EAI Endorsed Transactions
on Smart Cities

Research Article **EAI.EU**

An Intelligent Machine Learning based Intrusion Detection System (IDS) for Smart cities networks

Muhammad Yaseen Ayub[1,*], Usman Haider[2], Ali Haider[1], Muhammad Tehmasib Ali Tashfeen[3], Hina Shoukat[1] and Abdul Basit[4]

[1]Department of Computer science, COMSATS University Islamabad, Attock, Pakistan (E-mail: yaseen.ayub@ieee.org, sp17-bse-018@ciit-attock.edu.pk, fa18-bcs-053@cuiatk.edu.pk)
[2]Department of Electrical Engineering, National University of Computer & Emerging Sciences, Peshawar, Pakistan (E-mail: usmanhaider@ieee.org)
[3]School and Electrical and Electronics Engineering, FAST National University Peshawar Pakistan (E-mail: alitashfeen@gmail.com)
[4]Department of Electrical and Computer Engineering (ECE), COMSATS University Islamabad Campus (E-mail: abdulbasitmujahid925@gmail.com)

Abstract

INTRODUCTION: Internet of Things (IoT) along with Cloud based systems are opening a new domain of development. They have several applications from smart homes, Smart farming, Smart cities, smart grid etc. Due to IoT sensors operating in such close proximity to humans and critical infrastructure, there arises privacy and security issues. Securing an IoT network is very essential and is a hot research topic. Different types of Intrusion Detection Systems (IDS) have been developed to detect and prevent an unauthorized intrusion into the network.
OBJECTIVES: The paper presents a Machine Learning based light, fast and reliable Intrusion Detection System (IDS).
METHODS: Multiple Supervised machine learning algorithms are applied and their results are compared. Algorithms applied include Linear Discriminant analysis, Quadratic Discriminant Analysis, XG Boost, KNN and Decision Tree.
RESULTS: Simulation results showed that KNN Algorithm gives us the highest accuracy, followed by XG Boost and Decision Tree which are not far behind.
CONCLUSION: A fast, secure and intelligent IDS is developed using machine learning algorithms. The resulting IDS can be used in various types of networks especially in IoT based networks.

Keywords: IoT, IDS, Machine learning.

Received on 31 October 2022, accepted on 23 January 2023, published on 08 March 2023

doi: 10.4108/eetsc.v7i1.2825

1. Introduction

In the modern age of technological inventions, overall world dynamics is changed. Due to wireless communication and IoT networks connectivity is made possible. According to analytics, in 2022 around 14.4 billion IoT devices are connected [1]. In near future IoT devices will exceed up to 41 billion. Wireless sensor networks will provide better solutions for tracking and monitoring. There exist many applications of IoT networks which include home automation, digital banking and security systems. With the help of IoT based camera surveillance business shops and homes can be secured from intruders [2-6]. Collectively these applications form the basis of future Smart cities.

Smart cities, in particular, are heavily dependent on IoT networks for various critical services such as transportation, energy management, and public safety. This

[*] Corresponding author. Email: yaseen.ayub@ieee.org

increased dependence makes smart cities more vulnerable to cyber-attacks [7]. Security is considered the main problem with IoT based networks. Attacker tries to hijack IoT network by sending false data packets. Due to that network becomes vulnerable and intruder easily unbalances the entire system [8]. In smart cities there is extensive use of IoT networks which makes its security a huge concern. Attackers can exploit vulnerabilities in IoT devices to gain unauthorized access to sensitive information, disrupt city services, or cause physical damage. This makes intrusion detection a critical requirement for ensuring the security of smart cities [9]. Tele-medicine is a new concept in smart cities where doctor will operate and consult the patient remotely. Therefore, intruder can disturb the process by deploying DoS/DDoS, Sybil, spoofing, wormholes and man-in-the middle attack [10-12]. This can cause some serious life threatening situation for the patient. Figure 1, depicts the concept of IoT network of multiple devices using an IDS and its advantage in case of any intrusion

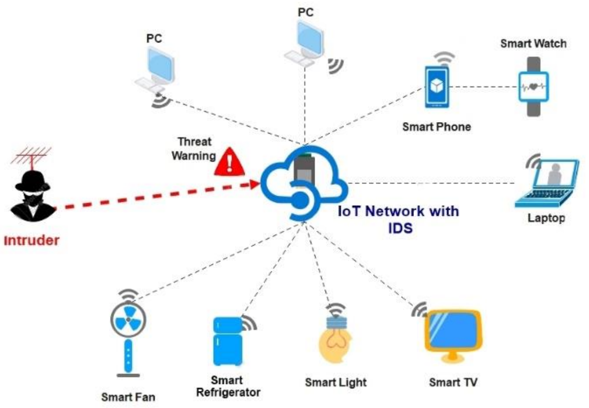

Figure 1. IoT network using concept of Intrusion Detection System

However, to make smart city environment safe from such attacks, threat detection is very much necessary. Therefore, Intrusion detection system (IDS) plays an important role in identification of various attacks on IoT-networks [13]. This research paper presents the concept of IDS using machine learning techniques for optimal detection of cyber-attacks. Figure 1, shows the concept of IDS in IoT networks.

Section 2 presents literature review of all research work that has been done recently in this domain. Section 3 explains intrusion detection systems in detail along with their different types, followed by section 4 which describes real time applications of IoT networks in a smart city concept. Then section 5 discusses simulation environment and simulation results generated by applying machine learning techniques on UNSW-NB15 dataset. At last section 6 presents conclusion and future discussions.

2. Literature Survey

This section presents limitations related to IoT-networks. In, IoT based communication networks sending information from one node to another is quite tough. Therefore, nature inspired E-AntHocNet has improved overall standards of communication. But still security is the main concern which needs to be addressed with possible solutions [14-16]. Machine learning technique decision tree enhance connectivity in between nodes by using received signal strength indicator (RSSI). Due to cyber-attacks on IoT networks connectivity will be unbalanced [17]. Intelligent detection system is introduced which can easily detect DoS/ DDoS and ping of death attacks. Markov chain distribution is used to balance false positive and false negative which lead to the problem of high accuracy [18]. Queue based traffic management is used to monitor data packets of IoT-networks. Anomaly based IDS is designed using Poisson distribution to minimize false alarm and missed detection. The proposed system is able to identify ping of death attacks but still higher attack probabilities need to be evaluated which use to degrade network performance [19]. Table 1 present's limitation of various proposed machine learning based IDS using different techniques as well as stimulation environment.

Table 1. Machine learning techniques & Limitations

Reference	**Machine Learning Techniques**	**Type of IDS**	**Simulation Tool**	**IDS Limitations**
[38]	Fusion Decision	Anomaly-based	TEST BED	Unable to detect host attack payload monitored attacks.
[39]	KNN & RSL	Hybrid	SDN and blockchain	Accuracy can be improved.
[40]	RNN	Hybrid	Python 3.0	RNN has a slow and complex training process and faces difficulty with long sequence.
[41]	RF	Anomaly-based	IoT System	Anomaly-based approach is deficient on true alarm rate
[42]	RF	Anomaly-based	SCADA	Less accurate than a

				hybrid model
[43]	ANN	Hybrid	MATLAB	ANN Technique usually lack in accuracy to some extant
[44]	SVM	Anomaly-based	MATLAB	Accuracy needs to be improved
[45]	DNN	Anomaly-based	TensorFlow & Python	Mitigation required for False Alarm
[46]	CNN	Anomaly-based	Python	Data Labeling is a better practice helps the algorithm’s better understanding
[47]	SNN, b-XG Boost & DNN	Anomaly-based	Python	Precision refinement is requisite.

3. Intrusion Detection System for IoT-Network

IoT Networks are usually poorly secured so the fact is that the critical data, they are carrying is vulnerable to various kind of attack. An IDS acts as an alarm that beeps in case of any possible attack [20]. IDSs have been more common because they continuously analyze the network traffic thus no unverified packet passed unattended. Currently researchers are more interested to impose various methodologies of Machine learning and deep learning powered with various algorithms on IoTs for the detection of intrusion [21-22]. In smart cities with such extensive use of IoT networks and in such close proximity of humans with sometimes sensitive data on them, it is absolutely necessary to incorporate strong intrusion detection system (IDS) that mitigates the threat of information leakage and network hijacking which. If in smart city a critical network is hijacked, it can result in loss of precious and sensitive information. It can also lead to life threatening situation. Thus protecting smart city infrastructure against possible attacks is very important. The advancement in IoT security has led to detection even on sensor node in IoT network [23]. There are three common types of IDS:

- Anomaly-based IDS
- Signature-based IDS
- Hybrid IDS

3.1 Anomaly Based IDS for IoT Networks

The anomaly-based detection system search and validate the IoT network pattern with the normal-behavior thus any anomaly beyond a specific level is considered as a threat and system is warned and system learns gradually. It has a threshold defined which acts as a boundary, any change in normal network behavior beyond that threshold is classified as a threat. Anomaly-based detection system overcomes various barriers of excellence like it can detect zero-day error and has capability to sense unknown attacks but has high false alarm rate. [24][25].

3.2 Signature Based IDS for IoT Networks

Signature-based Intrusion Detection System corroborates the network traffic pattern with the pre-existing signatures and makes a decision regarding an intrusion on basis of their match. They are also called Rule Based Intrusion Detection System. Their limitation is that they can only detect and classify those attacks which are already stored in its database. Any attack with unsaved pattern passes un-attended. This type of IDS has low false alarm rate but is unable detect zero-day error [24-26].

3.3 Hybrid Based IDS for IoT Networks

A Hybrid-based IDS is combination of both types so it can detect both zero-day attacks as well as pre-defined attack patterns. IT is a very flexible and customizable IDS, it can be customized to prioritize certain types of threat depending on scenario. With this approach the low false alarm rate and high detection rate is achieved thus precision and accuracy of IDS is improved [26-27].

.

4. Real-Time Application of IoT-Networks in smart cities

IoT market is growing continuously and researchers are pointing towards more and more application of IoTs. The concept of smart cities rely heavily on use of IoT networks for faster communication and automation. The world’s next target is automation and IoT Network is the tool to achieve this goal. The researchers have found the most interesting applications of IoT networks in smart cities scenario such as in Smart Traffic Management, Emergency Response, Health Care, Smart Homes, Smart Grids, Agriculture, smart monitoring etc. [28]. Some of the applications are further explained below:

4.1 Smart Traffic Management.

IoTs sensors can be installed on roads, intersections and other key areas to monitor traffic patterns in real time. These IoT sensors then can collect certain data about traffic flow, vehicle speeds, traffic density etc. Which can then be used for the optimization of traffic signal and routing to improve traffic flow and reduce congestion [29] [30]. This can be very useful in smart cities during peak traffic times as it can help reduce delays and improve the overall efficiency of the road network.

Another application of IoT in smart traffic management can be the integration of traffic data with public transport system. This can allow for more efficient routing and scheduling of busses and trains as well as the integration of real-time traffic data into public transport journey planning apps so people can know about traffic situation in a particular area before planning any trip or traveling plan.

4.2 Emergency Response

In Smart Cities, the use of IoT networks for emergency response can involve the installation of sensors in key areas such as public buildings, streets and parks to detect emergencies in real-time. These sensors can be triggered by factors such as smoke, fire or extreme temperatures to alert the authorities of potential emergencies. IoT networks can also be used to gather real-time data on the location and status of emergency services vehicles, allowing for more efficient routing and deployment of these resources in response to emergencies [31].

Another use can be integration of emergency data with public warning systems, such as sirens or messaging system. This can allow authorities to quickly and efficiently alert the public of any potential dangers and provide guidance on how to respond. IoT networks can be integrated in smart cities and they can help improve the speed and efficiency of emergency response efforts, leading to a faster resolution of emergencies and a reduction in the impact on the community. Thus creating a smart and safer smart city environment for public [32].

4.3 IoT for Healthcare

IoTs have the most critical advantage in healthcare. They have increased facility of Medicare with minimal expenditure even in remote areas. Smart IoT wearables can monitor a patient’s vital signs in real-time and alert healthcare professionals to any potential risks. Now any medical officer can monitor his patient without paying him personal visit or keeping patient in the hospital. Sensors applied for the patient’s care shares data with the doctor through IoT network and thus complete examination of the results is not a big deal anymore [33].

4.4 IoT based Smart Home

IoT has played an important role in home automation. Almost all home appliance i.e., AC, refrigerator, washing machine lights, fans, door locks etc. are now available in smart version even vehicles have been shifted towards IoT network thus they can be accessed remotely. IoT sensors can play a key role in security of a smart home in smart cities. Sensors can monitor and protect the home from potential threats such as burglaries or fire. A smart home has many sensors like Fire & Smoke Sensor, Gas sensor etc. that alert the user if any parameter crosses the threshold. So, a smart home with IoT network ensures the safety of residents [3] [34].

4.5 IoT for Smart Grid

The purpose of smart grid is to provide electricity to the customers by means two-way digital communication. A smart grid can track each consumption of the electricity at all the locations of the system. Smart grid targets have been achieved via IoT. Through an IoT network, a smart grid is capable of disaster as well as operation monitoring on high voltage transmission lines, efficiency, accuracy and operation period that is very strenuous in manual systems [35].

4.6 IoT for Agriculture

The production of the agriculture is going to increase using IoT through smart farming. IoT is been used for the monitoring of crops as well as animals through various tools and sensors connected through IoT network like monitoring of greenhouse temperature, humidity of field, disease diagnosis etc. Various machinery used in agriculture is been smart now can be controlled remotely through IoT network. Moreover, UAVs are also been deployed in the modern farming and agriculture [36].

4.7 IoT in Smart Cities

With the advancing world, the first idea is smart cities collectively creating a smart world. The evolution of smart city is parallel to the evolution of all its components. A smart health system, smart transport system, smart buildings, smart energy management, smart administration, smart industries and smart security etc. will collectively be the building blocks of a smart city and IoT provides the base to this progression [37].

5. Simulation Environment

For simulation python is used to do experimentation on IoT-networks. UNSW-NB15 dataset is utilized which is having updated network traffic information. Machine learning techniques like linear discriminant analysis, quadratic discriminant analysis, XG Boost, KNN and decision tree are simulated [48-54], which generated very good results. Table 2, shows results of machine learning classifiers where KNN is having better accuracy compared to the rest of algorithms about 98.3061%. The overall explanation of table 2 is illustrated in figure 2.

Table 2. Accuracy of Machine Learning Techniques

Algorithms	**Accuracy**
Linear Discriminant Analysis	97.6717
Quadratic Discriminant Analysis	94.0314
XG Boost	98.2507
KNN	98.3061
Decision Tree	98.2137

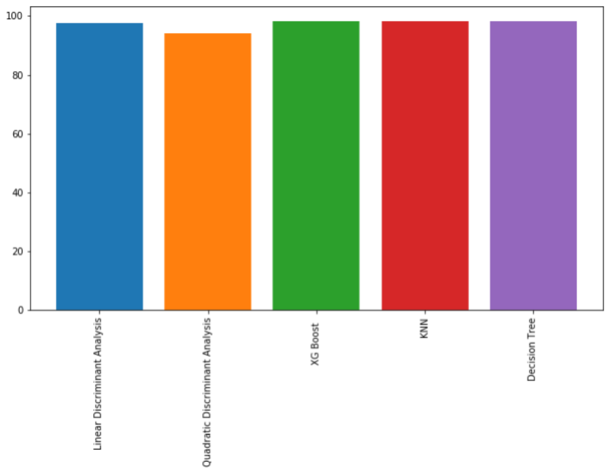

Figure 2. Machine learning algorithms like linear discriminant analysis, quadratic discriminant analysis, XG Boost, KNN and decision tree using UNSW-NB15 dataset’

6. Conclusion and Future Directions

IoT networks can be deployed in almost every field. There exist many problems in IoT networks due to that intruder easily attack and unbalance entire network. This paper has introduced machine learning techniques to detect possible cyber-attacks from updated Australian dataset called UNSW-NB-15. Types of intrusion detection system in IoT networks are incorporated which include anomaly, signature and hybrid. Different IoT-based applications are being discussed which provide a clear picture of limitations and vulnerabilities. Around five machine learning techniques like linear discriminant analysis, quadratic discriminant analysis, XG Boost, KNN and decision tree are utilized.

This paper is giving investigation of security countermeasures. Especially, the approach of intrusion detection system is used to identify various cyber-attacks. Moreover, in near future, as IoT devices are increasing continuously with the passage of time. IDS using supervised machine learning, deep learning, computational intelligence, optimization, genetic algorithm, supervised learning, reinforcement and sliding mode controller is helpful to detect possible cyber-attacks. Also, new dataset for network security is the need for researchers. Scientists must focus on real-time applications regarding intrusion detection system. In addition, novel security-based routing protocols need to be designed for secure communication with in network.

References

[1] Sairam KV, Kumar AP. A Review on Internet of Things based SWSN.

[2] Kadhim KT, Alsahlany AM, Wadi SM, Kadhum HT. An overview of patient’s health status monitoring system based on Internet of Things (IoT). Wireless Personal Communications. 2020 Oct;114(3):2235-62.

[3] Stolojescu-Crisan C, Crisan C, Butunoi BP. An IoT-based smart home automation system. Sensors. 2021 Jan;21(11):3784.

[4] Khanboubi F, Boulmakoul A, Tabaa M. Impact of digital trends using IoT on banking processes. Procedia Computer Science. 2019 Jan 1;151:77-84.

[5] Jeong JI. A study on the IoT based smart door lock system. InInformation Science and Applications (ICISA) 2016 2016 (pp. 1307-1318). Springer, Singapore.

[6] Olasupo TO. Wireless communication modeling for the deployment of tiny IoT devices in rocky and mountainous environments. IEEE Sensors Letters. 2019 May 22;3(7):1-4.

[7] Ahsaan SU, Mourya AK. Prognostic modelling for smart cities using smart agents and IoT: A proposed solution for sustainable development. EAI Endorsed Transactions on Smart Cities. 2021 May 13;5(16):e3-.

[8] Shukla P. ML-IDS: A machine learning approach to detect wormhole attacks in Internet of Things. In2017 Intelligent Systems Conference (IntelliSys) 2017 Sep 7 (pp. 234-240). IEEE.

[9] Pooja G, Sundar R, Harshini R, Arjuna S. Recent Trends and Challenges in Smart Cities. EAI Endorsed Transactions on Smart Cities. 2022 Sep 21;6(3).

[10] Nawir M, Amir A, Yaakob N, Lynn OB. Internet of Things (IoT): Taxonomy of security attacks. In2016 3rd international conference on electronic design (ICED) 2016 Aug 11 (pp. 321-326). IEEE.

[11] Chehida S, Baouya A, Bozga M, Bensalem S. Exploration of impactful countermeasures on IoT attacks. In2020 9th Mediterranean Conference on Embedded Computing (MECO) 2020 Jun 8 (pp. 1-4). IEEE.

[12] Tsiknas K, Taketzis D, Demertzis K, Skianis C. Cyber threats to industrial IoT: a survey on attacks and countermeasures. IoT. 2021 Mar;2(1):163-86.

[13] Bagaa M, Taleb T, Bernabe JB, Skarmeta A. A machine learning security framework for iot systems. IEEE Access. 2020 May 21;8:114066-77.

[14] Khan IU, Qureshi IM, Aziz MA, Cheema TA, Shah SB. Smart IoT control-based nature inspired energy efficient routing protocol for flying ad hoc network (FANET). IEEE Access. 2020 Mar 18;8:56371-8.

[15] Khan IU, Nain Zukhraf SZ, Abdollahi A, Imran SA, Qureshi IM, Aziz MA, Hussian Shah SB. Reinforce based optimization in wireless communication technologies and routing techniques using internet of flying vehicles. InThe 4th international conference on future networks and distributed systems (ICFNDS) 2020 Nov 26 (pp. 1-6).

[16] Khan IU, Abdollahi A, Jamil A, Baig B, Aziz MA, Subhan F. A Novel Design of FANET Routing Protocol Aided 5G Communication Using IoT. Journal of Mobile Multimedia. 2022 Apr 4:1333-54.

[17] Khan IU, Alturki R, Alyamani HJ, Ikram MA, Aziz MA, Hoang VT, Cheema TA. RSSI-controlled long-range communication in secured IoT-enabled unmanned aerial vehicles. Mobile information systems. 2021 Mar 1;2021.

[18] Khan IU, Abdollahi A, Alturki R, Alshehri MD, Ikram MA, Alyamani HJ, Khan S. Intelligent Detection System Enabled Attack Probability Using Markov Chain in Aerial Networks. Wireless Communications and Mobile Computing. 2021 Sep 9;2021.

[19] Abdollahi A, Fathi M. An intrusion detection system on ping of death attacks in IoT networks. Wireless Personal Communications. 2020 Jun;112(4):2057-70.

[20] Sherasiya T, Upadhyay H. Intrusion detection system for internet of things. Int. J. Adv. Res. Innov. Ideas Educ.(IJARIIE). 2016;2(3).

[21] Hodo E, Bellekens X, Hamilton A, Dubouilh PL, Iorkyase E, Tachtatzis C, Atkinson R. Threat analysis of IoT networks using artificial neural network intrusion detection system. In2016 International Symposium on Networks, Computers and Communications (ISNCC) 2016 May 11 (pp. 1-6). IEEE.

[22] Roopak M, Tian GY, Chambers J. An intrusion detection system against ddos attacks in iot networks. In2020 10th annual computing and communication workshop and conference (CCWC) 2020 Jan 6 (pp. 0562-0567). IEEE.

[23] Jan SU, Ahmed S, Shakhov V, Koo I. Toward a lightweight intrusion detection system for the internet of things. IEEE Access. 2019 Mar 28;7:42450-71.

[24] Ramadan RA, Yadav K. A novel hybrid intrusion detection system (IDS) for the detection of internet of things (IoT) network attacks. Annals of Emerging Technologies in Computing (AETiC), Print ISSN. 2020 Dec 20:2516-0281.

[25] Ramadan RA, Yadav K. A novel hybrid intrusion detection system (IDS) for the detection of internet of things (IoT) network attacks. Annals of Emerging Technologies in Computing (AETiC), Print ISSN. 2020 Dec 20:2516-0281.

[26] Abdollahi A, Fathi M. An intrusion detection system on ping of death attacks in IoT networks. Wireless Personal Communications. 2020 Jun;112(4):2057-70.

[27] Khraisat A, Gondal I, Vamplew P, Kamruzzaman J, Alazab A. A novel ensemble of hybrid intrusion detection system for detecting internet of things attacks. Electronics. 2019 Oct 23;8(11):1210.

[28] Attia TM. Challenges and opportunities in the future applications of IoT technology.

[29] Rizwan, P., Suresh, K. and Babu, M.R., 2016, October. Real-time smart traffic management system for smart cities by using Internet of Things and big data. In *2016 international conference on emerging technological trends (ICETT)* (pp. 1-7). IEEE.

[30] Fiore, S., Elia, D., Pires, C.E., Mestre, D.G., Cappiello, C., Vitali, M., Andrade, N., Braz, T., Lezzi, D., Moraes, R. and Basso, T., 2019. An integrated big and fast data analytics platform for smart urban transportation management. *IEEE Access*, *7*, pp.117652-117677.

[31] Mohammad, N., Muhammad, S., Bashar, A. and Khan, M.A., 2019. Formal analysis of human-assisted smart city emergency services. *Ieee Access*, *7*, pp.60376-60388.

[32] Shah, S.A., Seker, D.Z., Rathore, M.M., Hameed, S., Yahia, S.B. and Draheim, D., 2019. Towards disaster resilient smart cities: Can internet of things and big data analytics be the game changers?. *IEEE Access*, *7*, pp.91885-91903.

[33] Pradhan B, Bhattacharyya S, Pal K. IoT-based applications in healthcare devices. Journal of healthcare engineering. 2021 Mar 19;2021.

[34] Asadullah M, Raza A. An overview of home automation systems. In2016 2nd international conference on robotics and artificial intelligence (ICRAI) 2016 Nov 1 (pp. 27-31). IEEE.

[35] Ou Q, Zhen Y, Li X, Zhang Y, Zeng L. Application of internet of things in smart grid power transmission. In2012 third FTRA international conference on mobile, ubiquitous, and intelligent computing 2012 Jun 26 (pp. 96-100). IEEE.

[36] Kim WS, Lee WS, Kim YJ. A review of the applications of the internet of things (IoT) for agricultural automation. Journal of Biosystems Engineering. 2020 Dec;45(4):385-400.

[37] Gaur A, Scotney B, Parr G, McClean S. Smart city architecture and its applications based on IoT. Procedia computer science. 2015 Jan 1;52:1089-94.

[38] Al-Nashif Y, Kumar AA, Hariri S, Luo Y, Szidarovsky F, Qu G. Multi-level intrusion detection system (ML-IDS). In2008 International Conference on Autonomic Computing 2008 Jun 2 (pp. 131-140). IEEE.

[39] Derhab A, Guerroumi M, Gumaei A, Maglaras L, Ferrag MA, Mukherjee M, Khan FA. Blockchain and random subspace learning-based IDS for SDN-enabled industrial IoT security. Sensors. 2019 Jul 15;19(14):3119.

[40] Ullah S, Khan MA, Ahmad J, Jamal SS, e Huma Z, Hassan MT, Pitropakis N, Buchanan WJ. HDL-IDS: a hybrid deep learning architecture for intrusion detection in the Internet of Vehicles. Sensors. 2022 Feb 10;22(4):1340.

[41] Hussein AY, Falcarin P, Sadiq AT. Enhancement performance of random forest algorithm via one hot encoding for IoT IDS. Periodicals of Engineering and Natural Sciences (PEN). 2021 Aug 11;9(3):579-91.

[42] Zolanvari M, Teixeira MA, Gupta L, Khan KM, Jain R. Machine learning-based network vulnerability analysis of industrial Internet of Things. IEEE Internet of Things Journal. 2019 Apr 18;6(4):6822-34.

[43] Wang G, Hao J, Ma J, Huang L. A new approach to intrusion detection using Artificial Neural Networks and fuzzy clustering. Expert systems with applications. 2010 Sep 1;37(9):6225-32.

[44] Chahal JK, Gandhi V, Kaushal P, Ramkumar KR, Kaur A, Mittal S. KAS-IDS: A Machine Learning based Intrusion Detection System. In2021 6th International Conference on Signal Processing, Computing and Control (ISPCC) 2021 Oct 7 (pp. 90-95). IEEE.

[45] Prethi KN, Nithya S, Sangeeth DM, Rani RS, Praveen Kumar S. DNN Based Intelligent IDS for Anomaly Detection. International Journal of Advanced Research in Engineering and Technology. 2020 Oct 17;11(9).

[46] Yoshimura N, Kuzuno H, Shiraishi Y, Morii M. DOC-IDS: A Deep Learning-Based Method for Feature Extraction and Anomaly Detection in Network Traffic. Sensors. 2022 Jun 10;22(12):4405.

[47] Bedi P, Gupta N, Jindal V. I-SiamIDS: an improved Siam-IDS for handling class imbalance in network-based intrusion detection systems. Applied Intelligence. 2021 Feb;51(2):1133-51.

[48] Moustafa N, Slay J. UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). In2015 military communications and information systems conference (MilCIS) 2015 Nov 10 (pp. 1-6). IEEE.

[49] Moustafa N, Slay J. The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set. Information Security Journal: A Global Perspective. 2016 Apr 4;25(1-3):18-31.

[50] Moustafa N, Slay J, Creech G. Novel geometric area analysis technique for anomaly detection using trapezoidal area estimation on large-scale networks. IEEE Transactions on Big Data. 2017 Jun 14;5(4):481-94.

[51] Moustafa N, Creech G, Slay J. Big data analytics for intrusion detection system: Statistical decision-making using finite dirichlet mixture models. InData analytics and decision support for cybersecurity 2017 (pp. 127-156). Springer, Cham.

[52] Sarhan M, Layeghy S, Moustafa N, Portmann M. Netflow datasets for machine learning-based network intrusion detection systems. InBig Data Technologies and Applications 2020 Dec 11 (pp. 117-135). Springer, Cham.

[53] Moustafa N, Turnbull B, Choo KK. 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 Sep 24;6(3):4815-30.

[54] Koroniotis N, Moustafa N, Sitnikova E, Slay J. Towards developing network forensic mechanism for botnet activities in the IoT based on machine learning techniques. InInternational Conference on Mobile Networks and Management 2017 Dec 13 (pp. 30-44). Springer, Cham.