alarm the user. Researchers have deployed various ML techniques to IDS to improve the detection accuracy. This work presents a comparative analysis of various ML algorithms trained over UNSW-NB15 dataset. ADA Boost, Linear Support Vector Machine (LSVM), Auto Encoder Classifier, Quadratic Support Vector Machine (QSVM) and Multi-Layer Perceptron algorithms are being employed in the stimulation. ADA Boost showed an excellent accuracy of 98.3% in the results.

Keywords: IoT, Smart Cities, UAVs

Received on 09 April 2023, accepted on 17 June 2023, published on 28 June 2023

doi: 10.4108/eetsc.3222

*Corresponding author: usmanhaider@ieee.org
Emails: M.N. Chohan (maria.nawaz160@gmail.com), M.Y. Ayub (yaseen.ayub@ieee.org), H. Shoukat (fa18-bcs-053@cuiatk.edu.pk), T. K. Bhatia (tarandeepkaur42@gmail.com) M. F. Ul Hassan (sp19-bcs-011@cuiatk.edu.pk)

1. Introduction

Technological inventions have changed the dynamics of world. Infrastructure in every industry is automated with the use of IoT and wireless communication networks. Smart cities are based on wireless connectivity where infrastructure less topological scenario allows many cyber-attacks. Therefore, vulnerabilities in smart cities need to be addressed with proper solution. The area of smart cities is quite diverse with having many applications which include e-government, smart homes, intelligent transportation, tele-medicines, smart grid, UAVs monitoring, energy and many more [1-4].

Data network security is the topic for many researchers around the world due to ever-increasing cyber-attacks. Intrusion detection is the system which needs to identify fake data packets easily. Optimal IDS algorithm balance high accuracy with the metrics of false negative and false positive. Also, the main goal of IDS is to detect possible cyber-attacks. However, intrusion detection system is based on normal and

illegal data packets. Moreover, smart cities need secure communication channels due to that IDS plays important role [5-8]. Figure 1, shows the concept of smart cities which further explains smart house, hospitals, vehicles and how a smart city is going to be connected. UAVs can be merged with smart cities which can help in connectivity. Secure communication links are designed to reduce end-to-end delay. While, false data injection attacks can be deployed with help of intruder to unbalance communication in remote surgery of high official patient. Various technologies like markov chain, machine learning, deep learning, ant colony optimization and poisson distribution use to improve signature, anomaly or hybrid intrusion detection systems [9-13].

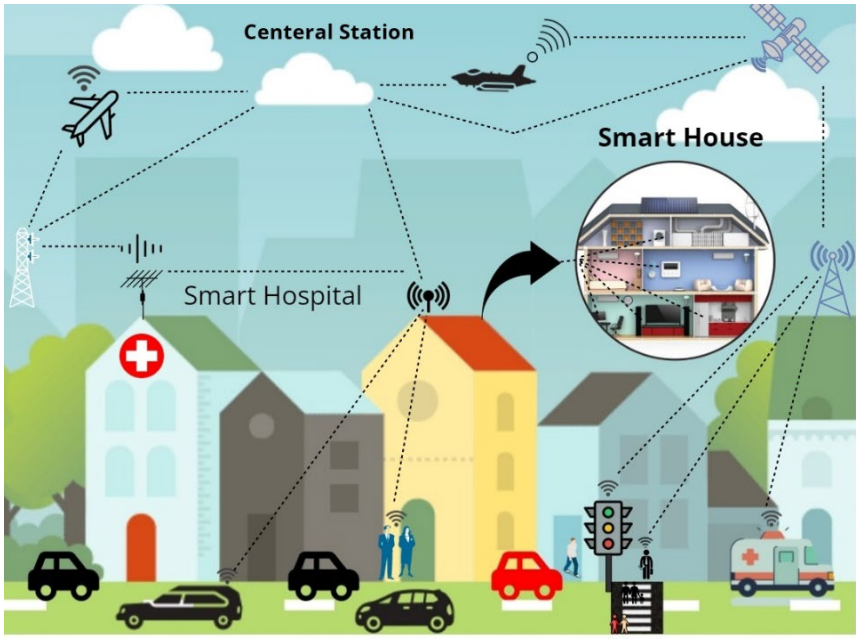


Figure1: Future Connected Smart Cities

2. Literature Study

The concept of smart cities is the need of today but due to automation there exist many connectivity problems. UAVs operations are possible in smart cities to collect information from IoT nodes and send to base station. Therefore, UAVs actively plays important role in smart cities. DSDV routing protocol is having the process of incremental updates which is helpful to improve and secure communication standards in UAV enabled smart cities [14]. Moreover, for secure communication protocols need to be designed to mitigate related problems of the network [15]. Wireless connected technology like IEEE 802.11 needs more improvements. RSSI controlled machine learning approach decision tree is introduced which has shown better results in signal strength indicator [16]. IoT networks in smart cities connect everything through wireless technology. Block chain in smart cities can provide better solutions in many applications [17]. Table 1, describes the security attacks/violation, related challenges in smart cities and gives an overview of researches in this area.

3. Cyber Threats on Smart Cities

IoT Networks are vulnerable to the cyber-attacks, so in a smart city such threats are a big challenge to counter. DOS, DDOS, Sybil attack, SQL injection and Malware attacks are common types of attacks in IoT environment thus smart cities are also subjected to these attacks. So, the result of this insecure sensor node network can be system crashing or service termination if left solution less and unsecure. Such technical failures can be a full stop to this advancement. Fortunately, no one is left helpless over these threats because many solutions are been available of various nature can be used accordingly [28-29].

3.1. Denial of Service Attack (DoS) on Smart cities

no one is Denial of Service (DoS) attack is most basic type of attack that can cause the victim system to crash down or become unavailable even for the legal users due is huge imbursement of the data packets by the hacker or intruder. Thus, the purpose of this attack is the hang up victim services, like an attack on a Smart Grid in Ukraine in 2015. In smart cities, such system unavailability can cause a havoc, so the monitoring of all network traffic is certain [30]. Figure 2, explains DoS attack mechanism in detail, how a system is being attacked in dos and represent the service termination as attack result.

Table 1: Cyber Attacks with related challenges

Reference	Security Attacks/Violations	Field of Study	Description
[18]	DDoS, Access Attack	IoT	IoT needs to be secure thus an analysis is necessary to be done on various kind of attacks and solution to them.
[19]	Man-in-the-middle (MITM) attack, Ping DDoS Flood attack, Modbus Query Flood attack, and TCP SYN DDoS Flood attack	IoT	This paper proposed a deep leaning approach to detect the mentioned attacks and applies long short-term memory (LSTM) module.
[20]	DDoS, Malware	IoT	This work analyzes the real time attacks and suggest a threefold approach.
[21]	DDoS	IoT	In a smart power system, IoT managed load could be vulnerable to attacks. This paper presents a detailed report on threat analysis.
[22]	False data injection attack	IoT	The security of smart electric vehicles is subject into account by this work and proposes semidefinite programming approach-based algorithm.
[23]	Denial of Service (DoS) attacks, injections, Man in the Middle attacks, buffer overflow	IoT	This paper proposed management-based solution to cyber-attacks.
[24]	DoS, DDoS, Zero-day attacks, MITM	IoT	Growth of IoT in the markets has given rise to cybercrime in this domain and this work offers detailed analysis of known defense techniques.
[25]	DDoS	IoT	This paper tries to cover the destruction of DDoS attack with deep learning approach with an excellent efficiency
[26]	Intrusion attacks	IoT	This paper provides a hybrid approach for intelligent secure system.

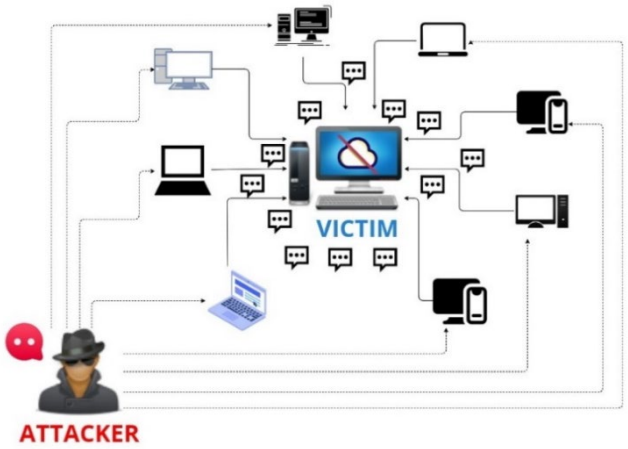
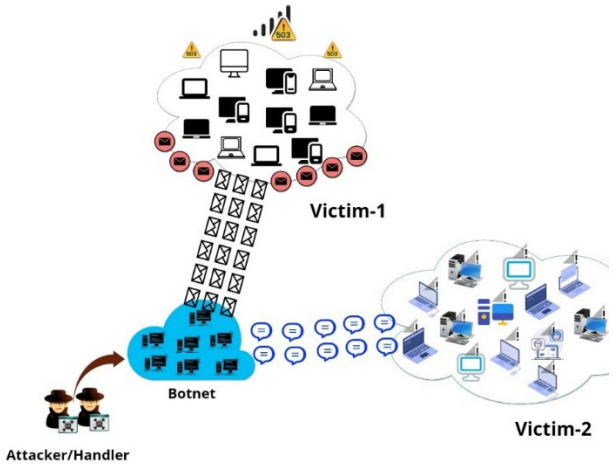


Figure 2: Denial-of-Service attack

3.2 Distributed Denial of Service Attack (DDoS) on Smart Cities

Distributed Denial of service (DDoS) Attack is type of DoS attacked and it can be on single victim or group of victims with multiple systems operated via channels using various compromised Systems or Botnets. A victim compromised with such an attack in smart, drains out resources of the server or network infrastructure by entertaining overwhelming faulty packets in place legitimate packets thus they remain unpleased over the victim. In this way all communications can be disrupted with multiple consequences [31]. Figure 3 shows the concept of DDoS attacks on smart cities and understanding of attacker, handler, botnet and victim in this type of attack.



[1]

Figure 3: DDoS attack

3.3 Sybil Attack on Smart Cities

In Sybil attack, the hacker pretends multiple identities using them all at the same time thus these pseudoidentities compromise the system efficiency. So, in a smart city, aftershocks of this of attacks are privacy loss, fallacious report generation, spam encounter etc. Moreover, Sybil attackers incorporate various other types of attacks like phishing, social engineering, malware etc. and also encourage Machine Learning (ML) methods in their attack patters [32].

3.4 SQL Injection Attack on Smart Cities

Whenever the target is sensitive data, SQL injective is famous way to proceed. This attack can read as well as delete data and also this intrusion has application to destroy SQL databases. All the sensitive data from various ends and sensor nodes of smart appliances in a smart city can be at risk. So, the databases in a smart city must be highly protected for the users to have their privacy [33].

3.5 Malware Attack on Smart Cities

Malware is one of the largest group of threats with various types and classes of intrusion and threats. Famous classes of malware are ransomwares, trojans, worms etc. They actually infect the victim with various kind of viruses thus resulting in victims' data loss. In a smart city, all the customer's data can be at stack of destruction thus leaving the core cause of easing humanity smart cities [34].

4. Machine Learning Based Intrusion Detection System

The finest approach in the detection and mitigation of various threats in smart cities is machine learning. We are using ML for the detection of Cyber threats in networks of a smart city. There are three main types of ML approaches: anomaly-based, signature-based and hybrid. Anomaly-based detection is through the system intelligence trained through various techniques [35], signature-based approach cross compares the network traffic with existing signature or attack pattern thus results threat detection [36] and hybrid system is mixture of assets of both thus more effective and accurate than both of then [37]. Depending on environment scenarios, various researchers have developed different types of IDSs using different approaches, algorithms with different target systems and compare the precision and accuracy of their proposed algorithm with other algorithms in their case study [38-39].

5. Simulation Environment & Results

Python is used to create the simulation environment. The most popular dataset UNSW-NB15 is used. However, machine learning algorithms like ADA Boost, Auto Encoder Classifier, Linear Support Vector Machine, Quadratic Support Vector Machine and Multi-Layer Perceptron are simulated to detect cyber-attacks [39-45]. Table 2 shows accuracies of machine learning algorithms where ADA Boost shows better results in comparison with other traditional techniques. Table 2, details are illustrated in figure 4.

Table 2: Accuracy details of Machine learning classifiers

S/No.	Algorithms	Accuracy
1	ADA Boost	98.3431
2	Auto Encoder Classifier	96.1133
3	Linear Support Vector Machine	97.8503
4	Quadratic Support Vector Machine	84.7305
5	Multi-Layer Perceptron	97.9735

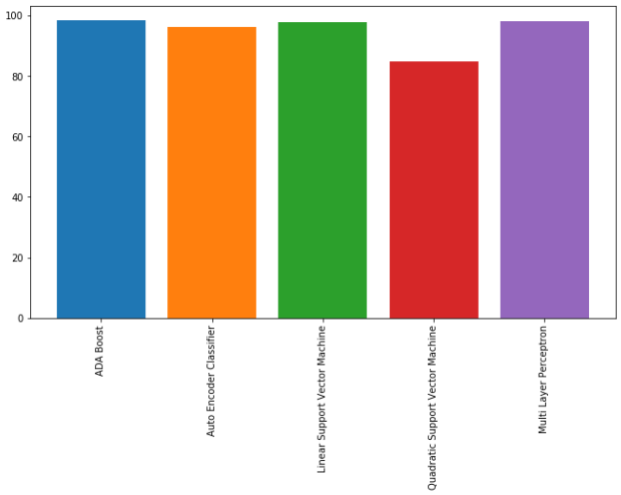


Figure 4: Comparative study of machine learning algorithms using UNSW-NB15

6. Conclusion

Smart cities are considered a novel concept while, cyber-attacks can unbalance life of humans. Therefore, most of the researchers have merged smart cities with UAVs to provide better connectivity. Machine learning based IDS approach is used in the concept of smart cities. For experimentation, UNSW Australia based dataset is used to check the raw traffic problems and attacks. Machine learning algorithms are used where ADA Boost has shown optimal results.

7. Future Direction

In near future, the use of technology is increasing on daily basis. Security is considered main issue in every field of study. Therefore, machine learning based intrusion detection system will easily detect attacks in IoT-networks. Moreover, deep learning, artificial intelligence, genetic algorithm-based IDS need to be designed for future smart cities.

References

[1] Çimen, H.; Palacios-García, E.J.; Kolaek, M.; Çetinkaya, N.; Vasquez, J.C.; Guerrero, J.M. Smart-Building Applications: Deep Learning-Based, Real-Time Load Monitoring. IEEE Ind. Electron. Mag. 2020, 15, 4–15.

[2] Santiago, I.; Moreno-Munoz, A.; Quintero-Jiménez, P.; Garcia-Torres, F.; Gonzalez-Redondo, M. Electricity demand during pandemic times: The case of the COVID-19 in Spain. Energy Policy 2021, 148, 111964.

[3] Coffey, K.; Maglaras, L.A.; Smith, R.; Janicke, H.; Ferrag, M.A.; Derhab, A.; Mukherjee, M.; Rallis, S.; Yousaf, A. Vulnerability assessment of cyber security for SCADA systems. In Guide to Vulnerability Analysis for Computer Networks and Systems; Springer: Berlin/Heidelberg, Germany, 2018; pp. 59–80.

[4] Panagiotis, Fountas, Kouskouras Taxiarxchis, Kranas Georgios, Leandros Maglaras, and Mohamed Amine Ferrag. "Intrusion Detection in Critical Infrastructures: A Literature Review." Smart Cities 4, no. 3 (2021): 1146-1157.

[5] L. Hung-Jen and C.-h. R. Lin, “Intrusion detection system a comprehensive review,” Journal of network and applications, vol. 36, no. 1, pp. 16–24, 2013.

[6] H. L. Motoda and H. Motoda, Feature Selection for Knowledge Discovery and Data Mining, vol. 454, Springer, 1998.

[7] L. D. S. Silva, A. C. Santos, T. D. Mancilha, J. D. Silva, and A. Montes, “Detecting attack signatures in the real network traffic with ANNIDA,” Expert Systems with Applications, vol. 34, no. 4, pp. 2326–2333, 2008.

[8] Rincy N, Thomas, and Roopam Gupta. "Design and development of an efficient network intrusion detection system using machine learning techniques." Wireless Communications and Mobile Computing 2021 (2021).

[9] A. Qayyum, L. Viennot, and A. Laouiti, “Multipoint relaying for flooding broadcast messages in mobile wireless networks,” in Proceedings of the 35th annual Hawaii international conference on system sciences, pp. 3866–3875, Big Island, HI, USA, 2002.

[10] I. U. Khan, I. M. Qureshi, M. A. Aziz, T. A. Cheema, and S. B. H. Shah, “Smart IoT control-based nature inspired energy efficient routing protocol for flying ad hoc network (FANET),” IEEE Access, vol. 8, pp. 56371–56378, 2020.

[11] M. Ahmed and A. K. Pathan, “False data injection attack (FDIA): an overview and new metrics for fair evaluation of its countermeasure,” Complex Adaptive Systems Modeling, vol. 8, no. 1, p. 4, 2020.

[12] A. Abdollahi and M. Fathi, “An intrusion detection system on ping of death attacks in IoT networks,” Wireless Personal Communications, vol. 112, no. 4, pp. 2057–2070, 2020.

[13] Khan, Inam Ullah, Asrin Abdollahi, Ryan Alturki, Mohammad Dahman Alshehri, Mohammed Abdulaziz Ikram, Hasan J. Alyamani, and Shahzad Khan. "Intelligent Detection System Enabled Attack Probability Using Markov Chain in Aerial Networks." Wireless Communications and Mobile Computing 2021 (2021).

[14] Khan, Inam Ullah, Muhammad Abul Hassan, Muhammad Fayaz, Jeonghwan Gwak, and Muhammad Adnan Aziz. "Improved sequencing heuristic DSDV protocol using nomadic mobility model for FANETS." Comput., Mater. Continua 70, no. 2 (2022): 3653-3666.

[15] Khan, Inam Ullah, Muhammad Abul Hassan, Mohammad Dahman Alshehri, Mohammed Abdulaziz Ikram, Hasan J. Alyamani, Ryan Alturki, and Vinh Truong Hoang. "Monitoring system-based flying IoT in public health and sports using ant-enabled energy-aware routing." Journal of Healthcare Engineering 2021 (2021).

[16] Khan, Inam Ullah, Ryan Alturki, Hasan J. Alyamani, Mohammed Abdulaziz Ikram, Muhammad Adnan Aziz, Vinh Truong Hoang, and Tanweer Ahmad Cheema. "RSSI-controlled long-range communication in secured IoT-enabled unmanned aerial vehicles." Mobile information systems 2021 (2021).

[17] Alasbali, Nada, Saaidal Razalli Bin Azzuhri, Rosli Bin Salleh, Miss Laiha Mat Kiah, Ahmad Aliff AS Shariffuddin, Nik Muhammad Izwan bin Nik Mohd Kamel, and Leila Ismail. "Rules of Smart IoT Networks within Smart Cities towards Blockchain Standardization." Mobile Information Systems 2022 (2022).

[18] Abomhara, Mohamed, and Geir M. Køien. "Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks." *Journal of Cyber Security and Mobility* (2015): 65-88.

[19] Saharkhizan, Mahdis, et al. "An ensemble of deep recurrent neural networks for detecting IoT cyber attacks using network traffic." *IEEE Internet of Things Journal* 7.9 (2020): 8852-8859.

[20] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz and J. Lopez, "A Survey of IoT-Enabled Cyberattacks: Assessing Attack Paths to Critical Infrastructures and Services," in IEEE Communications Surveys & Tutorials, vol. 20, no. 4, pp. 3453-3495, Fourthquarter 2018, doi: 10.1109/COMST.2018.2855563.

[21] Dvorkin, Yury, and Siddharth Garg. "IoT-enabled distributed cyber-attacks on transmission and distribution grids." *2017 North American Power Symposium (NAPS)*. IEEE, 2017.

[22] Rana, Md Masud. "IoT-based electric vehicle state estimation and control algorithms under cyber attacks." *IEEE Internet of Things Journal* 7.2 (2019): 874-881.

[23] Diaz Lopez, Daniel, et al. "Shielding IoT against cyber-attacks: An event-based approach using SIEM." *Wireless Communications and Mobile Computing* 2018 (2018).

[24] Tabassum, Aliya, and Wadha Lebda. "Security Framework for IoT Devices against Cyber-attacks." *arXiv preprint arXiv:1912.01712* (2019).

[25] Roopak, Monika, Gui Yun Tian, and Jonathon Chambers. "Deep learning models for cyber security in IoT networks." 2019 IEEE 9th annual computing and communication workshop and conference (CCWC). IEEE, 2019.

[26] F. Farivar, M. S. Haghighi, A. Jolfaei and M. Alazab, "Artificial Intelligence for Detection, Estimation, and Compensation of Malicious Attacks in Nonlinear Cyber-Physical Systems and Industrial IoT," in IEEE Transactions on Industrial Informatics, vol. 16, no. 4, pp. 2716-2725, April 2020, doi: 10.1109/TII.2019.2956474.

[27] Sikder, Amit Kumar, et al. "A survey on sensor-based threats and attacks to smart devices and applications." *IEEE Communications Surveys & Tutorials* 23.2 (2021): 1125-1159.

[28] AlDairi, Anwaar. "Cyber security attacks on smart cities and associated mobile technologies." *Procedia Computer Science* 109 (2017): 1086-1091.

[29] Al-Turjman, Fadi, Hadi Zahmatkesh, and Ramiz Shahroze. "An overview of security and privacy in smart cities' IoT communications." Transactions on Emerging Telecommunications Technologies 33.3 (2022): e3677.

[30] Sikder, Amit Kumar, et al. "A survey on sensor-based threats and attacks to smart devices and applications." *IEEE Communications Surveys & Tutorials* 23.2 (2021): 1125-1159.

[31] Zhang, Kuan, et al. "Sybil attacks and their defenses in the internet of things." *IEEE Internet of Things Journal* 1.5 (2014): 372-383.

[32] Gowtham, M., and H. B. Pramod. "Semantic query-featured ensemble learning model for SQL-injection attack detection in IoT-ecosystems." *IEEE Transactions on Reliability* (2021).

[33] Falco, Gregory, et al. "A master attack methodology for an AI-based automated attack planner for smart cities." *IEEE Access* 6 (2018): 48360-48373.

[34] Garcia-Teodoro, Pedro, et al. "Anomaly-based network intrusion detection: Techniques, systems and challenges." *computers & security* 28.1-2 (2009): 18-28.

[35] Kumar, Vinod, and Om Prakash Sangwan. "Signature based intrusion detection system using SNORT." *International Journal of Computer Applications & Information Technology* 1.3 (2012): 35-41.

[36] Otoum, Yazan, and Amiya Nayak. "As-ids: Anomaly and signature based ids for the internet of things." *Journal of Network and Systems Management* 29.3 (2021): 1-26.

[37] Einy, Sajad, Cemil Oz, and Yahya Dorostkar Navaei. "The anomaly-and signature-based IDS for network security using hybrid inference systems." *Mathematical Problems in Engineering* 2021 (2021).

[38] Xu, Chuanfeng, et al. "An SDNFV-based DDoS defense technology for smart cities." *IEEE Access* 7 (2019): 137856-137874.

[39] Moustafa, Nour, and Jill Slay. "UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)." *Military Communications and Information Systems Conference (MilCIS)*, 2015. IEEE, 2015.

[40] Moustafa, Nour, and Jill Slay. "The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 dataset and the comparison with the KDD99 dataset." *Information Security Journal: A Global Perspective* (2016): 1-14.

[41] Moustafa, Nour, et al. "Novel geometric area analysis technique for anomaly detection using trapezoidal area estimation on large-scale networks." *IEEE Transactions on Big Data (2017).*

[42] Moustafa, Nour, et al. "Big data analytics for intrusion detection system: statistical decision-making using finite dirichlet mixture models." *Data Analytics and Decision Support for Cybersecurity. Springer, Cham, 2017.* 127-156.

[43] Sarhan, Mohanad, Siamak Layeghy, Nour Moustafa, and Marius Portmann. NetFlow Datasets for Machine Learning-Based Network Intrusion Detection Systems. In *Big Data Technologies and Applications: 10th EAI International Conference, BDTA 2020, and 13th EAI International Conference on Wireless Internet, WiCON 2020, Virtual Event, December 11, 2020, Proceedings* (p. 117). Springer Nature.

[44] Moustafa, Nour, et al. "An Ensemble Intrusion Detection Technique based on proposed Statistical Flow Features for Protecting Network Traffic of Internet of Things." *IEEE Internet of Things Journal (2018).*

[45] Koroniotis, Nickolaos, Moustafa, Nour, et al. "Towards Developing Network Forensic Mechanism for Botnet Activities in the IoT Based on Machine Learning Techniques." *International Conference on Mobile Networks and Management. Springer, Cham, 2017.*