Deep Neural Network-Based Intrusion Detection in Internet of Things: A State-of-the-Art Review

Zhiqi Li[1,2], Weidong Fang[1,2,3(✉)], Chunsheng Zhu[4], Wentao Chen[5], Zhiwei Gao[6], Xinhang Jiang[7], and Wuxiong Zhang[1,2]

[1] Science and Technology on Microsystem Laboratory, Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences, Shanghai 201899, China
{lizhiqi,weidong.fang,wuxiong.zhang}@mail.sim.ac.cn
[2] School of Electronic, Electrical, and Communication Engineering, University of Chinese Academy of Sciences, Beijing 100049, China
[3] Shanghai Research and Development Center for Micro-Nano Electronics, Shanghai 201210, China
[4] College of Big Data and Internet, Shenzhen Technology University, Shenzhen 518118, China
[5] State Grid Xinjiang Company Limited Electric Power Research Institute, Urumqi 830011, China
[6] Ceprei Certification Body, the Fifth Electronics Research Institute of Ministry of Industry and Information Technology, Guangzhou 511370, China
[7] School of Computer Science and Technology, Wuhan University of Science and Technology, Wuhan 430081, China

Abstract. Various security threats are faced by the Internet of Things (IoT) as it enriches people's daily lives. Intrusion detection is employed as an effective method to mitigate these threats, encompassing Botnet, DDoS, and Scan attacks. Due to the rapid development of machine learning technology in recent years, deep neural networks (DNNs) emerge as powerful models utilized to significantly enhance the accuracy performance of intrusion detection systems (IDSs) and to increase their adaptability to dynamic networks. In this paper, related works proposed in the last three years are collected and selected, considering both traffic-based and behavior-based intrusion detection. Subsequently, a study and analysis of these related works is conducted. Additionally, we compare their techniques utilized, results, advantages, and disadvantages. Finally, we analyze the existing challenges and open issues and suggest some insightful future research works.

Keywords: Intrusion Detection · Internet of Things · Deep Neural Network · Machine Learning

1 Introduction

The Internet of Things (IoT) is a network formed by various devices, sensors, and objects connected through the internet, enabling interconnectivity and intelligent management [1]. In IoT, a number of personal sensitive data is often collected by devices, including users' geographical and health information. Therefore, if hackers infiltrate IoT devices,

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2024
D.-S. Huang et al. (Eds.): ICIC 2024, LNCS 14864, pp. 13–23, 2024.
https://doi.org/10.1007/978-981-97-5588-2_2

they may steal users' privacy for malicious purposes or even launch attacks on the entire network. Therefore, intrusions and attacks have become a significant security issue in IoT.

In the realm of IoT, the reliability of device connectivity hinges significantly on the security models implemented. These models used to be deployed in safeguarding user data and thwarting devices from partaking in nefarious activities. The IDSs stand out as one of the primary tools utilized to defend against malicious intrusions [2]. They often be designed based on methods such as Naive Bayes and fuzzy algorithms. However, IDSs designed based on traditional methods often struggle to adapt well to the dynamic network environment. Fortunately, intrusion and attack detection have been extensively studied in the fields of statistics and machine learning. Deep neural network (DNN) is a type of deep learning methods based on artificial neural network. They achieve high-level abstraction and processing of input data through the combination and learning of multiple layers of neurons, enabling tasks such as classification and regression [3]. Moreover, by incorporating techniques such as regularization and data augmentation, it demonstrates high generalizability and robustness based on DNNs.

Due to the numerous advantages of DNNs, a substantial amount of IDSs have been proposed based on DNNs in IoT. While some survey and review papers [4–6] on deep learning-based intrusion detection in IoT have been published, there still remains a gap for a review paper specifically focused on DNN-based intrusion detection. The main findings of this research are as follows:

1. Conducting a thorough analysis and comparison of advanced works related to trust evaluation using deep learning techniques in OSNs. Analyzing and comparing some advanced related works on intrusion detection in IoT with DNN.
2. Find that, in DDoS attacks, better performance is exhibited by network traffic-based systems. Additionally, higher accuracy is achieved by device behavior-based systems for internal threats and unknown types of attacks.
3. Analyzing challenges and open issues and suggesting some research directions.

This paper is organized as follows. The analysis and comparison of some advanced work is presented in Sect. 2. Current issues and challenges are discussed in Sect. 3, and several significant research directions worth studying are proposed in Sect. 4. Lastly, conclusions are drawn in Sect. 5.

2 Analysis and Comparison of Related Work

Due to the high generalization capability and robustness of DNNs, there has been a significant amount of research on DNN-based IDSs in IoT in recent years. We select some related works based on the influence and quality, ensuring diversity in terms of methods and techniques.

2.1 Network Traffic-Based Intrusion Detection

Real-time network communication data is analyzed by network traffic-based IDSs to detect network attacks, port scanning, and other potential intrusion behaviors. Distributed

Denial-of-Service (DDoS) attacks represent a form of network assault characterized by inundating a target system with an overwhelming volume of requests or traffic from numerous IP sources simultaneously. The flow of traffic exceeding the system's capacity leads to the target system being unable to provide services properly.

Recently, some network traffic-based IDSs have been proposed. L. Adi et al. proposed a neural network-based IDS to detect DDoS attacks [7]. It achieves higher accuracy compared to KNN-based schemes, yet its outcomes are heavily impacted by the learning rate and hidden layer's values. Besides, P. Varma et al. introduced a DDoS attack detection method based on the Enhanced Elman spike Neural Network (EENN), and a good accuracy in detecting DDoS attacks was demonstrated [8]. However, it incurred high computational overhead and time complexity.

Additionally, some researchers proposed intrusion detection strategies for DDoS based on recurrent neural network (RNN) [9, 10]. These approaches achieved an accuracy rate of up to 99%. Besides, some IDSs based on network traffic have been proposed using the DRNN [11, 12]. Dense random neural network (DRNN) was a neural network model based on random weights. Unlike traditional neural networks, the weights in the DRNN are randomly initialized and randomly updated at each training iteration. It permitted exploration of a broader weight space during training, thereby mitigating the risk of becoming ensnared in local optima and enhancing generalization capabilities. Z. Huma et al. introduced the Hybrid Deep Random Neural Network (HDRaNN), a hybrid approach designed for cyberattack detection within Industrial IoT (IIoT) environments [13]. K.-H. Le et al. proposed an intelligent IDS called IMIDS for cyber threats in IoT using CNN [14].

Machine learning technology in industrial networks have emerged as a prominent field, with IIoT being a common industrial network [15]. Intrusion often be characterized by complex patterns and features, which could be effectively modeled and captured by CNNs through multiple convolutional layers and activation functions. This facilitated the enhancement of intrusion detection accuracy [16]. However, in certain tasks involving sequential data or long-range temporal dependencies, they may struggle to effectively capture these long-term dependencies. The combination of CNNs and long short-term memory (LSTM) algorithm, known as CNN-LSTM, could effectively address the limitations mentioned above. G. Parra et al. introduced a cloud-based distributed DL framework aimed at detecting DDoS and botnet attacks [17]. This framework amalgamated two pivotal security mechanisms, operating synergistically: a Distributed Convolutional Neural Network (DCNN) model designed for detecting phishing attempts and application-layer DDoS attacks.

The practical deployment of an IDS based on DNNs has been impeded due to the constrained computing and storage capabilities of IoT devices. Researchers have attempted to design IDSs based on lightweight neural networks (LNNs) to overcome this challenge. LNN-based IDS maintenance has maintained a low model complexity and a reduced number of parameters, while achieving acceptable performance and accuracy. Additionally, R. Zhao et al. proposed a lightweight DNN-based method for network recognition in IoT [18]. It achieved high detection accuracy while having a compact system size and low time complexity. To reduce computational costs, an IDS proposed by M. Elaziz et al. with DNNs to extract optimal features from network data [19].

M. Elaziz et al. employed DNNs to extract optimal features from IoT network data and introduced an efficient feature selection technique leveraging the recently developed SI optimization Capuchin monkey search algorithm (CapSA) [20]. However, they found that the CapSA model exhibited poor generalization performance on imbalanced datasets. To enhance generalization and tackle class imbalance issues within intrusion detection datasets, A. Thakkar et al. employed an ensemble learning approach, employing label-class classifiers and utilizing DNNs as base estimators [21].

In Table 1, we summarize several proposed networks traffic-based IDSs using DNNs in IoT. The summary of the comparison on their results, advantages, and disadvantages is presented, where A, P, and R respectively represent accuracy, precision, and recall.

Table 1. Summary of Related Network Traffic-based Intrusion Detection Schemes Using DNNs in IoT

Scheme	Tech.	Dataset	Result	Advantage	Disadvantage
ADI [7]	DNN	DDoS dataset	A = 99.99%	Accuracy was significantly higher than KNN-based methods	The results were influenced greatly by the learning rate and hidden layers
VARMA [8]	EENN	CICDDoS 2018	A = 97.89%, P = 98.85%, R = 99.97%	High accuracy performance	High computational overhead and time complexity
ASWAD [9]	RNN, LSTM	CICIDS2017	A = 99.76%, P = 98.90%	Combining the advantages of three neural networks	Lacking of a realistic testing platform results in unstable reliability
YOUSUF [10]	RNN	NSL KDD	A = 99.98%, P = 99.9%, R = 99.9%	Excellent accuracy and throughput performance	A limited number of DDoS attack could be effectively detected
RED. [11]	DRNN	Synthetic	A = 98.28%	High accuracy and robustness	High time complexity
LATIF [12]	DRNN	DS2OS	A = 99.20%, P = 99.11%, R = 99.13%	High detection accuracy and small system size	The feasibility of the system has not been validated

(*continued*)

Table 1. (*continued*)

Scheme	Tech.	Dataset	Result	Advantage	Disadvantage
HUMA [13]	DRNN	DS2OS, UNSW-NB15	A = 98.56%, P = 98.25%, R = 98.36%	High accuracy in classifying the 16 types of attacks	High time complexity, and it has not been deployed on a real platform
LE [14]	CNN	UNSW-NB15	A = 96.69%	It could detect 9 types of network attacks with high f-score	The detection accuracy of IMIDS for the Backdoor attack was low
PARRA [17]	DCNN, LSTM	N_BaIoT	A = 94.3%, F1 = 93.58%	High detection rates for DDoS and Botnet	The detection of attack types was limited. High time complexity
ZHAO [18]	LNN	UNSW-NB15, Bot-IoT	A = 98.94%, 99.99%	High detection accuracy and low time complexity	The system has not been deployed and tested in a real platform
ASG. [19]	CNN	TON-IoT	A = 99.99%, P = 99.99%, R = 99.99%	Low computational costs and training expenses	Challenges still existed in practical deployment
ELAZIZ [20]	DNN	NSL-KDD, BoT-IoT, KDD99	F1 = 92.7%, 99.9%, 76.8%	Low computational costs and training expenses	Performing poorly in terms of accuracy and generalization

2.2 Device Behavior-Based Intrusion Detection

Device behavior-based IDS focuses on monitoring and analyzing the behavioral patterns of IoT devices, such as sensor data and device operation logs. By leveraging DNNs, device behavior-based IDSs can learn the normal behavior patterns of devices and identify anomalous behavior that deviates from the expected normal behavior.

DRNNs have also been used in designing behavior-based IDSs. S. Latif et al. proposed a lightweight DRNN for IoT intrusion detection [23]. It demonstrated good accuracy in binary classification and can effectively identify multiple attack types. However, it had high time complexity and energy consumption. The deep belief network (DBN) was an unsupervised learning algorithm based on a probabilistic graphical model. It consisted of multiple stacked restricted Boltzmann machines, which formed a directed

acyclic graph between layers. H. Bhor et al. proposed a detection method by combining Taylor series with spider monkey optimization algorithm and DBN [24].

Graph neural networks (GNNs) differed from traditional neural networks in that they can effectively model and learn from the nodes and edges of a graph, as opposed to handling vector and matrix data. Y. Zhang et al. proposed a framework based on a GNN for IoT to detection intrusion, but it had limitations in effectively detecting certain types of attacks [25]. A. Basati et al. introduced a lightweight architecture founded on parallel deep autoencoders, which capitalized on both local and contextual information of individual values within feature vectors [26]. On the other hand, S. Kasongo utilized various types of RNNs, such as LSTM, Gated Recurrent Unit (GRU), and Simple RNN, to develop an IDS framework [27]. Besides, P. Sanju presented an advanced heuristic algorithm with integrated RNNs to enhance intrusion detection.

We summarize several proposed device behavior-based IDSs using DNNs in IoT in Table 2. The summary of the comparison on their results, advantages, and disadvantages is presented. It shows that the majority of device behavior-based systems with DNN achieve high accuracy. However, the performance for other types may be limited.

Table 2. Summary of Related Device Behavior-based Intrusion Detection Schemes Using DNN in IoT

Scheme	Tech.	Intrusion handled	Dataset	Results	Advantage	Disadvantage
LATIF [23]	DRNN	DDoS, Scanning	TON_IOT	A = 99.14%	It exhibited good accuracy performance in binary classification	The model exhibited high time complexity and energy consumption
BHOR. [24]	DBN	CMRI, MPCI, RECO	KDD CUP'99	A = 90%, P = 90%, R = 92%	It was superior in terms of accuracy and has a low false alarm rate	When the number of hidden neurons was low, the false alarm rate was high (>10%)
ZHANG [25]	GNN	FDIA, MATM, PF	Gas pipeline dataset	A = 97.2%, P = 98%, R = 99%	High performance in small training sets and unbalanced class data	The types of attacks that could be detected effectively are limited
BASATI [26]	CNN	DoS, Probe	UNSW-NB15, KDD CUP'99, CICIDS2017	A = 100%, 99.92%, and 99.43%	High detection accuracy performance	The system had a high time complexity, and it has not been deployed on a real IoT platform
KASONGO [27]	RNN	–	NSLKDD, UNSW-NB15	F1 = 99.47% and 80.84%	It was suitable for resource-constrained situations	The detection accuracy was low for a minority of certain types

(*continued*)

Table 2. (*continued*)

Scheme	Tech.	Intrusion handled	Dataset	Results	Advantage	Disadvantage
SANJU [28]	LSTM	Botnet	IoT-23, CICIDS2017	A = 98.12% and 99.98%	It could capture both local and global patterns in the data	Poor model generalization performance
SAHRMA [29]	DNN, GAN	DoS	UNSW-NB15	A = 84%	It could reduce the number of features before classification, thus lowering the cost	It had slightly lower accuracy and cannot predict trust values in real-time
ROUZ. [30]	Snapshot Ensemble DNN	–	DS2OS	A = 90.58%, P = 87.42%	The detection accuracy was acceptable	The lack of testing on a real platform prevented accurate classification of attacks
PACH. [31]	ANN	Flood attack for fog nodes	Self-created dataset	A = 97.5%, P = 98.4%, R = 98.9%	High detection rates, low false-positive alerts, and small time overhead	The types of attacks that could be detected effectively are limited

3 Challenges and Open Problems

Based on our analysis and comparison, it can be observed that the aforementioned related works exhibit excellent performance. However, challenges and issues still persist in this field. Some of them are outlined as follows.

Initially, it is necessary for IDSs to function within real-time or high-throughput network environments. However, DNNs are frequently associated with high computational complexity and storage demands, potentially hindering real-time performance. Strategies are devised to tackle this challenge, such as lightweighting the model, implementing hardware acceleration, and optimizing algorithms.

Besides, DNNs are susceptible to adversarial attacks. Attackers could deceive IDSs by adding subtle perturbations, making them unable to correctly identify intrusions. Adversarial attacks encompass attacks on both training data and the model itself, which include adversarial sample generation and adversarial training. To enhance the robustness of IDSs, adversarial training and defense mechanisms need to be implemented.

Moreover, intrusion detection data is typically highly imbalanced, with normal data far outnumbering the anomalous data. It could lead to models being biased towards overfitting to normal data and neglecting anomalous samples during DNN training. It is a challenge to dealing with imbalanced data distribution that requires appropriate sampling strategies or the use of specific loss functions to address this issue. Besides, during inference or training, a significant amount of matrix operations and activation function computations are required, placing high demands on computational resources and energy consumption [32]. Besides, during the actual deployment and updating of IDSs, challenges arise in continuously collecting, processing, and analyzing network data. So, there is a need for rapid model updates to adapt to new intrusions.

4 Research Direction

4.1 An IDS Based on Federated Learning and Transfer Learning

Federated learning and transfer learning can be combined to address some challenges, such as data imbalance and diverse intrusion behaviors. Federated learning, by simultaneously considering multiple tasks or data sources and jointly modeling them, enhances the generalization capability and robustness of the model. The advantage of FL integrated with DNNs is that information is stored on localized IoT devices for model training and only shared on a centralized federated learning server. In intrusion detection, FL can be utilized to improve detection performance by leveraging different network traffic datasets and knowledge of various intrusion types.

Besides, through the utilization of transfer learning, researchers can leverage knowledge acquired from one or multiple related tasks and transfer it to the target task, effectively addressing issues related to data imbalance and few-shot learning. It leverages datasets or pre-trained models from related domains to transfer knowledge to the intrusion detection task, thereby improving the performance.

4.2 An IDS Based on Explainable DNNs

To enhance the interpretability and transparency of IDSs, attention can be directed towards research on interpretable DNNs. Explainable artificial intelligence (XAI) is a methodology and set of techniques designed for artificial intelligence systems with the aim of making their decision-making and operational processes understandable and explainable. It focuses on the design of model architectures and learning algorithms that render the decision-making process of the model more comprehensible and explicable. For the design of IDSs, it requires the construction of an interpretable model structure that can explain why a certain behavior is classified as an intrusion. In addition, combining explainability with adversarial training can enhance a model's ability to withstand adversarial attacks and provide explanations.

In addition, by combining explainability with adversarial training, the model's ability to withstand adversarial attacks can be enhanced and explanations provided. The goal of these proposed research directions is to address the challenges faced by deep neural network-based IDS while providing novel solutions and insights. By combining the knowledge of multi-source data and tasks of FL and transfer learning, the generalization ability and robustness of the model can be enhanced. The aim is to improve the interpretability of IDS, making it more trustworthy and easier to understand.

5 Conclusion

We provide a review of DNN-based intrusion detection within the context of the IoT. Firstly, we categorize the related works into network traffic-based and device behavior-based schemes for analysis and comparison. We find that for DDoS attacks, network traffic-based IDS performed better, while device behavior-based systems achieved higher accuracy for internal threats and unknown attack types. Due to the high generalization capability and robustness of DNN, DNN-based intrusion detection strategies often

achieve detection rates of up to 99% for certain attack types. However, DNNs typically have multiple layers and lots of parameters, resulting in high computational complexity and energy consumption requirements. Additionally, the imbalance in datasets is also an issue that needs to be addressed, as it leads to significant performance variations across different attack types. Finally, we propose two suggested future work. Researchers can explore the combined use of federated learning and transfer learning, or utilize interpretable DNNs, to enhance intrusion detection performance in IoT.

Acknowledgments. This study was funded in part by the Key Research and Development Task Special Project of the Xinjiang Uygur Autonomous Region (grant number 2022B01009), in part by the Shanghai Science and Technology Innovation Action Plan (grant number 21DZ1200600), in part by the National Key Research and Development Program (grant number 2020YFB2104202), and in part by the Shanghai Natural Science Foundation (grant number 21ZR1461700).

References

1. Fang, W., Cui, N., Chen, W., Zhang, W., Chen, Y.: A trust-based security system for data collection in smart city. IEEE Trans. Ind. Inf. **17**(6), 4131–4140 (2021)
2. Li, Z., Fang, W., Zhu, C., Gao, Z., Zhang, W.: AI-enabled trust in distributed networks. IEEE Access **11**, 88116–88134 (2023)
3. Fang, W., Zhu, C., Guizani, M., Rodrigues, J.J.P.C., Zhang, W.: HC-TUS: human cognition-based trust update scheme for AI-enabled VANET. IEEE Netw. https://doi.org/10.1109/MNET.2023.3320934
4. Yadav, N., Pande, S., Khamparia, A., Gupta, D.: Intrusion detection system on IoT with 5G network using deep learning. Wirel. Commun. Mob. Comput. **2022**, Article no. 9304689 (2022)
5. Jayalaxmi, P.L.S., Saha, R., Kumar, G., Conti, M., Kim, T.H.: Machine and deep learning solutions for intrusion detection and prevention in IoTs: a survey. IEEE Access **10**, 121173–121192 (2022)
6. Khan, A.R., Kashif, M., Jhaveri, R.H., Raut, R., Saba, T., Bahaj, S.A.: Deep learning for intrusion detection and security of Internet of Things (IoT): current analysis, challenges, and possible solutions. Secur. Commun. Netw. **2022** Article no. 4016073 (2022)
7. Adi, L.W.P., Mandala, S., Nugraha, Y.: DDoS attack detection system using neural network on Internet of Things. In: 2022 International Conference on Data Science and Its Applications (ICoDSA), Bandung, Indonesia, pp. 41–46. IEEE (2022)
8. Ravi Kiran Varma, P., Sathiya, R.R., Vanitha, M.: Enhanced Elman spike neural network based intrusion attack detection in software defined Internet of Things network. Concur. Comput. Pract. Exp. **35**(2), Article no. e7503 (2023)
9. Firas Mohammed Aswad, F.M.A., Ali Mohammed Saleh Ahmed, A.M.S.A., Nafea Ali Majeed Alhammadi, N.A.M.A., Bashar Ahmad Khalaf, B.A.K., Mostafa, S.A., Mostafa, S.A.: Deep learning in distributed denial-of-service attacks detection method for Internet of Things networks. J. Intell. Syst. **32**, 1–13 (2023)
10. Yousuf, O., Mir, R.N.: DDoS attack detection in Internet of Things using recurrent neural network. Comput. Electr. Eng. **101**, Article no. 108034 (2022)
11. Reddy, D.K., Behera, H.S., Nayak, J., Vijayakumar, P., Naik, B., Singh, P.K.: Deep neural network based anomaly detection in Internet of Things network traffic tracking for the applications of future smart cities. Trans. Emerg. Telecommun. Technol. **32**(7), Article no. e4121 (2021)

12. Latif, S., Zou, Z., Idrees, Z., Ahmad, J.: A novel attack detection scheme for the industrial Internet of Things using a lightweight random neural network. IEEE Access **8**, 89337–89350 (2020)
13. Huma, Z.E., Latif, S., Ahmad, J., et al.: A hybrid deep random neural network for cyberattack detection in the industrial Internet of Things. IEEE Access **9**, 55595–55605 (2021)
14. Le, K.H., Nguyen, M.H., Tran, T.D., Tran, N.D.: IMIDS: an intelligent intrusion detection system against cyber threats in IoT. Electronics **11**(4), Article no. 524 (2022)
15. Fang, W., Zhu, C., Yu, F.R., Wang, K., Zhang, W.: Towards energy-efficient and secure data transmission in AI-enabled software defined industrial networks. IEEE Trans. Ind. Inf. **18**(6), 4265–4274 (2022)
16. Fang, W., Zhu, C., Zhang, W.: Toward secure and lightweight data transmission for cloud–edge–terminal collaboration in artificial intelligence of things. IEEE Internet Things J. **11**(1), 105–113 (2024)
17. Parra, G.D.L.T., Rad, P., Choo, K.K.R., Beebe, N.: Detecting Internet of Things attacks using distributed deep learning. J. Netw. Comput. Appl. **163**, Article no. 102662 (2020)
18. Zhao, R., et al.: A novel intrusion detection method based on lightweight neural network for Internet of Things. IEEE Internet Things J. **9**(12), 9960–9972 (2021)
19. Asgharzadeh, H., Ghaffari, A., Masdari, M., Gharehchopogh, F.S.: Anomaly-based intrusion detection system in the Internet of Things using a convolutional neural network and multi-objective enhanced Capuchin Search Algorithm. J. Parallel Distrib. Comput. **175**, 1–21 (2023)
20. Abd Elaziz, M., Al-qaness, M.A., Dahou, A., Ibrahim, R.A., Abd El-Latif, A.A.: Intrusion detection approach for cloud and IoT environments using deep learning and Capuchin Search Algorithm. Adv. Eng. Softw. **176**, Article no. 103402 (2023)
21. Thakkar, A., Lohiya, R.: Attack classification of imbalanced intrusion data for IoT network using ensemble learning-based deep neural network. IEEE Internet Things J. **10**(13), 11888–11895 (2023)
22. Wang, X., Wang, Y., Javaheri, Z., Almutairi, L., Moghadamnejad, N., Younes, O.S.: Federated deep learning for anomaly detection in the Internet of Things. Comput. Electr. Eng. **108**, Article no. 108651 (2023)
23. Latif, S., Huma, Z.E., Jamal, S.S., et al.: Intrusion detection framework for the Internet of Things using a dense random neural network. IEEE Trans. Ind. Inf. **18**(9), 6435–6444 (2021)
24. Bhor, H.N., Kalla, M.: TRUST-based features for detecting the intruders in the Internet of Things network using deep learning. Comput. Intell. **38**(2), 438–462 (2022)
25. Zhang, Y., Yang, C., Huang, K., Li, Y.: Intrusion detection of industrial internet-of-things based on reconstructed graph neural networks. IEEE Trans. Netw. Sci. Eng. **10**(5), 2894–2905 (2022)
26. Basati, A., Faghih, M.M.: Efficient network intrusion detection in IoT using parallel deep auto-encoders. Inf. Sci. **598**, 57–74 (2022)
27. Kasongo, S.M.: A deep learning technique for intrusion detection system using a Recurrent Neural Networks based framework. Comput. Commun. **199**, 113–125 (2023)
28. Sanju, P.: Enhancing intrusion detection in IoT systems: a hybrid metaheuristics-deep learning approach with ensemble of recurrent neural networks. J. Eng. Res. Article no. 100122 (2023)
29. Sharma, B., Sharma, L., Lal, C., Roy, S.: Anomaly based network intrusion detection for IoT attacks using deep learning technique. Comput. Electr. Eng. **107**, Article no. 108626 (2023)

30. Rouzbahani, H.M., Bahrami, A.H., Karimipour, H.: A snapshot ensemble deep neural network model for attack detection in industrial Internet of Things. In: Karimipour, H., Derakhshan, F. (eds.) AI-Enabled Threat Detection and Security Analysis for Industrial IoT, pp. 181–194. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-76613-9_10
31. Pacheco, J., Benitez, V.H., Felix-Herran, L.C., Satam, P.: Artificial neural networks-based intrusion detection system for Internet of Things fog nodes. IEEE Access **8**, 73907–73918 (2020)
32. Fang, W., Zhang, W., Yang, W., Li, Z., Gao, W., Yang, Y.: Trust management-based and energy-efficient hierarchical routing protocol in wireless sensor networks. Digit. Commun. Netw. **7**(5), 470–478 (2021)