Current Trends in
Fashion Technology & Textile Engineering
ISSN: 2577-2929

Juniper Publishers
key to the Researchers

Research Article
Volume 9 Issue 4- October 2025
DOI: 10.19080/CTFTTE.2025.09.555767

Curr Trends Fashion Technol Textile Eng

Classification of IoT Traffic Security Attacks Using Deep Learning

Anum Ali*

School of Business and Management, Information Technology University, Pakistan

Submission: September 16, 2025; **Published:** October 08, 2025

***Corresponding author:** Anum Ali, School of Business and Management, Information Technology University, Pakistan

Abstract

The future smart cities trend will be towards Internet of Things (IoT), IoT create dynamic connection in ubiquitous manner. Smart cities offer ease and flexibility for daily life matters. By using small devices that are connected to cloud servers based on IoT, network traffic between these devices is growing exponentially. Whose security is a concerned issue, since ratio of cyber-attack may make the network traffic vulnerable. This paper discusses the latest machine learning approaches in related work further to tackle the increasing rate of cyber-attacks machine learning algorithm is applied on IoT based network traffic data. The proposed algorithm train itself on data and identify different sections of devices interaction by using supervised learning which is consider as a classifier related to specific IoT device class. The simulation results clearly identify the attacks and producing less false detections.

Keywords: IoT; Traffic security; Deep learning; Classification; Cyber-attack

Abbreviations: IoT: Internet of Things; SDN: Software Defined Network; WSN: Wireless Sensor Network; DL: Deep Learning; DNN: Deep Neural Network; TNR: True Negative Result; FPR: False Positive Result

Introduction

Our smart cities will be governed through internet of things (IoT). Coffee machines talking with your clock, your clock interacting with your smartphone for schedule payments. IoT has a wide architecture that act as umbrella over extension of internet with physical devices. Still there exists many challenges for IoT based transactions. Security is one of that challenge. Security relates to hiding of information and restricting unauthorized access to devices for accessing the network. Such as many harmful devices can act as a terminal to payment gateways. Such end points if connected to network may threatens security breach by manipulating information. Thus, security and privacy issues are main concern and the importance is rising. Many governments have issued interconnected devices security act to secure this future networking paradigm. To analyze and detect network intrusion requires the power of machine learning tools. Through machine learning, the system would be able to figure out solutions for intrusions problems. System learns through dataset based on classifiers.

Classifiers are the backbone of machine learning as they create observations for making decisions. Classification of dataset is already used in many applications for the purpose of security analysis, such as detection anomalies. Challenges of security can be categorized as cyber-attacks and zero-day attacks. There exist many vulnerabilities related cyber-attack but one of the most difficult exploitations is zero-day attacks. A zero-day issue is a software security problem the flaw does not have a patch for it. The whole network is exploited if the concern software is breached. By zero-day mean that the developer has zero-day time. In this scenario the hackers inject Department of Software Engineering, Lahore Garrison University [1-3] malware in the network before the network administrators have time to recover or secure the software from the attack. Usually the zero-day attacks are on publicly accessed software that does not has security patches.

IoT is comprised of variety of devices forming network architecture irrespective of their operational techniques. This becomes a challenge for providing security for various types of network traffic data. The main properties of these network data are mostly periodic diagnosis, data analysis, monitoring etc. The usage application becomes exploited if the data is tempered. Usually software defined network (SDN) applications has zero-day attacks and have many zero-day vulnerabilities. If attacker get control over SDN application it can expose the whole network. Zero-day attacks effects also depend on detection mode. There exist different types of detection modes. The expected vulnerability varies from software to software. First the hackers identify the flaw in the security of particular software leading to zero-day attacks. It is clear from the fact that zero-day attacks probability is increased if there are delays for updating security patches.

Background

a. **Traffic Classification:** For anomaly detection and traffic classification, usually bi-directional network flows are considered. These are composed of a collection of ordered packets, exchanged between two terminal points, and are uniquely identified through the following quintuple: destination IP address, source IP address, destination port, source port, transport protocol. Source and destination ports and addresses may be pairwise interchangeable and identify the two single main unidirectional sub-flows (from source to destination and vice versa) a flow is made of.

Internet traffic can be attained by using standard network sniffers like network emulators, tcpdump1 and Wireshark2 [4]. They allowance one to get traffic traces, composed of numerous packets belonging to different sessions or flows, flowing inside public or private networks. Historically, the main traffic classification methods can be roughly divided into three categories [5]: Content-based, Session-based and Statistical approaches. The usage of well- known ports belongs to the second category, while the exhaustive packet payload analysis is a proponent of the first category and the third category, which exploits concepts of statistics, information theory as well as artificial intelligence, and usually does not require any application-level protocol information. As concerns the inherent nature of statistical traffic classification approaches, they usually perform their tasks at two different levels:

i. at a coarse-grained level, to identify a larger group of protocols (e.g., bulk transfer, mailing, web browsing, etc.), and not a specific protocol.

ii. at a fine-grained level, to detect the particular application protocol that generated a certain flow (Figure 1) [6].

b. Perception Layer with Security Attacks

The perception or device layer is also referred to as the physical layer. It includes objects with attached sensors, smart meters, robots, cameras, etc. The perception layer identifies and collects physical parameters and the target sensor data. For example, data related to physical aspects like movements, vibrations, chemicals in the atmosphere, heat, orientation, humidity, or acceleration. These data are sent to the network layer and then to an information processing system [8]. There are two technologies we can use at the perception layer i.e., Wireless Sensor Network (WSN) and Radio Frequency. The perception layer is vulnerable to different kinds of attacks depending upon the type of technology being used e.g., jamming, tampering, exhaustion and relay attacks, etc. [9].

c. Network Layer with Security Attacks

It is the layer responsible for the transmission of data across different networks through gateways and interfaces using communication technologies. Data from the perception layer is carried out by the network layer and transmitted to IoT devices, hubs, and the gateway through networks [10]. Some of the examples of attacks to which the network layer is vulnerable include Sybil, blackhole, sinkhole, wormhole, IP spoofing, hijacking and smurf.

d. Application Layer with Security Attacks

The application layer is the final layer in this architecture. This layer prepares and shows data as well as offers a variety of applications to various types of customers, defining various smart applications for IoT usage, such as smart health, homes, cities, industries, and transportation. Based on object sensor data, this layer presents the user with a specific application [10]. Security is a major concern in this layer, with regular attacks such as the following:

i. **Malicious Code Injection:** These attacks make use of code within the software, which damages the system or has other unwanted consequences and can avoid detection by anti-virus software. The code can be triggered automatically or when the user performs a certain action [11].

ii. **Malicious Scripts:** IoT and network devices connected to the internet are vulnerable to this type of attack. The attack is carried out by running malicious codes or x-scripts that appear to be normal scripts and that the user must access in order for data theft and system failure to occur [12]. Data distortion attack: Using code within the software, this type of attack damages the system or leads to another unwanted impact on the system and remains undetected by anti-virus applications [12].

e. Deep Learning algorithms

Deep Learning (DL) is a subset of machine learning that encompasses approaches for simulating information processing in biological neural systems [13]. Receives distinct inputs from another layer and reorganizes the information hierarchically, allowing feature learning and pattern categorization to be performed. In environments with a high level of complexity, DL algorithms are generally thought to be more appropriate than other machine learning approaches (i.e., several attributes and a great number of data). The training of a neural network is divided into two phases:

i. **Back-propagation phase:** this phase allows one to enhance overall network performance by giving the correct and updated weights to the connection between the nodes, as well as bias values, if necessary, with the goal of enhancing overall neural network performance.

ii. **Feed-forward phase:** In classification problems, the network nodes are activated from the input layer, which typically contains a number of nodes equal to the number of investigated characteristics, to the output layer, and also a number of nodes equal to the number of classes. Except for the nodes in the input layer, the successive nodes in the intermediate layers represent neurons that activate their output using an appropriate and ad-hoc activation function [14].

Related Work

Smart infrastructures such as smart home, smart grid system including intelligent transportation and other smart domains as well with the perennial evolution of the autonomous IoT domain. In order to achieve an autonomous communication infrastructure interacting collaboratively. Therefore, it requires a lot of security measurements to control the zero attacks over these devices and their communicated data [1]. IoT infrastructure is quite collaborated and contain mesh network of devices that require usage of processing tasks and external data storage. The backbone of IoT infrastructure is based on wireless communication in order to send periodic data, the involved devices are spread in ubiquitous manner throughout the geographical space on a wireless communication those are either a peer-to-peer system or centralized architecture, or a Cloud based infrastructure. By introducing heterogeneity of devices and network types especially in 5G involves a new scale of security threats [2]. Already their exists various research works in order to tackle these intangible and tangible risks are in the existing system [3].

Basically, the architecture of IoT is subdivided into three main layers those are i) application layer, ii) network layer and iii) perception layer. This section deals with the previous related work related to security attacks on IoT data. IoT performance is affected by these attacks. The security is related by three main criteria: confidentiality, integrity and availability. IoT infrastructure is a collection of collaborating devices those can communicate with each other without human intervention. This infrastructure is still evolving and need many improvements at different level. The three layer of architecture is elaborated in [15-17]. Multiple possible attacks and different vulnerabilities are discussed in [17-21]. Ioannis Andrea et al. classifies attacks into four groups those are based on the vulnerability issued by an adversary faced during the attack. It is difficult to implement a solution for each attack because of computing and battery power restrain. Based on security issues of IoT, there is an immense need to find a common solution which will cover most of the issues at one solution (Table 1) [21-26].

Proposed

Like previous work [27], in this research study different approach is opted, a system that can detect the variation of common IoT cyber-attack using the machine learning techniques exploiting the power of Machine vector optimization was proposed. The proposed system employs the Deep neural network (DNN), along with its associated machine learning algorithms to classify the dataset records.

Experiment

The assessment has been performed on the aforementioned integrated dataset in order to identify malicious traffic attacks. The evaluation is performed using the deep learning architecture. The metrics that we used to evaluate the classification results have been the following: Precision, Recall, Accuracy and F-measure. Precision has been evaluated as the proportion of samples that truly belong to a given attack among all those which were assigned to it. It is computed as the ratio of the number of relevant detected samples (true positive) to the sum of irrelevant detected samples (false positives) and relevant detected samples (true positives):

$$\text{Precision} = \frac{\text{true positives}}{\text{true positives} + \text{false positives}} \quad 1$$

The recall, on the other side, has been defined as the proportion of samples tagged to a certain attack among all samples that really belong to the attack. It is computed as the ratio of relevant detected samples (true positive) to total relevant samples (sum of true positives and false negatives):

$$\text{Recall} = \frac{\text{true positives}}{\text{true positives} + \text{false negatives}} \quad 2$$

The F-score or F-measure, is the weighted harmonic mean of precision and recall, and is computed according to the formula given below:

$$\text{F} - \text{Score} = 2\frac{\text{PR}}{\text{P+R}} \quad 3$$

where P and R are precision and recall, respectively. However, precision and recall can be calculated both on average and per class, the accuracy is an overall metric and has been computed as the ratio of the sum of true positives and true negatives to the total number of samples:

$$\text{Accuracy} = \frac{\text{tp} + \text{tn}}{\text{tp} + \text{fn} + \text{tn} + \text{fp}} \quad 4$$

where tp means true positives, tn means true negatives, fn means false negatives, and fp means false positives.

In this section the experiment conducted over the proposed approach is presented in form of malware types where True negative result (TNR) is the number of instances correctly classified as normal traffic and False positive result (FPR) is the number of instances incorrectly classified as malware traffic.

How to cite this article: Anum A. Classification of IoT Traffic Security Attacks Using Deep Learning. Curr Trends Fashion Technol Textile Eng 2025; 9(4): 555767. DOI: 10.19080/CTFTTE.2025.09.555767

The experiment was conducted on a physical machine, running on Tesla T4 specifications using Google Collab. The supervised learning algorithm was used as a classifier in this experiment. There are many tests which carried out to evaluate the success of the detection method and determine the accuracy rate of the proposed classifier. The proposed method is trained on the created training data-set and the evaluation results are reported in (Table 1-3).

Table 1: comparative analysis of related studies.

Author Name	Paper Title	Main Elements
Gueltoum Bendiab et al. 2020 [21]	Residual neural network (ResNet- 50)	In this Research they introduced a unique approach that apply machine learning and visual representation to identify pernicious network traffic. Res Net50 produced results in identification of malware network traffic with 94.50 % accuracy rate.
Irina Baptista et al. 2019 [22]	Self-organizing incremental neural network (SOINN)	This Research presents a new technique for malware detection based on the binary visualization and self-organizing incremental neural network with the accuracy of 91.7 % and 94.1 %
Kazi Abu Tahir et al. 2019 [23]	Artificial neural network (ANN)with a support vector machine	In this study they have presented and find best model to classify the network traffic using SVM and ANN supervised learning technique with the accuracy of 94.02 %
Xianwei Gao et al. 2019 [24]	Deep neural network (DNN) with ensemble voting	The method of ensemble learning was used in this study to improve the detection effect and shows the results with 85.2% accuracy.
Chrisitiana Ioannou et al. 2019 [25]	ML-IDS-based SVM system	To detect abnormalities within the internet of things the use of support Vector Machine (SVM) learning detection model was used and shows the detection accuracy level up to 100% when the sinkhole and Blackhole attacks were present and when the model was evaluated in a different network topology it shows 81 % accuracy for all routing attacks.
Parachi Shukla 2017 [26]	Neural network hybrid learning (K means plus decision trees)	In this study they present three new Intrusion Detection Systems (IDSs) and all the three IDS are Scalable and centralized approaches. The detection rate for varying size of random IOT networks shows 70-93% results using K-means, similarly decision based and hybrid approaches achieved 71- 81% and 71-75% respectively. Although the hybrid IDS get lower detection rate but it is more accurate than other two approaches because it eliminates false positive significantly.

Table 2: Accuracy Chart obfuscated.

Malware Types	TPR	FPR	Precision	Recall	F-Measure	Accuracy
Virus	0.918	0.056	0.946	0.918	0.933	0.93
Worm	0.94	0.081	0.924	0.94	0.932	0.931
Trojan	0.898	0.035	0.96	0.898	0.928	0.945

Table 3: Accuracy Chart Non-obfuscated.

Malware Types	TPR	FPR	Precision	Recall	F-Measure	Accuracy
Virus	0.937	0.04	0.961	0.937	0.95	0.951
Worm	0.966	0.05	0.954	0.966	0.93	0.944
Trojan	0.902	0.033	0.959	0.902	0.935	0.956

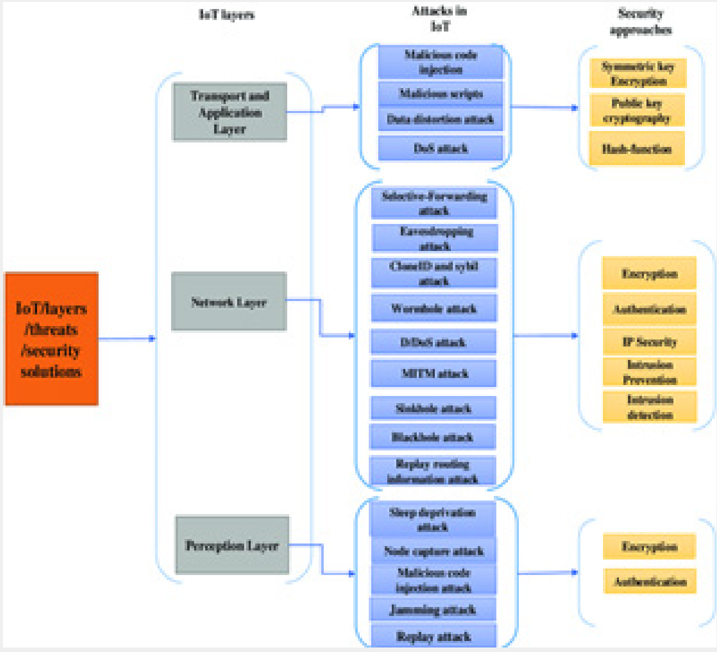

Figure 1: Classification of IoT layers, threats and security approaches [7].

Conclusion

In this paper machine vector optimization was used on supervised learning based on Dnn deep learning mechanism. The intrusion detection dataset was used for classification of zero-day attacks. The results are shown with accuracy reaching approximately 90%. False detection was avoided much of the time. Field of exploit record is constantly evolving in both complexity and quantity, for this reason it becomes difficult to collect data for future and existing exploitations activities. Deep learning methods are based on the assumption that the malicious record is different from the usual accessing data. For this record anomaly detection cannot be used as such type of exploitation is differential from usual data.

References

1. RH Weber (2010) Internet of Things - New security and privacy challenges. Computer Law & Security Review 26(1): 23-30.
2. S Sicari, A Rizzardi, LA Grieco, A Coen-Porisini (2015) Security, privacy and trust in Internet of things: The road ahead. Computer Networks 76: 146-164.
3. K Zhao, L Ge (2013) A survey on the internet of things security. IEEE Pp: 663-667.
4. L Veltri, L Davoli, R Pecori, A Vannucci, F Zanichelli (2019) NEMO: A flexible and highly scalable network EMulatOr. SoftwareX 10: 100248.
5. R Pecori, L Veltri (2014) A statistical blind technique for recognition of internet traffic with dependence enforcement. IEEE Pp: 328-333.
6. C Callegari, P Ducange, M Fazzolari, M Vecchio (2021) Explainable internet traffic classification. Appl Sci 11(10): 1-19.
7. A Gaware, SB Dhonde (2016) A survey on security attacks in wireless sensor networks. IEEE 1(8): 536-539.
8. J Deogirikar, A Vidhate (2017) Security attacks in IoT: A survey. IEEE Pp: 32-37.
9. K Aarika, M Bouhlal, R Ait Abdelouahid, S Elfilali, E Benlahmar (2020) Perception layer security in the internet of things. Procedia Computer Science 175: 591-596.
10. L Wallgren, S Raza, T Voigt (2013) Routing attacks and countermeasures in the RPL-based internet of things. Int J Distrib Sens Networks 9(8).
11. HA Abdul-Ghani, D Konstantas, M Mahyoub (2018) A comprehensive IoT attacks survey based on a building-blocked reference model. Int J Adv Comput Sci Appl 9(3): 355-373.
12. N Abosata, S Al-Rubaye, G Inalhan, C Emmanouilidis (2021) Internet of things for system integrity: A comprehensive survey on security, attacks and countermeasures for industrial applications. Sensors 21(11): 3654.
13. CD Mccaig (1990) Electric Fields in Vertebrate Repair. Edited by RB Borgens, KR Robinson, JW Vanable, ME McGinnis Pp: 310. (Alan R. Liss, New York, 1989.) $69.50 hardback. ISBN 0 8451 4274, Exp Physiol 75(2): 280-281.
14. MW Gardner, SR Dorling (1998) Artificial neural networks (the multilayer perceptron) - a review of applications in the atmospheric sciences. Atmospheric Environment. 32(14-15): 2627-2636.
15. S Li (2017) Security Architecture in the Internet of Things. Secur Internet Things Pp: 27-48.
16. R Mahmoud, T Yousuf, F Aloul, I Zualkernan (2016) Internet of things (IoT) security: Current status, challenges and prospective measures. IEEE 5(4): 336-341.
17. I Andrea, C Chrysostomou, G Hadjichristofi (2016) Internet of Things: Security vulnerabilities and challenges. Proc - IEEE Symp Comput Commun Pp: 180-187.
18. SN Uke, AR Mahajan, RC Thool (2013) UML Modeling of Physical and Data Link Layer Security Attacks in WSN. Int J Comput Appl 70(11): 25-28.

How to cite this article: Anum A. Classification of IoT Traffic Security Attacks Using Deep Learning. Curr Trends Fashion Technol Textile Eng 2025; 9(4): 555767. DOI: 10.19080/CTFTTE.2025.09.555767

19. L Hong, HC Yong, QH Zhang (2012) The survey of RFID attacks and defenses. IEEE Pp: 0-3.

20. F Kandah, Y Singh, C Wang (2011) Colluding injected attack in mobile ad-hoc networks. IEEE Pp: 235-240.

21. G Bendiab, S Shiaeles, A Alruban, N Kolokotronis (2020) IoT malware network traffic classification using visual representation and deep learning. IEEE Pp: 444-449.

22. I Baptista, S Shiaeles, N Kolokotronis (2019) A novel malware detection system based on machine learning and binary visualization. IEEE Pp: 20-24.

23. KA Taher, BMY Jisan, MM Rahman (2019) Network intrusion detection using supervised machine learning technique with feature selection. IEEE Pp: 643-646.

24. X Gao, C Shan, C Hu, Z Niu, Z Liu (2019) An Adaptive Ensemble Machine Learning Model for Intrusion Detection. IEEE Access 7: 82512-82521.

25. C Ioannou, V Vassiliou (2019) Classifying security attacks in IoT networks using supervised learning. IEEE Pp: 652-658.

26. P Shukla (2018) ML-IDS: A machine learning approach to detect wormhole attacks in Internet of Things. 2017 Intell Syst Conf Pp: 234-240.

27. R Pecori, A Tayebi, A Vannucci, L Veltri (2020) IoT Attack Detection with Deep Learning Analysis. 2020 International Joint Conference on Neural Networks (IJCNN) Pp: 1-8.

DOI: 10.19080/CTFTTE.2025.09.555767