IoT Intrusion Detection Taxonomy

Subjects: Computer Science, Artificial Intelligence
Contributor: Khalid Albulayhi

The taxonomy includes (1) IoT security attacks, (2) IoT architecture layers, (3) intrusion-detection systems for IoT, (3) DL techniques used in the IoT IDSs, (4) common datasets used in the evaluation of the DL systems, and (5) their classification strategies. The different areas included in the taxonomy are in various ways interconnected as root causes of IoT security vulnerabilities in IoT and/or solutions to counter such causes.

Keywords: anomaly-based IDS ; deep learning ; IoT security ; IoT-IDS Logic

1. Introduction

IoT technologies communicate without the need for human-to-human or human-to-computer interaction. IoT has increasingly been adopted by organizations to streamline their operations and is one of the fastest growing technology fields; by the end of 2030, estimates have IoT at 50 billion devices, which includes everything from smartphones to kitchen appliances [1]. IoT innovations are contributing to improvements across real-life smart applications (e.g., cities, healthcare, transportation, and education). Concomitant cutting-edge and large-scale adoption of IoT technology has introduced new security challenges. Adherence to IoT security requirements is hindered by the complexity and integrative arrangements of new and somewhat ad-hoc contexts. IoT devices are connected mostly over wireless networks and are typically utilized in an unattended fashion. In this type of environment, an attacker may easily gain both physical or logical access to these devices illegally. An attacker with assumed malicious intent may indeed cause critical, life-threatening consequences.

To counter the IoT security conundrum, researchers first opted for adopting conventional security mechanisms, including encryption, authentication, access control, network security, and application security. However, such adoptions of security technologies have proved inadequate and have needed enhancement to suit the various contextual needs of their respective environments. Nevertheless, implementing security measures against specific security threats has usually been effective, though often thwarted by new attack Methods and Tactics (M&T). For example, the Mirai botnet caused large-scale Distributed Denial of Service (DDoS) attacks by exploiting IoT devices. While amplifying DDoS, these recent attacks utilize spoofed-source IP addresses to circumvent current solutions targeted to the Mirai botnet M&T. These solutions have motivated newer, more sophisticated attacks that are more complex and more destructive than the original Mirai botnet attributed attacks. Therefore, investigating effective IoT security countermeasures remains a research priority.

Many related surveys on IoT already exist in the literature that cover different aspects of deep learning in cybersecurity. Our comparison of previous studies is based on several key properties as shown in **Table 1**. These surveys [2][3][4][5][6][7][8][9][10][11][12][13] provide a modest focus on IoT intrusion detection. Most studies are either descriptive of the IoT architecture, or they present the various IDSs as a general overview for a particular project evaluation and verification purpose. References [2][3][6][11] are completely dedicated to IoT architectures and include an incomplete assessment of some applications and protocols. References [4][12] propose a six-layer architecture for the IoT domains. However. IoT security and IDSs were not considered in their study. In [13], the architecture, protocols, and privacy are described only as brief IoT security concepts, including the interconnection between the objects of things. In [7], the authors presented a survey of IDS in IoT but nothing about DL/ML techniques in IDS. Several attacks targeting protocol topology (the Routing Protocol for Low-Power and Lossy Networks (RPL), IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN)) are discussed in [5] without classifying those attacks on an IoT layered architecture connected with IDS. Reference [8] similarly provides a classical comparative analysis for several existing papers based on advantages and disadvantages. Their focus, furthermore, concentrates on the attacks without due consideration of the ML/DL methods as a general solution.

Table 1. Comparison of Intrusion Detection Systems (IDSs) properties.

Survey Area	Survey Content	Design	Focused Domain	Attacks	ML/DL Methods	Type of Experiment	Reference
IoT Vision:	IoT application	six-layer IoT architecture	IoT architecture	√	-	-	[4] 2014
IDS in IoT	IDS in IoT	-	IDS	√	ML	Statistical analysis	[7] 2018
		Five research questions	IDS	√	-	-	[8] 2019
	IDS	-	IDS	√	-	-	[9] 2018
	IoT architecture IoT security	IoT-IDS architecture	IDS	√	-	-	[6] 2018
IoT Security-Based Data Analysis	IoT security	Five-layer IoT architecture	IoT Security	√	ML	-	[11] 2020
IoT Architectures and Applications	IoT architectures	IoT taxonomy	Five-layer architecture	-	-	-	[3] 2017
IoT-Based Info of Things		-	IoT architecture	-	-	-	[2] 2013
IoT Architecture		IoT survey taxonomy	IoT architecture, Protocols and security Privacy	-	-	-	[13] 2020
Attacks	Attacks	-	RPL and 6LoWPAN in IoT	√	-	-	[5] 2015
NIDS for IoT	NIDS	IoT threats classification	Three-layer architecture, IoT threats NIDS	√	ML	Statistical analysis	[10] 2019
ML/DL Methods for IoT Security	ML/DL in IoT IoT threats	IoTsys and threats ML/DL taxonomy	IoT security Six-layer IoT architecture	√	ML/DL	-	[12] 2020

Accordingly, the thesis of this paper is as follows: IoT architecture standards in term of compatibility and difference between those standards are discussed. This reconciles and creates a mapping between those various IoT architectures with respect to IoT security aspects making the IoT ecosystem robust against intrusions. A novel comprehensive taxonomy is presented that includes state-of-the-art deep learning for IoT-IDS in terms of (a) IoT targeted attacks, (b) IoT architecture, (c) various IDSs, (d) deep learning approaches, and (e) common IoTIDS datasets. The potential attacks and requisite security needs are proposed for each IoT layer defined in **Table 1**. A fine-grained review on anomaly-based IDSs in the IoT ecosystem using deep learning approaches and traditional anomaly-based IDS approaches is provided. A comparative and descriptive analysis of different anomaly-based IDS approaches in terms of strategy, advantage, and disadvantage is also presented. An experimental study of the performance of four ML approaches, (a) LR, (b) SVM, (c) DT, and (d) ANN, is performed using the Bot-IoT [14] and IoTID20 datasets [15].

2. Taxonomy of Deep Learning for IoT-IDS Logic

Hindy et al. [16] classified various common threats using the seven-layer OSI model. Those various threats are presented as a taxonomy here based on the tools need to carry out said attacks. In [17], the authors presented an overall taxonomy based on public IDS-established datasets. The references [3][4][11][12] provided new IoT architectures and classified current IoT architecture. Other investigators have focused on deep learning techniques, which are classified deep learning methods based on their view of knowledges. In [18], for example, the authors reviewed deep learning-based IDS taxonomy, whereas in [19], the authors provided a taxonomy based on machine learning methods. This section classifies deep learning for IoT-IDS through various aspects. The taxonomy described in **Figure 1** houses the aspects associated with IDS expertise by facilitating industry, government, and investigators to develop an intelligent intrusion-detection system in the IoT ecosystem. **Figure 1** provides a detailed taxonomy of deep learning approaches used in IDSs. The taxonomy includes the various areas that are important to understanding IoT security issues and their solutions. The taxonomy includes (1) IoT security attacks, (2) IoT architecture layers, (3) intrusion-detection systems for IoT, (3) DL

techniques used in the IoT IDSs, (4) common datasets used in the evaluation of the DL systems, and (5) their classification strategies. The different areas included in the taxonomy are in various ways interconnected as root causes of IoT security vulnerabilities in IoT and/or solutions to counter such causes.

In **Figure 1**, on the leftmost branch, IoT security attacks are enumerated along with the corresponding layer needed to detect them. Indeed, IoT architectures are vulnerable to various threat actors and attack methodologies. These attacks could be passive or active and internal or remote, as seen in **Table 1** and **Figure 2**. The passive attacks monitor for vulnerabilities and do not disturb IoT ecosystem services (i.e., collecting information needed for future penetration attempts). Active attacks disrupt (i.e., interrupt/block) the operation of targeted IoT devices or IoT ecosystems. These attacks and threats include but are not limited to the methods listed in **Figure 1** (e.g., data accessibility, man-in-the-middle, denial of service, distributed denial-of-service attack, eavesdropping, sniffing, routing attack, sybil, replay spoofing, and mass node authentication). Section 3 explains more about the challenges of IoT security Issues.

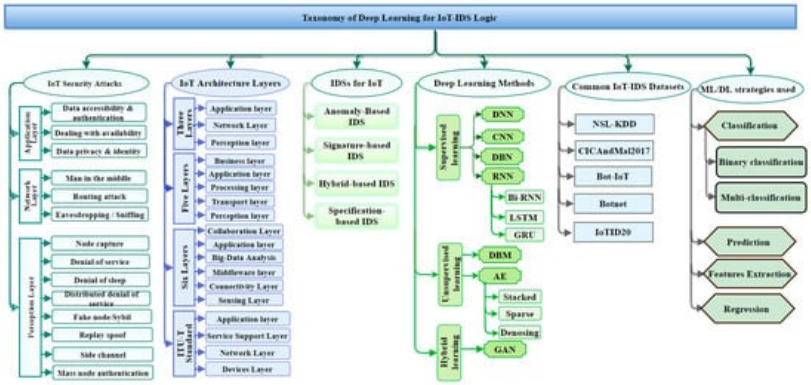

Figure 1. Taxonomy of Deep Learning for IoT-IDS Logic.

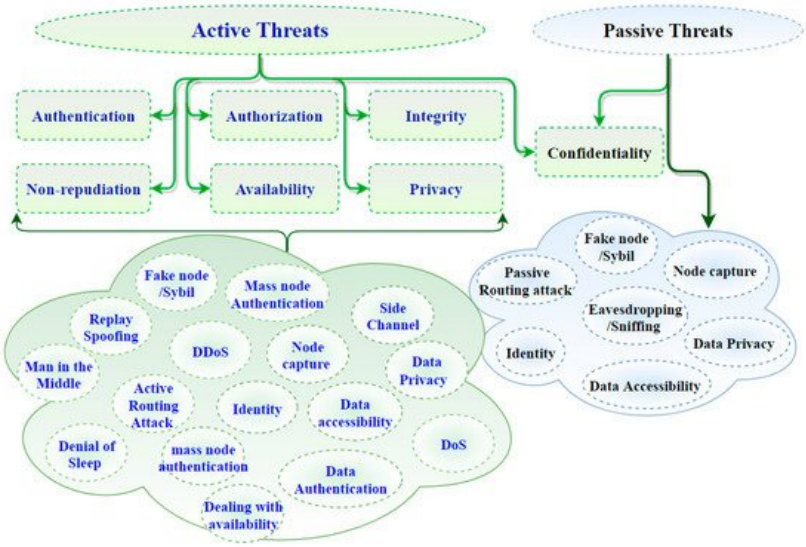

Figure 2. Passive and active threats in the IoT system.

Many studies have proposed, developed, and empirically evaluated different approaches for IDSs [20][21][22][23][24][25]. There are primarily four different categories as shown in **Figure 1**: (1) anomaly-based intrusion-detection system (AD-IDS), (2) signature-based intrusion-detection system (S-IDS), (3) hybrid-based intrusion-detection system (Hybrid-IDS), and (4) specification-based IDS. AD-IDS depends on established known patterns for normal behavior. Behavior outside the realm of “normal” is considered anomalous, thus causing some sort of warning or alert. S-IDS relates to the known pattern (signature) of malicious traffic to detect attacks. The zero-day (unknown; never been seen before) attack cannot be detected by S-IDSs. Specification-based IDS and hybrid-IDS attempt to leverage complementary capabilities by integrating the first two types (AD-IDS and S-IDS). ML and DL algorithms are good examples of the core capability used in AD-IDS. The snort tool is an excellent example of S-IDS [26][27][28].

DL models can be categorized based on the primary goal for the analysis, such as classification, feature extraction, prediction, and expression. The feature-extraction technique plays a significant role in extracting important features, especially in high-dimensional data, such as IoT ecosystem. Feature extraction is significant for creating a suitable prediction or classification model. Most studies describe how to create non-handcrafted features of the data as the basis for training their IDS model for the purpose of enhancing the quality of classification, prediction, and/or regression

outcomes. In classification, the model organizes the existing traffic data into two classes, benign (normal) or malicious traffic (a binary classification), with the goal of minimizing false-negative and false-positive rates. Another strategy is to create a model that can handle multi-classification to categorize the abnormal patterns into different malicious attack types. To build a robust prediction model, the feature extractions must be carried out before building the predictive application. A prediction model analyzes the past data and generates a predictive model to forecast future data. It may be a possible solution for transmission issues of IoT sensors data to cloud applications. A prediction model plays an important role to solve spatial-temporal problems in IoT ecosystem. It plays an important role in improving industrial IoT products, reducing the cost, and providing good decision making. The regression model comes with two different kinds of regression: linear regression and nonlinear regression. It fits the time-series problems. It began to surface in IoT ecosystem as one of the solutions for spatial-temporal problems, but it remains the least popular in the IoT research community. To preview those strategies, refer to **Figure 1**.

3. IoT Security Challenges

One important challenge reported in the literature [2][3][4][5][7][8][9][10][11][12][13] is securing IoT technologies, which can be life threatening. A harmful scenario can result with Integrated Smart-Devices (ISD) when exploited by hackers, especially in industrial IoT applications or Internet of Vehicles (IoV). There is a number of IoT technology-hacking scenarios as illustrated in [29][30] that could cause a high level of harm to the system. IoT information security issues are associated with the preservation of authentication, authorization, integrity, confidentiality, non-repudiation, availability, and privacy [31][32]. Security issues and challenges related to IoT technologies can be approached from aspects of issues associated with different IoT layers. Some studies [4][6][33] have proposed security requirements for each layer within the IoT architecture separately, whereas some other references [8][12][24][26][27][28] remain focused on analysis and presentation of the potential threats that attack each layer. This paper seeks to combine security requirements against threats to propose a three-layer IoT architecture. Accordingly, the most basic IoT architecture, the three-layered architecture, provides a simple platform from which to present security requirements and concerns as well as threats/exploits at each layer of the architecture as illustrated by considering **Table 2** combined with **Figure 2**.

Table 2. IoT architecture, attacks, and security requirements.

Layers	Attacks	Security Requirements
Application	**Data accessibility and authentication, Data privacy and identity, Dealing with availability**	**Privacy protection, Authentication, Information security management,**
Network	**Man-in-the-middle, Denial of service, Eavesdropping/Sniffing, Routing attack.**	**Authentication, Communication security, Key management, Routing security, Intrusion detection,**
Perception	**Node capture, Denial of service, Denial of sleep, Distributed denial of service, Fake node/Sybil, Replay, Side channel, Mass node authentication,**	**Data confidentiality, Lightweight encryption, Key management, Authentication.**

The security requirements of **Table 2** are defined here. Authentication is confirming the identity of a claimer. Thus, in IoT, each device is expected to have the ability to verify the identity of its user and another device for the interaction with others. Authorization is giving access to an entity to interact in the IoT environment. Integrity refers to maintaining the consistency, precision, and dependability of information, while confidentiality is about making sure that sensitive information is accessed by authorized entities. Non-repudiation guarantees holding an entity accountable for its actions. Availability ensures that IoT services are there and can be accessed from anywhere and anytime the user needs them. Privacy is a property and/or process of ensuring that private information is only accessible by authorized entities. The properties above, taken as requirements, should be enforced to achieve the highest levels of safety. However, IoT device constraints will naturally limit the extent and depth achievable, which therefore necessitates a risk assessment to understand better the threats, impacts, and tradeoffs. **Figure 2** shows how active and/or passive threats can impact those aforementioned properties within the IoT ecosystem [12][34][35][36].

4. Intrusion Detection System (IDS) in IoT

In IoT environments, anomaly-based IDSs are used to monitor the behavior of a normal network and to define a threshold to detect deviations from the normal behavior [37]. In this section, we review existing anomaly-based IDSs proposed for the purpose of protecting the security of IoT environments. We study different detection techniques employed in each of the reviewed systems. For example, in [38], the researchers present an anomaly-based IDS system that uses data-mining techniques as a distributed intrusion-detection scheme to detect anomalies in IoT environments. Their research

theoretically showed, by using the intrusion semantic to distinguish intrusive from a normal behavior, that the proposed approach is accurate and extensible. Ding et al. [39] proposed a non-cooperative differential game model that uses statistical techniques to allow all nodes in an IoT environment to choose the optimal amount of network resources to invest in information security contingent upon the state of the game. This research models selfish-nodes and malicious-nodes interactions as a differential game. The results show that malicious behavior can be discovered with high probability and high detection accuracy, good performance, and low resource consumption. Chen et al. [40] proposed a fusion-based approach for attack inference at the IoT network level. The approach details the attack and IDS procedure as a zero-sum game. The outcome of the game equilibrium is used to evaluate the network robustness achievable from a given proposed defense mechanism.

Hybrid or semi-supervised DL methods combine generative features in early phases and discriminative features at a later stage for data differentiation. Generative adversarial network (GAN) is a good example of hybrid deep learning. GAN has been adapted into the IoT environment for security purposes [41][42]. GAN may show improved success because it can learn different attack scenarios that are combined to generate samples similar to a zero-day attack scenario. Such predictive capabilities represent a higher level of learning and require that such hybrid algorithms receive extra attacks samples to learn other than existing attacks [12] that approximate suspicious zero-day behaviors. This course aims to achieve lower false-negative rates, though perhaps at the expense of higher false-positive rates. Yet, some would argue that higher learning layers are necessary to anticipate unknown, sophisticated attack strategies.

Traditional detection techniques, noted previously, have fallen short of detecting new complex attacks. As the volume of data increases, for example, into terabytes, it has become even more important to find alternative techniques. DL models can train using massive amounts of data to build robust anomaly detection systems. The model classifies the new traffic into either a normal or anomaly class [43]. DL techniques learn from hierarchical discriminative features discernable in the data. The fact that anomalous behavior is often not precisely defined poses challenges for conventional techniques; therefore, domain experts have begun to advocate solving the problem using DL techniques [44]. Some anomaly-based IDSs are used in the IoT context by employing deep learning techniques for their insights. The most common deep learning architectures employed for anomaly detection in conventional systems include CNN [45][46], DNN [47], LSTM [48][49][50], and RNN [51]. Such deep learning architectures are employed in an anomaly-detection system for either feature learning or classification [52]. **Figure 3** shows the (typical) overall framework of IDS based on deep learning.

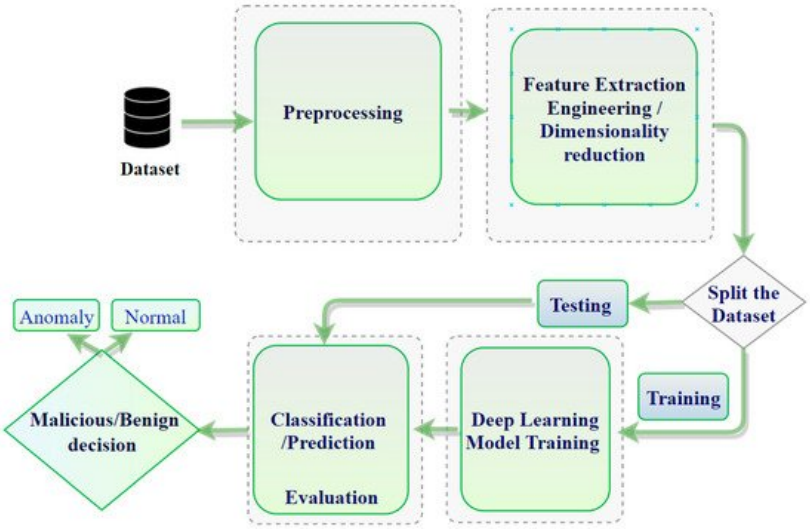

Figure 4. Diagram of the framework of IDS based on deep learning.

There are a good number of datasets available for the development and validation of IDSs. The most popular datasets used in the implementation of IoT-IDSs include NSL-KDD [53], the Bot-IoT [14], the Botnet [54], and the Android malware [55] datasets. The NSL-KDD dataset is designed to solve some of the inherent problems of the KDD'99 dataset. Thus, NSL-KDD eliminated redundant duplicate records, thereby significantly reducing the total number of records. The number of borderline (i.e., difficult) records were eliminated based on the inverse percentage so that the NSL-KDD dataset has far fewer borderline records than other datasets. Several papers focused on IoT intrusion detection have used this NSL-KDD and reported judicious and sensible results. The Android malware dataset (CICAndMal2017) contains malware and benign applications, proposed in [55]. The malware samples used to develop this dataset consist of Adware, Ransomware, Scareware, and Short Message Service (SMS) malware and include more than 80 network traffic features. The Bot-IoT is an IoT traffic-based dataset that contains more than 72,000,000 records, including DDoS, DoS, OS and Service Scan, Key-logging, and data exfiltration attacks [14]. The Bot-IoT, compared to other datasets, is dedicated to the validation of

IDS within an IoT environment. The Botnet dataset is an internet-connected devices-based dataset containing training and test data that include 7 and 16 types of botnet attacks, respectively [54]. The data featured in the botnet dataset include four groups: Byte- , Packet- , Time- , and Behavior-based . Finally, IoTID20 was developed for anomalous activity detection for the IoT ecosystem. It was generated by including laptops, smartphones, Wi-Fi cameras, and other IoT devices.

References

1. Holst, A. Number of Connected Devices Worldwide 2030; Statista: Hamburg, Germany, 2018.
2. Said, O.; Masud, M. Towards Internet of Things: Survey and Future Vision. Int. J. Comput. Netw. 2013, 5, 17.
3. Sethi, P.; Sarangi, S.R. Internet of Things: Architectures, Protocols, and Applications. J. Electr. Comput. Eng. 2017, 2017, 9324035.
4. Borgia, E. The Internet of Things vision: Key features, applications and open issues. Comput. Commun. 2014, 54, 1–31.
5. Pongle, P.; Chavan, G. A survey: Attacks on RPL and 6LoWPAN in IoT. In Proceedings of the 2015 International Conference on Pervasive Computing (ICPC), Pune, India, 8–10 January 2015; IEEE: Manhattan, NY, USA, 2015.
6. Benkhelifa, E.; Welsh, T.; Hamouda, W. A Critical Review of Practices and Challenges in Intrusion Detection Systems for IoT: Toward Universal and Resilient Systems. IEEE Commun. Surv. Tutor. 2018, 20, 3496–3509.
7. Elrawy, M.F.; Awad, A.I.; Hamed, H.F.A. Intrusion detection systems for IoT-based smart environments: A survey. J. Cloud Comput. 2018, 7, 21.
8. Hajiheidari, S.; Wakil, K.; Badri, M.; Navimipour, N.J. Intrusion detection systems in the Internet of things: A comprehensive investigation. Comput. Netw. 2019, 160, 165–191.
9. Santos, L.; Rabadao, C.; Goncalves, R. Intrusion detection systems in Internet of Things: A literature review. In Proceedings of the 2018 13th Iberian Conference on Information Systems and Technologies (CISTI), Caceres, Spain, 13–16 June 2018; IEEE: Manhattan, NY, USA, 2018.
10. Chaabouni, N.; Mosbah, M.; Zemmari, A.; Sauvignac, C.; Faruki, P. Network Intrusion Detection for IoT Security Based on Learning Techniques. IEEE Commun. Surv. Tutor. 2019, 21, 2671–2701.
11. Mrabet, H.; Belguith, S.; Alhomoud, A.; Jemai, A. A Survey of IoT Security Based on a Layered Architecture of Sensing and Data Analysis. Sensors 2020, 20, 3625.
12. Al-Garadi, M.A.; Mohamed, A.; Al-Ali, A.K.; Du, X.; Ali, I.; Guizani, M. A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security. IEEE Commun. Surv. Tutor. 2020, 22, 1646–1685.
13. Sobin, C.C. A Survey on Architecture, Protocols and Challenges in IoT. Wirel. Pers. Commun. 2020, 112, 1383–1429.
14. Koroniotis, N.; Moustafa, N.; Sitnikova, E.; Turnbull, B. Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset. Future Gener. Comput. Syst. 2019, 100, 779–796.
15. Ullah, I.; Mahmoud, Q.H. A Scheme for Generating a Dataset for Anomalous Activity Detection in IoT Networks. In Advances in Artificial Intelligence; Goutte, C., Zhu, X., Eds.; Springer International Publishing: Cham, Switzerland, 2020; pp. 508–520.
16. Hindy, H.; Brosset, D.; Bayne, E.; Seeam, A.K.; Tachtatzis, C.; Atkinson, R.; Bellekens, X. A Taxonomy of Network Threats and the Effect of Current Datasets on Intrusion Detection Systems. IEEE Access 2020, 8, 104650–104675.
17. Ferrag, M.A.; Maglaras, L.; Moschoyiannis, S.; Janicke, H. Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. J. Inf. Secur. Appl. 2019, 50, 102419.
18. Aldweesh, A.; Derhab, A.; Emam, A. Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues. Knowl. Based Syst. 2019, 189, 105124.
19. Liu, H.; Lang, B. Machine Learning and Deep Learning Methods for Intrusion Detection Systems: A Survey. Appl. Sci. 2019, 9, 4396.
20. Ghosh, A.K.; Wanken, J.; Charron, F. Detecting anomalous and unknown intrusions against programs. In Proceedings of the 14th Annual Computer Security Applications Conference, Phoenix, AZ, USA, 7–11 December 1998; IEEE Computer Society: Washington, DC, USA, 1998; pp. 259–267.
21. García-Teodoro, P.; Díaz-Verdejo, J.; Maciá-Fernández, G.; Vázquez, E. Anomaly-based network intrusion detection: Techniques, systems and challenges. Comput. Secur. 2009, 28, 18–28.

22. Abduvaliyev, A.; Pathan, A.-S.K.; Zhou, J.; Roman, R.; Wong, L. On the Vital Areas of Intrusion Detection Systems in W ireless Sensor Networks. IEEE Commun. Surv. Tutor. 2013, 15, 1223–1237.

23. Le, A.; Loo, J.; Chai, K.K.; Aiash, M. A Specification-Based IDS for Detecting Attacks on RPL-Based Network Topology. Information 2016, 7, 25.

24. Bostani, H.; Sheikhan, M. Hybrid of anomaly-based and specification-based IDS for Internet of Things using unsupervis ed OPF based on MapReduce approach. Comput. Commun. 2017, 98, 52–71.

25. Li, W.; Tug, S.; Meng, W.; Wang, Y. Designing collaborative blockchained signature-based intrusion detection in IoT env ironments. Future Gener. Comput. Syst. 2019, 96, 481–489.

26. Roesch, M. Snort–Lightweight Intrusion Detection for Networks. In Proceedings of the LISA '99: 13th Systems Administ ration Conference, Seattle, WA, USA, 7–12 November 1999; p. 11.

27. Snort—Network Intrusion Detection & Prevention System. Available online: https://www.snort.org/ (accessed on 25 Dec ember 2020).

28. Shah, S.A.R.; Issac, B. Performance comparison of intrusion detection systems and application of machine learning to Snort system. Future Gener. Comput. Syst. 2018, 80, 157–170.

29. Trappe, W.; Howard, R.; Moore, R.S. Low-Energy Security: Limits and Opportunities in the Internet of Things. IEEE Sec ur. Priv. Mag. 2015, 13, 14–21.

30. Hernandez, G.; Arias, O.; Buentello, D.; Jin, Y. Smart Nest Thermostat: A Smart Spy in Your Home; Black Hat: San Fra ncisco, CA, USA, 2015; p. 8.

31. Mouaatamid, O.E.; Lahmer, M.; Belkasmi, M. Internet of Things Security: Layered classification of attacks and possible Countermeasures. Electron. J. Inf. Technol. 2016, 9, 24–37.

32. Smadi, A.; Ajao, B.; Johnson, B.; Lei, H.; Chakhchoukh, Y.; Abu Al-Haija, Q. A Comprehensive Survey on Cyber-Physic al Smart Grid Testbed Architectures: Requirements and Challenges. Electronics 2021, 10, 1043.

33. El-Hajj, M.; Fadlallah, A.; Chamoun, M.; Serhrouchni, A. A Survey of Internet of Things (IoT) Authentication Schemes. S ensors 2019, 19, 1141.

34. Cho, K.; van Merrienboer, B.; Bahdanau, D.; Bengio, Y. On the Properties of Neural Machine Translation: Encoder-Dec oder Approaches. arXiv 2014, arXiv:1409.1259.

35. Salakhutdinov, R.; Hinton, G. Deep Boltzmann Machines. In Proceedings of the Machine Learning Research: Artificial I ntelligence and Statistics, Clearwater, FL, USA, 16–18 April 2009.

36. Hinton, G.E.; Salakhutdinov, R.R. Reducing the Dimensionality of Data with Neural Networks. Science 2006, 313, 504– 507.

37. Raza, S.; Wallgren, L.; Voigt, T. SVELTE: Real-time intrusion detection in the Internet of Things. Ad Hoc Netw. 2013, 1 1, 2661–2674.

38. Fu, R.; Zheng, K.; Zhang, D.; Yang, Y. An Intrusion Detection Scheme Based on Anomaly Mining in Internet of Things; I EEE: Manhattan, NY, USA, 2011; pp. 315–320.

39. Ding, Y.; Zhou, X.-W.; Cheng, Z.-M.; Lin, F.-H. A Security Differential Game Model for Sensor Networks in Context of th e Internet of Things. Wirel. Pers. Commun. 2013, 72, 375–388.

40. Chen, P.-Y.; Cheng, S.-M.; Chen, K.-C. Information Fusion to Defend Intentional Attack in Internet of Things. IEEE Inter net Things J. 2014, 1, 337–348.

41. Hiromoto, R.E.; Haney, M.; Vakanski, A. A secure architecture for IoT with supply chain risk management. In Proceedin gs of the 2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Te chnology and Applications (IDAACS), Bucharest, Romania, 21–23 September 2017.

42. Chen, Z.; Fu, A.; Zhang, Y.; Liu, Z.; Zeng, F.; Deng, R.H. Secure Collaborative Deep Learning against GAN Attacks in t he Internet of Things. IEEE Internet Things J. 2020, 8, 5839–5849.

43. Marín, G.; Casas, P.; Capdehourat, G. RawPower: Deep Learning Based Anomaly Detection from Raw Network Traffic Measurements; Association for Computing Machinery: New York, NY, USA, 2018.

44. Chalapathy, R.; Chawla, S. Deep Learning for Anomaly Detection: A Survey. arXiv 2019, arXiv:1901.03407.

45. Napoletano, P.; Piccoli, F.; Schettini, R. Anomaly Detection in Nanofibrous Materials by CNN-Based Self-Similarity. Sen sors 2018, 18, 209.

46. Ng, B.A.; Selvakumar, S. Anomaly detection framework for Internet of things traffic using vector convolutional deep lear ning approach in fog environment. Future Gener. Comput. Syst. 2020, 113, 255–265.

47. Gómez, J.A.; Arévalo, J.; Paredes, R.; Nin, J. End-to-end neural network architecture for fraud scoring in card payment s. Pattern Recognit. Lett. 2018, 105, 175–181.
48. Javaid, A.; Niyaz, Q.; Sun, W.; Alam, M. A Deep Learning Approach for Network Intrusion Detection System. In Proceed ings of the 9th EAI International Conference on Bio-Inspired Information and Communications Technologies (Formerly BIONETICS), New York, NY, USA, 3–5 December 2015; ACM: New York, NY, USA, 2016.
49. Wang, X.; Lu, X. A Host-Based Anomaly Detection Framework Using XGBoost and LSTM for IoT Devices. Wirel. Com mun. Mob. Comput. 2020, 2020, 8838571.
50. Wu, D.; Jiang, Z.; Xie, X.; Wei, X.; Yu, W.; Li, R. LSTM Learning With Bayesian and Gaussian Processing for Anomaly Detection in Industrial IoT. IEEE Trans. Ind. Inform. 2020, 16, 5244–5253.
51. O'Shea, T.J.; Clancy, T.C.; McGwier, R.W. Recurrent Neural Radio Anomaly Detection. arXiv 2016, arXiv:1611.00301.
52. Xu, C.; Chen, S.; Su, J.; Yiu, S.M.; Hui, L.C.K. A Survey on Regular Expression Matching for Deep Packet Inspection: A pplications, Algorithms, and Hardware Platforms. IEEE Commun. Surv. Tutor. 2016, 18, 2991–3029.
53. NSL-KDD|Datasets|Research|Canadian Institute for Cybersecurity|UNB. Available online: https://www.unb.ca/cic/datas ets/nsl.html (accessed on 20 September 2021).
54. Beigi, E.B.; Jazi, H.H.; Stakhanova, N.; Ghorbani, A.A. Towards effective feature selection in machine learning-based b otnet detection approaches. In 2014 IEEE Conference on Communications and Network Security; IEEE: Manhattan, N Y, USA, 2014.
55. Shiravi, A.; Shiravi, H.; Tavallaee, M.; Ghorbani, A.A. Toward developing a systematic approach to generate benchmark datasets for intrusion detection. Comput. Secur. 2012, 31, 357–374.