# Deep Learning Approaches for Intrusion Detection in IIoT Networks – Opportunities and Future Directions

Thavavel Vaiyapuri[1], Zohra Sbai[2], Haya Alaskar[3], Nourah Ali Alaseem[4]

College of Computer Engineering and Sciences,
Prince Sattam bin Abdulaziz University, Saudi Arabia[1,2,3,4]
National Engineering School of Tunis, Tunis El Manar University, Tunisia[2]

***Abstract*—In recent years, the Industrial Internet of things (IIoT) is a fastest advancing innovative technology with a potential to digitize and interconnect many industries for huge business opportunities and development of global GDP. IIoT is used in diverse range of industries such as manufacturing, logistics, transportation, oil and gas, mining and metals, energy utilities and aviation. Although IIoT provides promising opportunities for the development of different industrial applications, they are prone to cyberattacks and demands for higher security requirements. The enormous number of sensors present in the IIoT network generates a large amount of data and has attracted the attention of cybercriminals across globe. The intrusion detection system (IDS) that monitors the network traffic and detects the behaviour of the network is considered as one of the key security solution for securing IIoT application from attacks. Recently, the application of machine and deep learning techniques have proved to mitigate multiple security threats and enhance the performance of intrusion detection. In this paper, we present a survey of deep learning-based IDS technique for IIoT. The main objective of this research is to provide the various deep learning-based IDS detection methods, datasets and comwparative analysis. Finally, this research aims to identify the limitations and challenges of existing studies, solutions and future directions.**

***Keywords*—Industrial Control System; Industrial Internet of Things (IIoT); cybersecurity; intrusion detection system and deep learning***

## I. Introduction

Industrial Internet of Things (IIoT) provides all industries with more excellent connectivity that, in turn, creates valuable information and intelligence regarding operations. IIoT is utilized in diverse range of industries to interface information, service, and people for intelligent operations in multiple management domains such as smart power, smart city, healthcare, automation industry, agriculture, logistics and transportation [1]. It connects with various sensors and maintains the critical infrastructure, and it requires a larger network scale. IIoT aims to provide intelligent manufacturing goods that establish smart factories with efficient communication between business partners and customers [2]. Industry 4.0 focused on the optimization problems in the industry to utilize data-driven services by using smart devices. This intelligence can achieve more efficiencies and manufacturing enhancements. However, this expanded network opens up these connected devices to specific threats of cyber-attacks. The industrial facilities become more connected, and hackers are more sophisticated. Industrial Control System (ICS) encompasses the various categories of control systems and integrated components utilized to control the industrial process. The ICS is facing an increased number of cyber-attacks that had multiple issues. Inefficient safety measures have an adverse impact on the workforce and organization. Some of the effects are production delays, building damage, medical and compensation costs, material losses, loss of business, legal expenses, and tool and equipment damages.

Intrusion detection systems detect the vulnerabilities within network traffic on network infrastructure. It could determine when the hackers begin probing devices that is the initial step to generate secure IIoT [3]. IDS system collects and identifies network traffic, audit data, security logs, and information from system key points to check whether there exist security damages in the network. The solution of IDS for IIoT requires to be customized to the nature of devices. Deep learning methods are used with IoT to improve the efficiency of IIoT applications. It maintains the balance between efficiency and computational cost for next-generation IoT networks.

Various researches provided several techniques for IDSs in industries. This paper provides a survey of multiple existing deep learning techniques for intrusion detection in IIoT. This survey offers various objectives. First, this research describes the preliminary analysis of IIoT systems and Intrusion Detection systems. Then we analyse the different existing deep learning techniques with their advantages and disadvantages for detecting intrusions in IIoT designs. Then we focus on various performance measures and datasets involved in IDS-IIoT. From the integration of surveys, we describe the limitations and challenges of existing methods. Finally, the solutions to rectify these challenges and future directions are sketched. The key contribution of this paper is listed below,

(a) We review the deep learning-based IDS systems for various industrial IoT applications.
(b) We present the multiple known cyber datasets, which are utilized in existing researches to classify the intrusions.
(c) We compare several existing deep learning methods with regard to their advantages and disadvantages.

## II. Background

### A. Intrusion Detection System (IDS)

IDS is used for monitoring the malicious attack in the interconnected network or node. It acts as the line of defence that can protect the node or network from attackers [4]. The malicious activity is defined as the intrusion that is destructive

to sensor nodes. The IDS system can be hardware or software tools. IDS can examine the user actions that determine the known attacks and identifies malicious network behaviour. It analyses the activity of nodes and networks with the determination of various intrusions and alerts the users after detecting the intrusions. So, it's called an alarm or network observer. It eliminates the systems damage by the alert generation before attains the unauthorized attacks. The IDS system can detect both Internal Attacks (IA) and External Attacks (EA). IA's are produced by malicious nodes that interconnected network. EA's are made by third parties that are attained by an external structure. The IDS system observes the network packets and detects whether they are unauthorized users or valid users. IDS involves three stages such as monitoring, investigation and alert. The monitoring component monitors the network patterns, traffics and resources. The study is the core component that determines the intrusions based on the specified algorithm. Alert module raised the alarm when the intrusions are determined. IDSs are categorized into three types which are described below [5],

*1) Host-based IDS System (HIDS):* HIDS estimates the information determined on a single or multiple host systems which include design, operating system and application files. This system collects the data from internal sources to computer at the operational system level, monitor user activities and monitor executions of system programs. It had the advantages of improved recovery, descriptive logging, fewer false positives, and unknown attack prediction. The disadvantages are unreadable information, complete coverage, indirect information, outsiders, and host interference.

*2) Anomaly-based IDS System (AIDS):* This system is called as event-based intrusion detection. It determines the malicious behaviours by analysing the event. Initially, it describes the normal activities of the attack. When the activities are varied from normal activity, then it's represented as an intrusion.

*3) Network-based IDS System (NIDS):* This system identifies the intrusions by monitoring the network traffic through the network interface cards, routers and switches. The data are mainly collected through general network stream like internet packets. NIDS can detect all attacks in LAN and can determine attacks that cannot be achieved by host-based IDS. Advantages of NIDS are ease of deployment, cost, detection range, forensics integrity, and detects all attempts. The disadvantages are a failure at wire speed, direct attack susceptibility, indecipherable packets and Problem of complete coverage .

### *B. Requirement for IDS in Internet of Things (IoT) Networks*

IoT is the growing technology that defines the physical objects that had the capability of exchanging information with other items. These objects communicate with each other without human intervention. IoT is a smart network that communicates all things through the internet for information exchange with approved protocols. Therefore, the user can access anything from anywhere at any time. It utilizes unique addressing methods to communicate these objects and collaborate with objects to generate new services and applications. It presents multiple applications like smart cities, smart homes, smart environment, health monitoring and smart water [6]. Despite IoT provides various facilities for human routine life based on its reliable and available actions, It requires multi-class security solutions with regard to integrity, privacy and other verification services. The IoT network should be protected against intrusions, and information captured by IoT sensor should be uploaded in an encrypted format. Thus, developing a secure communication is an essential task in the IoT network.

Among the multiple issues of IoT, the security issue cannot be left unnoticed as IoT devices can be retrieved from anywhere through the unauthorized network [7]. When the security problems are not analysed, then the sensitive data may be attacked at any time. So, the security issues are must be identified from the following aspects,

(a) Confidentiality: The attacker can easily interrupt the message passing from source to destination so that the user sensitive information can be leaked and the data can be modified. So, secure information transformation is the most important.
(b) Integrity: The transmit information should be received at the receiver side without any modification. Integrity assures that the information has not been modified by unapproved attackers in transmission.
(c) Availability: Resources should be available when required. The attackers can overflow the resources bandwidth to destruct the accessibility. This accessibility can damage by some malicious attacks.
(d) Authenticity: It performs the identity proof. The users can determine other's identity with that they are in communication. It can be validated through the verification process. So the unauthorized attacks cannot involve in the interaction.
(e) Non-repudiation: It enhances that the sender and receiver are not able to reject the sent and received the information. It provides the proof of origin of the data and integrity of the data.

### *C. Requirement for IDS in Industrial IoT (IIoT) Networks*

IIoT is the revolutionary effort to create smart manufacturing eco-system by using the IoT advantages for industrial process management. IIoT rapidly expands the various industries and services that are discussed in below: In healthcare systems, the IoT devices are used for tracking, sensing, and monitoring of machines, patients and medicines[8]. In the agriculture industry, the IoT devices are utilized for security surveillance of farms, efficient watering of plants, and product storage management. [9].

Transportation and logistics industry plays a vital role in supply chain industries [10]. In this field, the IoT devices are used to determine the vehicle's location for tracking the movements. It's also used to determine the supply time of the product. In the energy sector, the IIoT maintains the supply from and to the grid, billing, and monitoring of leakage. In the mining industry, the IoT devices are used for managing warning systems, sensing disaster signals, tracking underground miner's movement, and monitoring shipments [11]. The strength of the automation industry defines ICS that includes Supervisory Control and Data Acquisition (SCADA)

networks and Programmable Logic Controllers (PLC). Most of the cyber-attacks involve against industrial automated systems such as Stuxnet attack, German steel mill blast furnace attack, Shamoon attack, Mirai, etc..

Numerous cyberattacks are targeted the industrial enterprises around the world. A large amount of vulnerabilities presents in IoT devices for cyber-criminals to attack the industrial process. In traditional, well-protected networks are created with stable defensive mechanisms. Therefore, the robust intrusion detection mechanism is required to fight against attacks and to protect the industrial systems. In the next section, the existing intrusion detections systems are discussed for IIoT by using deep learning.

## III. Review on Deep Learning-based IDS Approaches

In IIoT, the cyber-attacks are growing at an alarming rate with the increase in connected applications, devices and communication networks. When the attacks occur in IIoT networks, it reduces the availability of systems for end-users, and it increases the theft identity and the number of data breaches, costs and revenue impacts. Though various surveys and researches had been published on IDSs for IoT using deep learning, no survey is present on IDS approaches for IIoT. This section discusses the various deep learning based IDS approaches for IoT and IIoT applications. Some of the discussed deep learning techniques for IDS systems are as follow,

### A. Applied for Securing IoT Networks

The authors in [12] have developed an algorithm leveraging the benefits of deep learning to detect DDoS attacks. Also, they have compared the performance of several deep learning approaches over machine learning techniques for DDoS attack detection. The results have confirmed the potential of deep learning to increase the accuracy in detecting DDoS attacks that occur within IoT network. Also, the authors in [13] developed IDS leveraging the potential of convolutional neural networks (CNN) and high performance computing to achieve better intrusion detection performance within IoT networks. In this line, an IDS based on deep belief network based IDS is proposed in [14]. The approach has proved to provide better intrusion detection performance in term of accuracy, F1-score, precision and detection rate on the benchmark dataset, CICIDS. Also, the authors in [15] presented deep learning based IDS by stacking nearly five residual networks that pretrained to learn the malicious network behavior and recognize intrusion within IoT network. Several other researchers have attempted to design IDS leveraging the benefits of deep learning from different perspectives as follows

(a) **Self-taught learning:** The authors in [21] have developed an IDS based on deep learning approaches to recognize four types of attacks that occur within IoT system specially to protect smart-home environment. The approach utilizes self-taught learning framework to analyze six features for attack detection
(b) **Transfer learning:** The work in [22] adopts feed-forward deep neural networks and transfer learning in encoding the network traffic features to build multi-class and binary classifiers for recognizing different types of attacks within IoT networks.
(c) **Ensemble learning:** The work in [23] ensembles set of long term short memory and then employs decision tree to make the final decision in recognizing the attacks within IoT network. The system has proved its effectiveness on real-word datasets with an accuracy of 99% in detection different types of attacks against IoT devices
(d) **Cloud-based IDS:** The authors in [24] have attempted to incorporate blockchain and deep learning to design a deep blockchain framework for Intrusion detection. Here, authors utilize smart contracts to establish privacy-based blockchain in IoT networks and bidirectional LSTM to analyze network data for intrusion. The framework has proven to serve as a decision support system in supporting the IoT users and cloud providers in securely sharing the data. Similarly, the authors in [25] proposed a IDS based on distributed deep learning approach for detecting different types of attacks within IoT network. The model employs distributed blockchain to detect phishing attacks and LSTM hosted on cloud for detecting botnet attacks within IoT network
(e) **Fog-Assisted IDS:** The work in [26] proposed an IDS based on recurrent neural networks (RNN) for securing Fog computing from cyberattacks. Here, the system is built using multiple layer of RNN to achieve stability and robustness in protecting the fog computing from cyberattacks. Similarly, the authors in [27] employed DNN to develop network IDS that can be deployed in Fog nodes to detect different types of attacks within Fog assisted IoT network.
(f) **Botnet IDS:** The authors in [28] utilize convolutional neural networks (CNN) with oversampling and feature engineering techniques to handle effectively the imbalance in intrusion dataset and achieve trade-off in performance between effectiveness and efficiency to detect different types of bot attacks that occur within IoT network. The authors in [29] proposed an IDS integrating the benefits of dendritic cell algorithm and deep learning to select discriminate network traffic features for Botnet attacks. The system has demonstrated its potential in improving the detection rate with reduced false alarm rate for bot-net attacks within IoT networks. The authors in [30] investigates the performance of different deep learning approaches for Botnet attacks within IoT network against machine learning approaches. The deep learning approaches have proved their potential over machine learning approaches for botnet attack detection within IoT networks.

Further, the readers can refer these literature [31], [32], [33] to understand the challenges, solutions and future directions in applying deep learning approaches for IDS within IoT.

### B. Applied for Securing Industrial Control System (ICS)

In literature, several machine learning based IDS are proposed for ICS. The state-of-the-art and related works are summarized in Table-I. With the breakthrough evolution of DNN various other fields, the researchers have applied DNN to design IDS for ICS. For example, DNN based IDS is presented for vehicle network security [10]. The system utilizes

TABLE I. SUMMARY ON IDS APPROACHES FOR ICS

| Authors | Techniques Adopted | Dataset Used | Detection Performance | Remarks |
|---|---|---|---|---|
| Liang, Wei, et al [16] | Utilizes multi-feature data clustering and optimization model | NSL-KDD and KDDCup99 | Accuracy - 97.8%, and FAR - 8.8% | The model is not evaluated for its efficacy with recent industrial network traffic datasets |
| Tsang, Chi-Ho et al [17] | Utilizes biologically inspired learning model to extract effective features and enhances clustering based IDS solutions | KDD-Cup99 | Accuracy - 92.23%, and FAR - 1.53% | No Efforts are taken to reduce the time complexity of biological inspired learning model. Therein, detection time of the model may be higher than other IDS models. |
| Jin, Chenglu et al [18] | Applies forward secure logging mechanism for intrusion detection | Proof of concept evaluation | NA | Lightweight IDS model with 54 $\mu s$ per scan cycle |
| Butun, Ismail, et al [19] | Leverages parallel and distributed computing for executing Data streaming applications in intrusion detection | Dataset from real-world AMI | - | Recommends Data streaming paradigm as effective technique for intrusion detection in big industrial networks |
| Yang, Kai, et al [20] | Deterministic Finite automata uses register status to generate fingerprint of ICS controller and performs both active and passive intrusion detection | Real-worlds experiments are conducted for validation | 98% recall rate | The model shows detection rate within 2s |

DNN to improve the vehicular network security. The designed DNN is trained with probability-based feature vectors that are retrieved from in-vehicular network packets to learn the network parameters. The system displays the probability of each class as either normal or intrusion based on the malicious traffic packets flows to the vehicle. Also, the system demonstrated higher detection rate for intrusion in the Controller Area Network (CAN) bus. Also, the reference in [34] described the IDS system against malicious attacks on communication network of driverless cars. This research investigated the IDS system for VANET by using ANN that determines the DoS attacks. The focus of this suggested system is to determine the attack through the generated data using network behaviour like trace file. The IDS system utilizes the extracted features as auditable data from the trace file.

Similarly, the reference [9] presented the deep learning method for detecting the intrusions in the agricultural field. This study provided a fast state-of-the-art detector to detect the unknown anomalies. Then the RCNN method is used to attain high accuracy and minimum computation time.

The literature [35] presented a survey on IDS for ICS. They described the various characteristics and updated security needs of ICS. This research defined a new taxonomy for IDS in IDS using multiple techniques such as traffic mining based, protocol analysis-based and control process identification based. They identified the merits and demerits of various classes of IDS and discussed some future developments of IDS system for ICS.

The authors in [36] utilized the Long-short term memory (LSTM) for Omni SCADA intrusion detection. It acts as the data acquisition or supervisor control to detect both temporally correlated and uncorrelated attacks. The feedforward network (FNN) network determines the temporally uncorrelated attacks with the F1-measures of $99.967 \pm 0.005\%$, and for correlated attacks, it had $58 \pm 2\%$. The combination of FNN and LSTM hybridization method enhanced the IDS performance with $99.68 \pm 0.04\%$ F1 measure. The summary of DNN based IDS for ICS are presented in Table-II.

### C. Applied for Securing IIoT Networks

In 2018, two IDS was developed utilizing two different types of deep learning models [41]. The first model utilized deep belief network (DBN). Here, the model was trained and tested with disjoint datasets. In the second model, unlabeled dataset has been utilized to train DBN to learn the changes in intrusion network traffic patterns. In the same year, a secure architecture is introduced.[42] for analyzing SCADA network traffic for intrusion detection and securing ICS equipped with IoT platform. The architecture includes an IDS developed with the ensemble of DBN and SVM. Notably, the architecture utilizes network traffic features and payload features to distinguish normal network traffic from malicious activities. The architecture proved its potential on real SCADA network traffic data with higher detection rate. Also, an IDS was proposed for IIoT utilizing the benefits of deep learning [43]. The system here uses deep feedforward neural network and deep autoencoder for learning the characteristics of malicious network traffic. The system uses information captured from TCP/IP packets to distinguish the intrusion network traffic from normal network traffic behavior. The system was evaluated on NSL-KDD and UNSW-NB15 datasets to demonstrate lower false alarm rate and higher detection rate for intrusion within IIoT system.

TABLE II. SUMMARY ON DEEP LEARNING BASED IDS APPROACHES FOR ICS

| Authors | Techniques Adopted | Dataset Used | Detection Performance | Remarks |
|---|---|---|---|---|
| Li, Beibei, et al [37] | Utilizes federated deep learning scheme based on convolutional neural networks and gated recurrent unit | real industrial CPS | 98.64% recall rate | Applicable only for same-domain industrial CPSs |
| Wang, Zhidong, et al [38] | Utilizes deep neural network with different degrees of discrimination | gas pipeline | 100% recall rate all attack types | The model is not evaluated with regard to detection accuracy and detection rate |
| Leyi, Shi, et al [39] | Utilizes CNN, Bi-LSTM and correlation information entropy | gas pipeline | Accuracy-99.21% and FAR-0.77% | Detection rate of 11.73s |
| Chu, Ankang et al [40] | Utilizes GoogLeNet to extract features for inception module and LSTM | gas pipeline | Accuracy-97.56% and FAR-2.42% | Adopts attention mechanism for time-series level detection |

In 2019 a IDS model leveraging the benefits of unsupervised deep learning methods [44], sparse and noisy deep autoencoder was presented to learn the high level network traffic features and later the network traffic is distinguished using supervised deep learning networks. The proposed model is evaluated for its effectiveness to detect intrusion in IIoT system using dataset collected from remote telemetry streams of gasline system.

In 2020, the authors have proposed an IDS utilizing the advantages of deep random neural network to secure and safeguard IIoT system [1]. But, the system was evaluated on UNSW-NB15 dataset to demonstrate its feasibility and applicability for IIoT. The system displayed higher detection accuracy of 99.54% with low false alarm rate. Similarly, In [45] a fusion based IDS is introduced for securing IIoT. The system partitions the acquired network traffic features into four parts based on the correlation between features. The four group of features namely, content, time-based, host-based and statistics features are transformed to matrix form as an image to enable the processing by four respective CNN for intrusion detection. The system proved its potential for intrusion detection in IIoT system when evaluated with NSL-KDD dataset.

The authors in [2] have attempted to address the significant gap in literature confined to the unavailability of dataset for designing and evaluating IoT/IIoT defense solutions. The authors have presented a representative testbed with seven different sensors and three layers of Cloud, Fog, and Edge to simulate realistic IoT/IIoT system and capture network and intrusion traffic. The new dataset collected from the simulated IoT/IIoT testbed with features to distinguish normal and intrusion network traffic is published under the name TON_IoT and made available for research purpose. Also, the authors have applied several machine learning and deep learning algorithms on the generated TON_IoT dataset as a first-hand evaluation that can serve as a baseline and encourage researchers in this direction. The summary of DNN based IDS for IIoT are presented in Table-III

## IV. KEY FINDINGS FROM LITERATURE REVIEW

The aforementioned literature review clearly indicates that plethora of works are published on the application of deep learning approaches for building efficient IDS in IoT environment. Although the industrial sectors have experienced several cyberattack incidents across the world with huge loss, comparatively, less researches have taken place in designing deep learning based IDS for ICS. Also, it can be noticed that very few researches have taken place in IIoT environment when compared to ICS and IoT environment. This clearly indicates that security of IIoT is still in its infancy. Hence, the researchers working in the field of cybersecurity are recommended to focus on the application of deep learning approaches for developing IDS for IIoT environment.

## V. LIMITATIONS AND CHALLENGES

The effectiveness of the IDS designed for IIoT system should be evaluated with more experimentations to examine the strong and weak points of detection method in various circumstances. IIoT systems expand a large number of heterogeneous connected devices with power, memory and computational constraints that affect the quality of data. Therefore, some of the challenges of existing deep learning methods in IDS-IIoT are defined as below,

(a) Deep learning methods demand high computation cost and pose challenge for its implementation on resource-constrained devices to assist onboard security system.
(b) The deep learning methods are characterized with large number of network parameters and their success depend on training process adopted for network parameter learning. Also it depends on techniques utilized for network parameter initialization.
(c) IIoT networks are object driven that makes it challenging to apply existing computer networks security mechanisms. Therefore, some specialized tools are required to simulate IIoT environment to capture network traffic and conduct experiment for evaluating the designed ap-

TABLE III. SUMMARY ON DEEP LEARNING BASED IDS APPROACHES FOR IIOT

| Authors | Techniques Adopted | Dataset Used | Detection Performance | Remarks |
|---|---|---|---|---|
| Li, Yanmiao, et al [45] | Utilizes deep learning fusion learning with different single CNN and correlation for feature extraction | NSL-KDD | Accuracy-86.95% and FAR-13.45% | The model is not evaluated for its efficacy with IIoT network traffic datasets |
| Wu, Di, et al [46] | Utilizes LSTM network and Gaussian Naïve Bayes model | real-life time time-series datasets | Accuracy-100% | Model is evaluated for anomaly detection rather than network intrusion |
| Latif, Shahid, et al [1] | Deep random neural network | UNSW-NB15 | Accuracy-99.54% | Model is evaluated for IoT network traffic data but not for industrial IoT network traffic |
| Muna et al [43] | Utilizes deep autoencoder and deep forwards neural networks | UNSW-NB15 NSL-KDD | Accuracy-99% and FAR-1.8% | Model is evaluated for IoT network traffic data but not for industrial IoT network traffic |

proaches with regard to security of IIoT systems from evolving vulnerabilities and threats.

## VI. FUTURE DIRECTIONS

In future, the researchers in the field of cybersecurity can focus on the following directions to enhance the security of IIoT,

(a) Develop IDS model that can enable to enhance the detection performance against unknown attacks
(b) Lack of sufficient number network traffic samples for training deep learning models for IDS
(c) Develop lightweight IDS model that can be implemented on resource constrained IIoT devices
(d) Develop distributed and collaborative IDS model that can safeguard the resources of IIoT from sophisticated attacks
(e) Develop intrusion detection and prevention system that can secure IIoT from different types of attacks

## VII. CONCLUSION

IIoT is the most important part to connect the physical objects to the internet in various industrial applications of the future. During the last decade, the IoT devices usage has rapidly increased due to its capacity of converting objects from application areas into internet hosts. Although, the user's privacy and security are an important challenge due to the security vulnerabilities. Therefore, IoT security must be developed and investigated. The IDS security mechanism is used for IIoT systems and networks with deep learning concept.

In this paper, we presented the various literature survey about deep learning-based IDS for IIoT networks. In this survey paper, we analysed existing papers that were published between 2015 to 2020.

We conclude that research in IDS is still in its incipient and infancy. In addition, it is very hard to develop the comprehensive IDS that can provide more accuracy, robustness, scalability, and protection against all types of intrusions.

## ACKNOWLEDGMENT

The authors are very grateful to thank their Deanship of Scientific Research for technical and financial support in publishing this work successfully.

## REFERENCES

[1] Shahid Latif, Zeba Idrees, Zhuo Zou, and Jawad Ahmad. Drann: A deep random neural network model for intrusion detection in industrial iot. In *2020 International Conference on UK-China Emerging Technologies (UCET)*, pages 1–4. IEEE, 2020.

[2] Abdullah Alsaedi, Nour Moustafa, Zahir Tari, Abdun Mahmood, and Adnan Anwar. Ton_iot telemetry dataset: a new generation dataset of iot and iiot for data-driven intrusion detection systems. *IEEE Access*, 8:165130–165150, 2020.

[3] Thavavel Vaiyapuri and Adel Binbusayyis. Application of deep autoencoder as an one-class classifier for unsupervised network intrusion detection: a comparative evaluation. *PeerJ Computer Science*, 6:e327, 2020.

[4] Adel Binbusayyis and Thavavel Vaiyapuri. Identifying and benchmarking key features for cyber intrusion detection: an ensemble approach. *IEEE Access*, 7:106495–106513, 2019.

[5] Adel Binbusayyis and Thavavel Vaiyapuri. Comprehensive analysis and recommendation of feature evaluation measures for intrusion detection. *Heliyon*, 6(7):e04262, 2020.

[6] Thavavel Vaiyapuri. Deep learning enabled autoencoder architecture for collaborative filtering recommendation in iot environment. *CMC-Computers, Materials & Continua*, 68(2):487–503, 2021.

[7] Adel Binbusayyis and Thavavel Vaiyapuri. Unsupervised deep learning approach for network intrusion detection combining convolutional autoencoder and one-class svm. *Applied Intelligence*, pages 1–15, 2021.

[8] Thavavel Vaiyapuri, Adel Binbusayyis, and Vijayakumar Varadarajan. Security, privacy and trust in iomt enabled smart healthcare system: A systematic review of current and future trends. *International Journal of Advanced Computer Science and Applications*, 12(2):731–737, 2021.

[9] Peter Christiansen, Lars N Nielsen, Kim A Steen, Rasmus N Jørgensen, and Henrik Karstoft. Deepanomaly: Combining background subtraction and deep learning for detecting obstacles and anomalies in an agricultural field. *Sensors*, 16(11):1904, 2016.

[10] Min-Joo Kang and Je-Won Kang. Intrusion detection system using deep neural network for in-vehicle network security. *PloS one*, 11(6):e0155781, 2016.

[11] Samyak Jain and K Chandrasekaran. Industrial automation using internet of things. In *Security and Privacy Issues in Sensor Networks and IoT*, pages 28–64. IGI Global, 2020.

[12] Bambang Susilo and Riri Fitri Sari. Intrusion detection in iot networks using deep learning algorithm. *Information*, 11(5):279, 2020.

[13] Qasem Abu Al-Haija and Saleh Zein-Sabatto. An efficient deep-learning-based detection and classification system for cyber-attacks in iot communication networks. *Electronics*, 9(12):2152, 2020.

[14] S Manimurugan, Saad Al-Mutairi, Majed Mohammed Aborokbah, Naveen Chilamkurti, Subramaniam Ganesan, and Rizwan Patan. Effective attack detection in internet of medical things smart environment using a deep belief neural network. *IEEE Access*, 8:77396–77404, 2020.

[15] Bandar Alotaibi and Munif Alotaibi. A stacked deep learning approach for iot cyberattack detection. *Journal of Sensors*, 2020, 2020.

[16] Wei Liang, Kuan-Ching Li, Jing Long, Xiaoyan Kui, and Albert Y Zomaya. An industrial network intrusion detection algorithm based on multifeature data clustering optimization model. *IEEE Transactions on Industrial Informatics*, 16(3):2063–2071, 2019.

[17] Chi-Ho Tsang and Sam Kwong. Multi-agent intrusion detection system in industrial network using ant colony clustering approach and unsupervised feature extraction. In *2005 IEEE international conference on industrial technology*, pages 51–56. IEEE, 2005.

[18] Chenglu Jin, Saeed Valizadeh, and Marten van Dijk. Snapshotter: Lightweight intrusion detection and prevention system for industrial control systems. In *2018 IEEE Industrial Cyber-Physical Systems (ICPS)*, pages 824–829. IEEE, 2018.

[19] Ismail Butun, Magnus Almgren, Vincenzo Gulisano, and Marina Papatriantafilou. Intrusion detection in industrial networks via data streaming. In *Industrial IoT*, pages 213–238. Springer, 2020.

[20] Kai Yang, Qiang Li, Xiaodong Lin, Xin Chen, and Limin Sun. ifinger: Intrusion detection in industrial control systems via register-based fingerprinting. *IEEE Journal on Selected Areas in Communications*, 38(5):955–967, 2020.

[21] Marjia Akter, Gowrab Das Dip, Moumita Sharmin Mira, Md Abdul Hamid, and MF Mridha. Construing attacks of internet of things (iot) and a prehensile intrusion detection system for anomaly detection using deep learning approach. In *International Conference on Innovative Computing and Communications*, pages 427–438. Springer, 2020.

[22] Mengmeng Ge, Naeem Firdous Syed, Xiping Fu, Zubair Baig, and Antonio Robles-Kelly. Toward a deep learning-driven intrusion detection approach for internet of things. *Computer Networks*, page 107784, 2021.

[23] Mahdis Saharkhizan, Amin Azmoodeh, Ali Dehghantanha, Kim-Kwang Raymond Choo, and Reza M Parizi. An ensemble of deep recurrent neural networks for detecting iot cyber attacks using network traffic. *IEEE Internet of Things Journal*, 7(9):8852–8859, 2020.

[24] Osama Alkadi, Nour Moustafa, Benjamin Turnbull, and Kim-Kwang Raymond Choo. A deep blockchain framework-enabled collaborative intrusion detection for protecting iot and cloud networks. *IEEE Internet of Things Journal*, 2020.

[25] Gonzalo De La Torre Parra, Paul Rad, Kim-Kwang Raymond Choo, and Nicole Beebe. Detecting internet of things attacks using distributed deep learning. *Journal of Network and Computer Applications*, 163:102662, 2020.

[26] Muder Almiani, Alia AbuGhazleh, Amer Al-Rahayfeh, Saleh Atiewi, and Abdul Razaque. Deep recurrent neural network for iot intrusion detection system. *Simulation Modelling Practice and Theory*, 101:102031, 2020.

[27] Nausheen Sahar, Ratnesh Mishra, and Sidra Kalam. Deep learning approach-based network intrusion detection system for fog-assisted iot. In *Proceedings of International Conference on Big Data, Machine Learning and their Applications*, pages 39–50. Springer, 2021.

[28] Abdelouahid Derhab, Arwa Aldweesh, Ahmed Z Emam, and Farrukh Aslam Khan. Intrusion detection system for internet of things based on temporal convolution neural network and efficient feature engineering. *Wireless Communications and Mobile Computing*, 2020, 2020.

[29] Sahar Ahmed Aldhaheri. Deepdca: Intrusion detection over iot based on artificial immune system and deep learning. 2020.

[30] S Sriram, R Vinayakumar, Mamoun Alazab, and KP Soman. Network flow based iot botnet attack detection using deep learning. In *IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pages 189–194. IEEE, 2020.

[31] Javed Asharf, Nour Moustafa, Hasnat Khurshid, Essam Debie, Waqas Haider, and Abdul Wahab. A review of intrusion detection systems using machine and deep learning in internet of things: Challenges, solutions and future directions. *Electronics*, 9(7):1177, 2020.

[32] Ankit Thakkar and Ritika Lohiya. A review on machine learning and deep learning perspectives of ids for iot: Recent updates, security issues, and challenges. *Archives of Computational Methods in Engineering*, pages 1–33, 2020.

[33] Idriss Idrissi, Mostafa Azizi, and Omar Moussaoui. Iot security with deep learning-based intrusion detection systems: A systematic literature review. In *2020 Fourth International Conference On Intelligent Computing in Data Sciences (ICDS)*, pages 1–10. IEEE, 2020.

[34] Khattab M Ali Alheeti, Anna Gruebler, and Klaus D McDonald-Maier. An intrusion detection system against malicious attacks on the communication network of driverless cars. In *2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC)*, pages 916–921. IEEE, 2015.

[35] Yan Hu, An Yang, Hong Li, Yuyan Sun, and Limin Sun. A survey of intrusion detection on industrial control systems. *International Journal of Distributed Sensor Networks*, 14(8):1550147718794615, 2018.

[36] Jun Gao, Luyun Gan, Fabiola Buschendorf, Liao Zhang, Hua Liu, Peixue Li, Xiaodai Dong, and Tao Lu. Omni scada intrusion detection using deep learning algorithms. *IEEE Internet of Things Journal*, 8(2):951–961, 2020.

[37] Beibei Li, Yuhao Wu, Jiarui Song, Rongxing Lu, Tao Li, and Liang Zhao. Deepfed: Federated deep learning for intrusion detection in industrial cyber-physical systems. *IEEE Transactions on Industrial Informatics*, 2020.

[38] Zhidong Wang, Yingxu Lai, Zenghui Liu, and Jing Liu. Explaining the attributes of a deep learning based intrusion detection system for industrial control networks. *Sensors*, 20(14):3817, 2020.

[39] Shi Leyi, Zhu Hongqiang, Liu Yihao, and Liu Jia. Intrusion detection of industrial control system based on correlation information entropy and cnn-bilstm. *Journal of Computer Research and Development*, 56(11):2330, 2019.

[40] Ankang Chu, Yingxu Lai, and Jing Liu. Industrial control intrusion detection approach based on multiclassification googlenet-lstm model. *Security and Communication Networks*, 2019, 2019.

[41] Shamsul Huda, Suruz Miah, John Yearwood, Sultan Alyahya, Hmood Al-Dossari, and Robin Doss. A malicious threat detection model for cloud assisted internet of things (cot) based industrial control system (ics) networks using deep belief network. *Journal of Parallel and Distributed Computing*, 120:23–31, 2018.

[42] Shamsul Huda, John Yearwood, Mohammad Mehedi Hassan, and Ahmad Almogren. Securing the operations in scada-iot platform based industrial control system using ensemble of deep belief networks. *Applied soft computing*, 71:66–77, 2018.

[43] AL-Hawawreh Muna, Nour Moustafa, and Elena Sitnikova. Identification of malicious activities in industrial internet of things based on deep learning models. *Journal of information security and applications*, 41:1–11, 2018.

[44] Muna Al-Hawawreh, Elena Sitnikova, and Frank den Hartog. An efficient intrusion detection model for edge system in brownfield industrial internet of things. In *Proceedings of the 3rd International Conference on Big Data and Internet of Things*, pages 83–87, 2019.

[45] Yanmiao Li, Yingying Xu, Zhi Liu, Haixia Hou, Yushuo Zheng, Yang Xin, Yuefeng Zhao, and Lizhen Cui. Robust detection for network intrusion of industrial iot based on multi-cnn fusion. *Measurement*, 154:107450, 2020.

[46] Di Wu, Zhongkai Jiang, Xiaofeng Xie, Xuetao Wei, Weiren Yu, and Renfa Li. Lstm learning with bayesian and gaussian processing for anomaly detection in industrial iot. *IEEE Transactions on Industrial Informatics*, 16(8):5244–5253, 2019.