

A Survey Paper on Device Type Identification and Intrusion Detection using Deep Learning Techniques in Securing IoT Environments

Indira¹ and Dr. A K Sampath²

¹Research Scholar, School of Computer Science and Engineering, Presidency University, Bangalore, India
Email: indira@pdit.ac.in

²Assoc. Professor, School of Computer Science and Engineering, Presidency University, Bangalore, India
Email: sampath.ak@presidencyuniversity.in

Abstract—Green Internet of Things (IoT) encompasses various sectors like farming, home automation, smart transport, and wellness, aiming to simplify people's lives. However, cyberattacks pose a significant threat to IoT devices. Deep learning techniques have emerged as effective solutions for IoT security, particularly in intrusion detection. Anomaly-based Intrusion Detection Systems (IDS) are favored over signature-based detection to combat zero-day threats. This study provides a comprehensive literature review on deep learning-based anomaly detection and device classification for safeguarding IoT systems.

Index Terms— IoT, device identification, intrusion detection, deep learning, literature survey.

I. INTRODUCTION

The Internet of Things (IoT) is rapidly connecting billions of sensors and controls to the Internet, enabling seamless interactions [1]. With around 7 billion operational IoT devices worldwide [2], prioritizing smart technologies is vital for fostering sustainable economies and promoting intelligent living, security, and cultural enrichment [1]. The IoT's versatility spans various domains like smart homes, wearable technology, and healthcare, promising significant improvements in our daily lives [1].



Fig 1. Examples of IoT based applications

Numerous groups, including scientific research organizations, are actively involved in various aspects of IoT development. They have outlined a framework for understanding how IoT will impact the economy and industries in the next decade. By 2019, Cisco had delivered the majority of the world's 24 billion smart objects, establishing itself as a leading provider of IoT projects. Predictions suggest that by 2025, Huawei will introduce 100 billion IoT connections.



Fig 2. Connected IoT devices worldwide, in billions from 2018 to 2030 [5]

Figure 2 illustrates the growth of connected IoT devices worldwide from 2018 to 2030. Statistics indicate that approximately 127 new Internet-connected gadgets are added every second globally. In 2020, 63% of all electronic gadgets had internet access. Notably, IoT deployment accounted for 23% of all smart city commercial projects, with 40% of healthcare institutions incorporating embedded IoT systems. Furthermore, the cost of IoT is rising steadily as advancements in related technologies, such as automated machine systems and gadgets, continue to improve. This trend is depicted in Figure 3, illustrating worldwide investment in the Internet of Things from 2018 through 2023. In 2018, costs totaled \$616 billion, with marginal increases observed in 2019. However, a significant shift occurred in 2022 and 2023.



Fig 3. Worldwide expenditure on IoT devices and applications

The IoT market has seen significant growth, reaching 20.4 billion connections in 2022, and projected to hit 27 billion M2M connections by 2024 [3]. Forecasts suggest a market size of \$4 trillion by 2025 [3], but the lack of awareness and government guidelines on IoT security has made organizations vulnerable to cyber attacks [4]. Despite available security solutions like firewalls and IDS, new threats continue to pose challenges [5]. Prompt patching and removal of malicious IoT devices are crucial, yet tracking them within networks remains problematic [6], especially with traditional identifiers like MAC addresses and IP addresses prone to forgery, necessitating alternative methods for device identification [7].

II. SECURITY

The rapid expansion of IoT devices heightens security risks due to increasing cyber attacks and system complexity [8-10]. Despite a growing market for IoT security solutions, reports indicate prevalent attacks, emphasizing the need for better security measures [11, 12]. Standardizing platforms could enhance security, but current risk assessment techniques struggle in dynamic IoT environments [13, 14]. Protecting devices and user data is essential, necessitating comprehensive risk management frameworks [15]. The increase in IoT devices creates opportunities for criminal activity, with cybercriminals exploiting vulnerabilities across layers [16], including the perception layer facing vulnerabilities like node capturing and malicious code insertion [17, 18], and the network layer prone to phishing, DDoS, and routing attacks [21-23]. The support layer is vulnerable to DDoS, MITM, and SQL injection attacks [21-23], while smart applications in the application layer encounter security concerns like data leakage, unauthorized access, and malicious code injection [24,25].

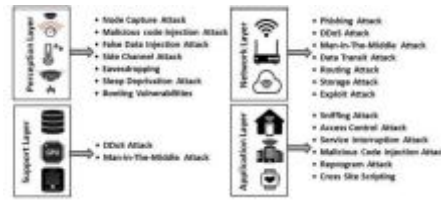


Fig 4. Attacks on different IoT layers

A. Need for IoT

The IoT necessitates robust security measures to bridge human activities with digital and physical environments [38]. AI integration enhances fraud detection and addresses security threats comprehensively, while efficient management expedites G-IoT investigations [38]. Data privacy requires regular encryption and deletion of private files. Security assessments must encompass the IoT's expansive attack surfaces, demanding a comprehensive network security approach. Key security properties like confidentiality, integrity, authentication, authorization, and availability are essential for safeguarding information and ensuring uninterrupted service amidst threats like denial of service attacks [38].

The literature review highlights various methods for device type identification and intrusion detection in IoT environments. Marchal et al. [38] developed AUDI for IoT device type identification, while Prasad et al. [62] proposed a clustering approach for Intrusion Detection Systems (IDS). Deep learning models, including CNNs, DBNs, RBMs, and RNNs, have shown superior performance in intrusion detection, contributing to enhanced security threat detection in IoT systems.

Deep learning for IDS

Ullah et al. [82] discussed the rise of deep learning in IoT intrusion detection, presenting an RNN-based model using LSTM, BiLSTM, and GRU for anomaly detection. They also proposed a hybrid model combining CNN and RNN for feature learning. Donkol et al. [83] introduced ELSTM to address shortcomings in intrusion detection, enhancing security with RNNs and mitigating issues like gradient vanishing and overfitting. Their approaches were validated using the NSL-KDD dataset, showing improved feature selection and attack classification.

Article	Techniques	Accuracy	Precisionn	Recall	FAR	F1-Measure
Lopezet al.[70]	AE	81%	8.58%	80.1%	NA	79.08
Yang et al.[88]	VAE + DNN	89.07%	86.04%	95.67%	NA	0.62%
Thamilarasu et al.[89]	DBN	NA	97%	NA	NA	NA
Shi etal. [91]	LSTM +RNN	99.35	97.96	98.79	NA	98.39
Muniret al.[92]	CNN	99	100	NA	0.007	NA
Mani muruganetal. [94]	DBN	98.29	97.22	98.35	NA	98
Diro et al.[99]	Multi-LayerDL	99.03	NA	99.28	99.11	0.86
Parra et al.[100]	CNN +LSTM	94.31	93.39	93.68	NA	93.49
Chenget al.[101]	CNN	99.89	99.88	97.98	NA	98.65
Moustafa etal. [102]	DFNN	98.5	NA	99	NA	NA

Xie et al. [103]	LSTM	NA	NA	NA	NA	NA
Zhao et al. [104]	CNN	86.96	NA	NA	NA	NA
Li et al. [105]	LSTM	97.59	83.78	2.03	NA	NA
Kim et al. [106]	AE	99.80	NA	NA	NA	NA
Hwang et al. [107]	CNN + AE	100	100	100	NA	100
Yin et al. [108]	CNN + AE	99.61	97.77	97.21	NA	98.77
Telikani et al. [109]	AE	99.62	100	100	100	0.0058
Shone et al. [110]	AE	97.86	100	100	NA	85.42
Drosou et al. [111]	GNN/ RNN	99	NA	NA	NA	NA
Deng et al. [112]	III. ML	IV. 9.77	V. 8.99	VI. 1.52	VII. .23	VIII. A

Xiao et al. [84] introduced a CNN-based Intrusion Detection System (CNN-IDS) for network attacks, employing dimensionality reduction and automatic feature extraction through CNN processing to reduce computational costs while preserving intrusion detection details.

Khanam et al. [85] proposed CFLVAE to address data imbalance in intrusion detection datasets by generating new samples for minority attack classes.

Lahasan et al. [86] stressed the importance of developing compact deep autoencoder models using a two-layer optimizer, considering input features, training examples, and hidden neuron count simultaneously, guided by the precision of a KNN classifier and the depth of the autoencoder model.

Yang et al. [88] introduced ICVAE-DNN, merging a Deep Neural Network (DNN) with Improved Conditional Variational AutoEncoder (ICVAE) for intrusion detection, enhancing identification rates for diverse attacks by exploring sparse representations. Thamilarasu et al. [89] devised a smart Intrusion Detection System (IDS) for IoT environments, ensuring protocol compatibility and effective detection of malicious activities. Shi et al. [91] proposed a botnet detection method analyzing network packet traffic patterns using time-based sampling. Munir et al. [92] presented DeepAnT, a deep learning-based approach for time series anomaly detection, utilizing unlabeled data for prediction. Gurina et al. [93] utilized deep autoencoders to detect anomalous network activity from compromised IoT devices. Kim et al. [96] employed Deep Learning (DL) in their Intrusion Detection System (IDS) research to detect Denial of Service (DoS) attacks. Jung et al. [97] developed an 8-layer Convolutional Neural Network (CNN)-based model for power usage data. Gurina et al. [98] introduced a lightweight method for anomaly-based attack identification, analyzing dynamic responses of web servers to incoming requests using a dynamic response anomaly recognizer based on an auto encode

DL Method	Attack Type Handled	Pros	Cons
RNN	R2L, DoS, U2R, Botnet, Time series anomaly detection	Best suited for environment where data is processed sequentially	Learning extended data sequences with RNNs is difficult because of the problem of the gradient disappearing or exploding.
CNN	Malware attacks	CNN is ideal for quick and effective feature extraction from raw data. Better learning with reduced training error	High computational power is required therefore it becomes a challenge for resource constrained IoT devices
Deep Autoencoder	Malware attacks, BotNet attacks	Efficient feature extraction, Dimension reduction	Computational complexity, The classification performance dips if the sample data used for training does not accurately test data.
RBM	R2L, DoS, U2R	It has a feedback mechanism which helps to extract the important attributes that can be used to capture the behaviour of IoT devices.	High computational resources for resource constrained devices, Poor feature representation if inadequate RBM is used.
DBN	R2L, DoS, U2R	Appropriate for critical feature extraction with unlabeled data training	High computation resources
GAN	BotNet, Scanning, MiTM	Ability to detect zero-day attack, It uses only one pass through the model	Complex training process, Produces the unstable results.

III. CONCLUSION

This study provides a comprehensive analysis of machine learning and deep learning methods for IoT anomaly detection, focusing on deep learning techniques for IDS in the IoT environment. It consolidates recent literature to organize and compare various studies, datasets, attack detection methods, and evaluation procedures. Additionally, it highlights challenges associated with deep learning for IoT anomaly detection, serving as a valuable resource for researchers and identifying areas for further development in IoT-specific IDS systems.

REFERENCES

- [1] Sethi, P., & Sarangi, S. R. (2017). Internet of things: architectures, protocols, and applications. Journal of Electrical and Computer Engineering, 2017.
- [2] Yu, M., Zhuge, J., Cao, M., Shi, Z., & Jiang, L. (2020). A survey of security vulnerability analysis, discovery, detection, and mitigation on IoT devices. Future Internet, 12(2), 27.
- [3] Huawei. Tap into New Growth with Intelligent Connectivity. 2018. Available online: https://www.huawei.com/minisite/gci/assets/files/gci_2018_whitepaper_en.pdf?v=20180716
- [4] Hussain, M. Z., & Hanapi, Z. M. (2023). Efficient Secure Routing Mechanisms for the Low-Powered IoTNetwork:A Literature Review. Electronics, 12(3), 482.
- [5] Statista. Several Connected Devices Worldwide2030.2020.Available online: <https://www.statista.com/statistics/802690/worldwide-connected-devices-by-access-technology>
- [6] Vega, M. Internet of things statistics facts & predictions [2020's update]. Retrieved Novemb. 2020, 30, 2020.

- [7] Mukherjee, B. Iot Statistics for 2020. Available online: <https://www.stoodnt.com/blog/iot-statistics- for-2020> (accessed on 8 November 2020).
- [8] D. F. Rajesh Kandaswamy, "Blockchain-based transformation," <https://www.gartner.com/en/doc/3869696- blockchain-basedtransformation-a-gartner-trend- insight-report/>, online;
- [9] T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on the use of blockchain for the internet of things," *IEEE Access*, vol. 6, pp. 32 979–33 001, 2018.
- [10] M. Frustaci, P. Pace, G. Aloï, and G. Fortino, "Evaluating critical security issues of the iot world: present and future challenges," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2483–2495, 2018
- [11] Atlam, H. F., & Wills, G. B. (2020). IoT security, privacy, safety and ethics. *Digital twin technologies and smart cities*, 123-149.
- [12] Shodan,<https://www.shodan.io> Hue, A., Sharma, G., & Dricot, J. M. (2021). Privacy- Enhanced MQTT Protocol for Massive IoT. *Electronics*, 11(1), 70.
- [13] Kotak, J., Shah, A., Rajdev, P.: A Comparative Analysis on Security of MQTT Brokers, In: *IET Conference Proceedings*, p. 7 (5 pp.)-7 (5 pp.)(2019)
- [14] Shah, A., Rajdev, P., Kotak, J.: Memory Forensic Analysis of MQTT Devices.(2019)arXiv preprint arXiv:1908.07835.
- [15] Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). Ai-driven cybersecurity: an overview, security intelligence modeling and research directions. *SN Computer Science*, 2, 1-18.
- [16] MahdaviFar, S., & Ghorbani, A. A. (2019). Application of deep learning to cybersecurity: A survey. *Neurocomputing*, 347, 149-176.
- [17] Ratta, P., Kaur, A., Sharma, S., Shabaz, M., & Dhiman, G. (2021). Application of blockchain and internet of things in healthcare and medical sector: applications, challenges, and future perspectives. *Journal of Food Quality*, 2021, 1-20.
- [18] 3. Nurse, J.R.C.; Creese, S.; de Roure, D. Security risk assessment in Internet of Things systems. *IT Prof.* 2017, 19, 20–26.
- [19] Malik, V.; Singh, S. Security risk management in IoT environment. *J. Discret. Math. Sci. Cryptogr.* 2019, 22, 697–709.
- [20] MarketsandMarkets. IoT Security Market Worth\$35.2 Billion by 2023. 2019. Available online: <https://www.marketsandmarkets.com/PressReleases/i ot-security.asp>
- [21] PwC. Managing Emerging Risks from the Internet of Things. 2016. Availableonline: <https://www.pwc.com/us/en/services/consulting/cybersecurity/library/broader-perspectives/managing-iot- risks.html>
- [22] Irdeto. New 2019 Global Survey: IoT-Focused Cyberattacks Are the New Normal. 2019. Available online:<https://resources.irdeto.com/global- connected-industries-cybersecurity-survey/new-2019- globalsurvey-iot-focused-cyberattacks-are-the-new- normal>
- [23] Aldmour, R., Burnap, P., & Lakoju, M. (2019). Risk assessment methods for converged IoT and SCADA systems: Review and recommendations.
- [24] Arul, R., Basheer, S., Abbas, A., & Bashir, A. K. (2021). Role of Deep Learning Algorithms in Securing Internet of Things Applications. In *Deep Learning for Internet of Things Infrastructure* (pp. 145-164). CRC Press.
- [25] Lu, Y., Hu, X., & Su, Y. (2020). Framework of industrial networking sensing system based on edge computing and artificial intelligence. *Journal of Intelligent & Fuzzy Systems*, 38(1), 283-291.
- [26] Mishra, N., & Pandya, S. (2021). Internet of things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review. *IEEE Access*, 9, 59353-59377.
- [27] M. Devi and A. Majumder, "Side-channel attack in Internet of Things: A survey," in *Applications of Internet of Things (Lecture Notes in Networks and Systems)*, J. K. Mandal, S. Mukhopadhyay, and A. Roy, Eds. Singapore: Springer, 2021, pp. 213–222.
- [28] K. O. A. Alimi, K. Ouahada, A. M. Abu-Mahfouz, and S. Rimer, "A survey on the security of low power wide area networks: Threats, challenges, and potential solutions," *Sensors*, vol. 20, no. 20, pp. 1– 19, 2020
- [29] H. Mrabet, S. Belguith, A. Alhomoud, and A. Jemai, "A survey of IoT security based on a layered architecture of sensing and data analysis," *Sensors*, vol. 20, no. 13, pp. 1–20, 2020.
- [30] K. Nirmal, B. Janet, and R. Kumar, "Analyzing and eliminating phishing threats in IoT, network and other Web applications using iterative intersection," *Peer-Peer Netw. Appl.*, pp. 1–13, Jun. 2020.
- [31] R. Vishwakarma and A. K. Jain, "A survey of DDoS attacking techniques and defence mechanisms in the IoT network," *Telecommun. Syst.*, vol. 73, no. 1, pp. 3–25, Jan. 2020.
- [32] A. Raoof, A. Matrawy, and C.-H. Lung, "Enhancing routing security in IoT: Performance evaluation of RPL's secure mode under attacks," *IEEE Internet Things J.*, vol. 7, no. 12, pp. 11536–11546, Dec. 2020.
- [33] D. Dinculeană and X. Cheng, "Vulnerabilities and limitations of MQTT protocol used between IoT devices," *Appl. Sci.*, vol. 9, no. 5, p. 848, Feb. 2019.
- [34] A. Tewari and B. B. Gupta, "Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework," *Future Gener. Comput. Syst.*, vol. 108, pp. 909–920, Jul. 2020.
- [35] Ahlawat, A. Sangwan, and V. Sindhu, "IoT system model, challenges and threats," *Int. J. Sci. Technol. Res.*, vol. 9, no. 3, pp. 6771–6776, 2020.
- [36] Prabadevi and N. Jeyanthi, "A review on various sniffing attacks and its mitigation techniques," *Indonesian J. Elect. Eng. Comput. Sci.*, vol. 12, no. 3, pp. 1117–1125, 2018.
- [37] Marchal, S., Miettinen, M., Nguyen, T. D., Sadeghi,

- [38] R., & Asokan, N. (2019). Audi: Toward autonomous iot device-type identification using periodic communication. *IEEE Journal on Selected Areas in Communications*, 37(6), 1402-1412.
- [39] Bao, J., Hamdaoui, B., & Wong, W. K. (2020, June). Iot device type identification using hybrid deep learning approach for increased iot security. In *2020 International Wireless Communications and Mobile Computing (IWCMC)* (pp. 565-570). IEEE.
- [40] Hamad, S. A., Zhang, W. E., Sheng, Q. Z., & Nepal,
- [41] S. (2019, August). Iot device identification via network-flow based fingerprinting and learning. In *2019 18th IEEE international conference on trust, security and privacy in computing and communications/13th IEEE international conference on big data science and engineering (TrustCom/BigDataSE)* (pp. 103-111). IEEE.
- [42] Salman, O., Elhadj, I. H., Chehab, A., & Kayssi, A. (2022). A machine learning based framework for IoT device identification and abnormal traffic detection. *Transactions on Emerging Telecommunications Technologies*, 33(3), e3743.
- [43] Meidan, Y., Bohadana, M., Shabtai, A., Ochoa, M., Tippenhauer, N. O., Guarnizo, J. D., & Elovici, Y. (2017). Detection of unauthorized IoT devices using machine learning techniques. *arXiv preprint arXiv:1709.04647*.
- [44] Ullah, I., & Mahmoud, Q. H. (2021, April). Network traffic flow based machine learning technique for IoT device identification. In *2021 IEEE International Systems Conference (SysCon)* (pp. 1-8). IEEE.
- [45] H. Kawai, S. Ata, N. Nakamura, and I. Oka, "Identification of communication devices from analysis of traffic patterns," in *Proc. 13th Int. Conf. Netw. Service Manage.*, Tokyo, Japan, Nov. 2017, pp. 1-5.
- A. K. Dalai and S. K. Jena, "WDTF: A technique for wireless device type fingerprinting," *Wireless Pers. Commun.*, vol. 97, no. 2, pp. 1911-1928, Nov. 2017.
- [46] M. Markus, S. Marchal, I. Hafeez, N. Asokan, A.-R. Sadeghi, and S. Tarkoma, "IoT sentinel: Automated device-type identification for security enforcement in IoT," in *Proc. IEEE 37th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Jun. 2017, pp. 2177-2184.
- [47] Charyyev, B., & Gunes, M. H. (2020). Locality- sensitive iot network traffic fingerprinting for device identification. *IEEE Internet of Things Journal*, 8(3), 1272-1281.
- [48] Gu, T., & Mohapatra, P. (2018, October). Bf-iot: Securing the iot networks via fingerprinting-based device authentication. In *2018 IEEE 15Th international conference on mobile ad hoc and sensor systems (MASS)* (pp. 254-262). IEEE.
- [49] Aneja, S., Aneja, N., Bhargava, B., & Chowdhury, R.
- [50] R. (2022). Device fingerprinting using deep convolutional neural networks. *International Journal of Communication Networks and Distributed Systems*, 28(2), 171-198. Abbas, S., Nasir, Q., Nouichi, D., Abdelsalam, M., Abu Talib, M., Abu Waraga, O., & Khan, A. U. R. (2021). Improving security of the Internet of Things via RF fingerprinting based device identification system. *Neural Computing and Applications*, 33(21), 14753-14769.
- [51] Ammar, N., Noirie, L., & Tixeuil, S. (2020, June). Autonomous identification of IoT device types based on a supervised classification. In *ICC 2020-2020 IEEE International Conference on Communications (ICC)* (pp. 1-6). IEEE.
- [52] Liu, X., Han, Y., & Du, Y. (2022). IoT Device Identification Using Directional Packet Length Sequences and 1D-CNN. *Sensors*, 22(21), 8337.
- [53] Msadek, N.; Soua, R.; Engel, T. Iot device fingerprinting: Machine learning based encrypted traffic analysis. In *Proceedings of the 2019 IEEE Wireless Communications and Networking Conference (WCNC)*, Marrakech, Morocco, 15-19 April 2019; pp. 1-8.
- [54] Pinheiro, A.J.; de M. Bezerra, J.; Burgardt, C.A.P.; Campelo, D.R. Identifying IoT devices and events based on packet length from encrypted traffic. *Comput. Commun.* 2019, 144, 8-17
- [55] OConnor, T.; Mohamed, R.; Miettinen, M.; Enck, W.; Reaves, B.; Sadeghi, A.-R. HomeSnitch: Behavior transparency and control for smart home IoT devices. In *Proceedings of the Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, Miami, FL, USA, 15-17 May 2019; pp. 128-138.
- [56] Terrell, J.; Jeffay, K.; Smith, F.D.; Gogan, J.; Keller,
- [57] J. Passive, streaming inference of TCP connection structure for network server management. In *Proceedings of the International Workshop on Traffic Monitoring and Analysis*, Aachen, Germany, 11 May 2009; pp. 42-53.
- [58] Alrawi, O.; Lever, C.; Antonakakis, M.; Monrose, F. Sok: Security evaluation of home-based iot deployments. In *Proceedings of the 2019 IEEE Symposium on Security and Privacy (sp)*, San Francisco, CA, USA, 19-23 May 2019; pp. 1362- 1380.
- [59] Trimmananda, R.; Varmarken, J.; Markopoulou, A.; Demsky, B. Packet-level signatures for smart home devices. In *Proceedings of the Network and Distributed Systems Security (NDSS) Symposium*, San Diego, CA, USA, 23-26 February 2020.
- [60] Hafeez, I.; Antikainen, M.; Ding, A.Y.; Tarkoma, S. IoT-KEEPER: Detecting malicious IoT network activity using online traffic analysis at the edge. *IEEE Trans. Netw. Serv. Manag.* 2020, 17, 45-59.
- [61] Ortiz, J.; Crawford, C.; Le, F. DeviceMien: Network device behavior modeling for identifying unknown
- [62] IoT devices. In *Proceedings of the Proceedings of the International Conference on Internet of Things Design and Implementation*, Montreal, QC, Canada, 15-18 April 2019; pp. 106-117.
- [63] Tekler, Z.D.; Low, R.; Zhou, Y.; Yuen, C.; Blessing, L.; Spanos, C. Near-real-time plug load identification using low-frequency power data in office spaces: Experiments and applications. *Appl. Energy* 2020, 275, 115391.

- [64] Prasad, M., Tripathi, S., & Dahal, K. (2020). Unsupervised feature selection and cluster center initialization based arbitrary shaped clusters for intrusion detection. *Computers & Security*, 99, 102062.
- [65] Pu, G., Wang, L., Shen, J., & Dong, F. (2020). A hybrid unsupervised clustering-based anomaly detection method. *Tsinghua Science and Technology*, 26(2), 146-153.
- [66] Abou El Houda, Z., Senhaji Hafid, A., & Khoukhi, L. (2021). A novel unsupervised learning method for intrusion detection in software-defined networks. In *Computational Intelligence in Recent Communication Networks* (pp. 103-117). Cham: Springer International Publishing.
- [67] Hanselmann, M., Strauss, T., Dormann, K., & Ulmer,
- [68] H. (2020). CANet: An unsupervised intrusion detection system for high dimensional CAN bus data. *Ieee Access*, 8, 58194-58205.
- [69] Chen, Y., Ashizawa, N., Yeo, C. K., Yanai, N., & Yean, S. (2021). Multi-scale self-organizing map assisted deep autoencoding Gaussian mixture model for unsupervised intrusion detection. *Knowledge- Based Systems*, 224, 107086.
- [70] Zoppi, T., Gharib, M., Atif, M., & Bondavalli, A. (2021). Meta-learning to improve unsupervised intrusion detection in cyber-physical systems. *ACM Transactions on Cyber-Physical Systems (TCPS)*, 5(4), 1-27.
- [71] Siddiqui, A. J., & Boukerche, A. (2021). Adaptive ensembles of autoencoders for unsupervised IoT network intrusion detection. *Computing*, 103(6), 1209-1232.
- [72] Anthi, E., Williams, L., Słowińska, M., Theodorakopoulos, G., & Burnap, P. (2019). A supervised intrusion detection system for smart home IoT devices. *IEEE Internet of Things Journal*, 6(5), 9042-9053.
- [73] Lopez-Martin, M., Carro, B., & Sanchez-Esguevillas,
- [74] (2020). Application of deep reinforcement learning to intrusion detection for supervised problems. *Expert Systems with Applications*, 141, 112963.
- [75] Yin, C., Zhu, Y., Liu, S., Fei, J., & Zhang, H. (2020). Enhancing network intrusion detection classifiers using supervised adversarial training. *The Journal of Supercomputing*, 76(9), 6690-6719.
- [76] Wazirali, R. (2020). An improved intrusion detection system based on KNN hyperparameter tuning and cross-validation. *Arabian Journal for Science and Engineering*, 45(12), 10859-10873.
- [77] Panigrahi, R., Borah, S., Bhoi, A. K., Ijaz, M. F., Pramanik, M., Kumar, Y., & Jhaveri, R. H. (2021). A consolidated decision tree-based intrusion detection system for binary and multiclass imbalanced datasets. *Mathematics*, 9(7), 751.
- [78] Khraisat, A., Gondal, I., Vamplew, P., Kamruzzaman, J., & Alazab, A. (2019). A novel ensemble of hybrid intrusion detection system for detecting internet of things attacks. *Electronics*, 8(11), 1210.
- [79] Qaddoura, R., Al-Zoubi, A. M., Almomani, I., & Faris, H. (2021). A multi-stage classification approach for iot intrusion detection based on clustering with oversampling. *Applied Sciences*, 11(7), 3022.
- [80] 76. Wu, Y., Lee, W. W., Gong, X., & Wang, H. (2020). A hybrid intrusion detection model combining SAE with kernel approximation in internet of things. *Sensors*, 20(19), 5710.
- [81] Davahli, A., Shamsi, M., & Abaei, G. (2020). Hybridizing genetic algorithm and grey wolf optimizer to advance an intelligent and lightweight intrusion detection system for IoT wireless networks. *Journal of Ambient Intelligence and Humanized Computing*, 11, 5581-5609.
- [82] Abbas, A., Khan, M. A., Latif, S., Ajaz, M., Shah, A. A., & Ahmad, J. (2021). A new ensemble-based intrusion detection system for internet of things. *Arabian Journal for Science and Engineering*, 1-15.
- [83] Mhawi, D. N., Aldallal, A., & Hassan, S. (2022). Advanced feature-selection-based hybrid ensemble learning algorithms for network intrusion detection systems. *Symmetry*, 14(7), 1461.
- [84] Khonde, S. R., & Ulagamuthalvi, V. (2019). Ensemble-based semi-supervised learning approach for a distributed intrusion detection system. *Journal of Cyber Security Technology*, 3(3), 163-188.
- [85] Tama, B. A., Comuzzi, M., & Rhee, K. H. (2019). TSE-IDS: A two-stage classifier ensemble for intelligent anomaly-based intrusion detection system. *IEEE access*, 7, 94497-94507.
- [86] Ullah, I., & Mahmoud, Q. H. (2022). Design and development of RNN anomaly detection model for IoT networks. *IEEE Access*, 10, 62722-62750.
- [87] Donkol, A. A., Hafez, A. G., Hussein, A. I., & Mabrook, M. M. (2023). Optimization of Intrusion Detection Using Likely Point PSO and Enhanced
- [88] LSTM-RNN Hybrid Technique in communication Networks. *IEEE Access*.
- [89] Y. Xiao, C. Xing, T. Zhang, and Z. Zhao, "An intrusion detection model based on feature reduction and convolutional neural networks," *IEEE Access*, vol. 7, pp. 42210-42219, 2019.
- [90] Khanam, S., Ahmedy, I., Idris, M. Y. I., & Jaward,
- [91] M. H. (2022). Towards an Effective Intrusion Detection Model Using Focal Loss Variational Autoencoder for Internet of Things (IoT). *Sensors*, 22(15), 5822.
- [92] Lahasan, B., & Samma, H. (2022). Optimized deep autoencoder model for Internet of Things intruder detection. *IEEE Access*, 10, 8434-8448.
- [93] Lopez-Martin, M.; Carro, B.; Sanchez-Esguevillas, A.; Lloret, J. Conditional Variational Autoencoder for Prediction and Feature Recovery Applied to Intrusion Detection in IoT. *Sensors* 2017, 17, 1967.
- [94] Yang, Y.; Zheng, K.; Wu, C.; Yang, Y. Improving the classification effectiveness of intrusion detection by using improved conditional variational autoencoder and deep neural network. *Sensors* 2019, 19, 2528
- [95] Thamilarasu, G.; Chawla, S. Towards Deep- Learning-Driven Intrusion Detection for the Internet of Things. *Sensors* 2019, 19, 1977.

- [96] Xu, R.; Cheng, Y.; Liu, Z.; Xie, Y.; Yang, Y. Improved Long Short-Term Memory based anomaly detection with concept drift adaptive method for supporting IoT services. *Futur. Gener. Comput. Syst.* 2020, 112, 228–242
- [97] Shi, W.-C.; Sun, H.-M. DeepBot: A time-based botnet detection with deep learning. *Soft Comput.* 2020, 24, 16605–16616.
- [98] Munir, M.; Siddiqui, S.A.; Dengel, A.; Ahmed, S. DeepAnT: A Deep Learning Approach for Unsupervised Anomaly Detection in Time Series. *IEEE Access* 2018, 7, 1991–2005
- [99] Meidan, Y.; Bohadana, M.; Mathov, Y.; Mirsky, Y.; Shabtai, A.; Breitenbacher, D.; Elovici, Y. N- BaIoT—Network-Based Detection of IoT Botnet Attacks Using Deep Autoencoders. *IEEE Pervasive Comput.* 2018, 17, 12–22.
- [100] Manimurugan, S.; Al-Mutairi, S.; Aborokbah, M.M.; Chilamkurti, N.; Ganesan, S.; Patan, R. Effective Attack Detection in Internet of Medical Things Smart Environment Using a Deep Belief Neural Network. *IEEE Access* 2020, 8, 77396–77404
- [101] Manimurugan, S.; Al-Mutairi, S.; Aborokbah, M.M.; Chilamkurti, N.; Ganesan, S.; Patan, R. Effective Attack Detection in Internet of Medical Things Smart Environment Using a Deep Belief Neural Network. *IEEE Access* 2020, 8, 77396–77404
- [102] Malaiya, R.K.; Kwon, D.; Suh, S.C.; Kim, H.; Kim, I.; Kim, J. An Empirical Evaluation of Deep Learning for Network Anomaly Detection. *IEEE Access* 2019, 7, 140806–140817
- [103] Kim, J.; Kim, J.; Kim, H.; Shim, M.; Choi, E. CNN- Based Network Intrusion Detection against Denial- of-Service Attacks. *Electronics* 2020, 9, 916.
- [104] Jung, W.; Zhao, H.; Sun, M.; Zhou, G. IoT botnet
- [105] detection via power consumption modeling. *Smart Health* 2020, 15, 100103
- [106] Gurina, A.; Eliseev, V. Anomaly-Based Method for Detecting Multiple Classes of Network Attacks. *Information* 2019, 10, 84
- [107] Diro, A.A.; Chilamkurti, N. Distributed attack detection scheme using deep learning approach for Internet of Things. *Futur. Gener. Comput. Syst.* 2018, 82, 761–768
- [108] Cheng, Y.; Xu, Y.; Zhong, H.; Liu, Y. Leveraging Semi-supervised Hierarchical Stacking Temporal Convolutional Network for Anomaly Detection in IoT Communication. *IEEE Internet Things J.* 2020, 8, 144–155
- [109] Al-Hawawreh, M.; Moustafa, N.; Sitnikova, E. Identification of malicious activities in industrial internet of things based on deep learning models. *J. Inf. Secur. Appl.* 2018, 41, 1–11. [
- [110] Xu, R.; Cheng, Y.; Liu, Z.; Xie, Y.; Yang, Y. Improved Long Short-Term Memory based
- [111] anomaly detection with concept drift adaptive method for supporting IoT services. *Futur. Gener. Comput. Syst.* 2020, 112, 228–242
- [112] Li, Y.; Xu, Y.; Liu, Z.; Hou, H.; Zheng, Y.; Xin, Y.;
- [113] Zhao, Y.; Cui, L. Robust detection for network intrusion of industrial IoT based on multi-CNN fusion. *Measurement* 2020, 154, 107450.
- [114] Li, X.; Xu, M.; Vijayakumar, P.; Kumar, N.; Liu, X. Detection of Low-Frequency and Multi-Stage Attacks in Industrial Internet of Things. *IEEE Trans. Veh. Technol.* 2020, 69, 8820–8831
- [115] Kim, S.; Hwang, C.; Lee, T. Anomaly Based Unknown Intrusion Detection in Endpoint Environments. *Electronics* 2020, 9, 1022