1

A Systematic Literature Review on Cyber Security Threats of Industrial Internet of Things

Ravi Gedam* **and Surendra Rahamatkar**†

Amity University Chhattisgarh, Raipur, India

Abstract

In recent years, the Industrial Internet of Things (IIoT) has become one of the popular technology among Internet users for transportation, business, education, and communication development. With the rapid adoption of IoT technology, individuals and organizations easily communicate with each other without great effort from the remote location. Although, IoT technology often confronts unauthorized access to sensitive data, personal safety risks, and different types of attacks. Hence, it is essential to model the IoT technology with proper security measures to cope up with the rapid increase of IoT-enabled devices in the real-time market. In particular, predicting security threats is significant in the Industrial IoT applications due to the huge impact on production, financial loss, or injuries. Also, the heterogeneity of the IoT environment necessitates the inherent analysis to detect or prevent the attacks over the voluminous IoT-generated data. Even though the IoT network employs machine learning and deep learning-based security mechanisms, the resource constraints create a set-back in the security provisioning especially, in maintaining the trade-off between the IoT devices' capability and the security level. Hence, in-depth analysis of the IoT data along with the time efficiency is crucial to proactively predict the cyber-threats. Despite this, relearning the new environment from the scratch leads to the time-consuming process in the large-scale IoT environment when there are minor changes in the learning environment while applying the static machine learning or deep learning models. To cope up with this constraint, incrementally updating the learning environment is essential after learning the partially changed environment with the knowledge

**Corresponding author*: gedam.hemraj@s.amity.edu
†*Corresponding author*: srahamatkar@rpr.amity.edu

Uzzal Sharma, Parma Nand, Jyotir Moy Chatterjee, Vishal Jain, Noor Zaman Jhanjhi and R. Sujatha (eds.)
Cyber-Physical Systems: Foundations and Techniques, (1–18) © 2022 Scrivener Publishing LLC

of previously learned data. Hence, to provide security to the resource-constrained IoT environment, selecting the potential input data for the incremental learning model and fine-tuning the parameters of the deep learning model for the input data is vital, which assists towards the proactive prediction of the security threats by the time-efficient learning of the dynamically arriving input data.

Keywords: Industrial IoT, smart manufacturing, industry 4.0, interoperability, deep learning, incremental learning

1.1 Introduction

In recent years, Industrial Internet of Things (IIoT) technology [1] has gained significant attention among the internet users in the real-world with the increased advantage of the ubiquitous connectivity and interaction between the physical and cyber worlds. With the enormously interconnected IoT devices, IIoT devices have been used in various applications such as smart homes, smart cars, smart healthcare, smart agriculture, and smart retail. The exponential rise of IoT technology often confronts security and privacy concerns [2]. Nowadays, cyber-attacks such as ransomware and malware have increasingly targeted IoT applications to impact the distributed network. Even though the existing security measures are adopted in the IoT environment, IIoT applications are still vulnerable to different attacks due to the massive attack surface [3, 4]. Hence, it is essential to design the defense mechanisms to detect and predict the attacks in the IIoT platform. Applying the traditional security models or mechanisms is inadequate for the IIoT environment due to the intrinsic resource and computational constraints. Intrusion detection models dynamically monitor abnormal behaviors or patterns in the system to detect malicious activity. The existing intrusion detection researches have mainly focused on rule-based detection techniques, which lack to support the detection of anomalies in the emerging IIoT platform [5]. To detect anomalies without false alarms, artificial intelligence methods have been widely used by security researchers. For the most part, in order to deal with the massive amount of data generated by IoT devices, machine learning and deep learning algorithms have been used to perform automated data analysis as well as to provide meaningful interpretations [6, 7]. Several research works have employed machine learning and deep learning techniques to detect malicious activity in the IIoT environment. Despite the combination of intrusion detection and artificial intelligence-based research, it still confronts the precise detection of anomalies in IIoT networks.

Owing to the dynamic arrival of the new malware classes and instances in the IIoT platform, traditional machine learning, and deep learning-based security models deal with the catastrophic forgetting problems. Catastrophic forgetting is the ignorance of the knowledge about previous significant classes while performing the classification for the new classes. The security experts have widely utilized incremental learning models [8, 9]. The incremental learning model continuously learns the new data with the knowledge of the previous learning results. It plays a significant role in improving the detection or prediction performance in developing the security models for the detection of known and unknown attacks. The incremental learning model often confronts the stability-plasticity problem: previous data retaining and new data preserving [10]. Hence, harvesting useful insights from the enormous amount of data are crucial to improve the learning performance. In essence, preprocessing the continuously arriving data streams to augment the training data is crucial for the incremental learning model. Thus, this work focuses on modeling the security mechanism for the IIoT application with the contextual preprocessing and the enhanced deep incremental learning model. With the target of improving the detection performance, it employs the incremental feature selection with optimization for the contextual preprocessing and fine-tunes the learning parameters for the proactive prediction of the malicious activities in the IIoT environment.

1.2 Background of Industrial Internet of Things

The Fourth Industrial Revolution (4.0) paradigm can be thought of as a road map that takes us through the four industrial revolutions in the development of manual-to-market industrial production processes. Figure 1.1 illustrates the process of creation. With the beginning of the First Industrial Revolution in the 1800s came the development of mechanization and electric power generation [11]. When mechanical and mechanical power were introduced in the 1800s, the very first Industrial Revolution was launched (Figure 1.2). This resulted in the transition away from physical labor toward the very first methods of production, which was particularly noticeable in the textile industry [12]. The improved overall quality of life played a significant role in the transition process, according to the researchers. Because of the electrification of the world, millions of people were able to industrialize and develop, sparking the Second Industrial Revolution [13]. To illustrate this point, consider the following quote from Henry Ford, which refers to the Ford T-Model automobile: “You can have

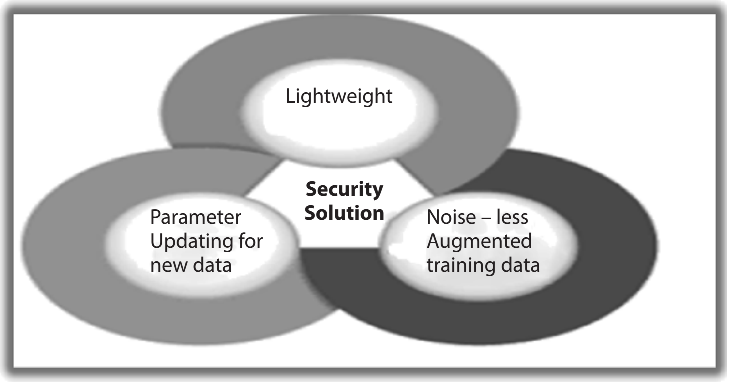
Lightweight
Security Solution
Parameter Updating for new data
Noise – less Augmented training data

Figure 1.1 Challenges in artificial intelligence-based IIoT security model.

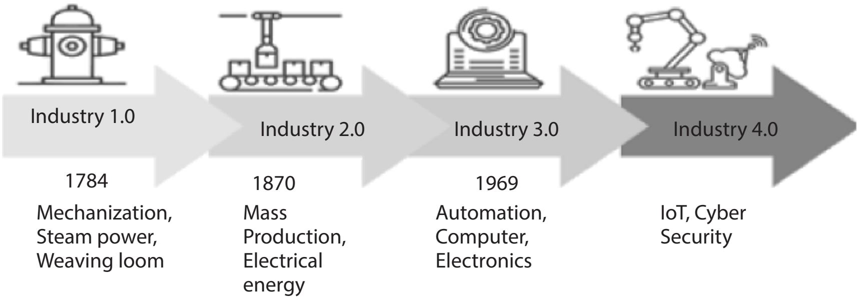
Industry 1.0
1784
Mechanization, Steam power, Weaving loom
Industry 2.0
1870
Mass Production, Electrical energy
Industry 3.0
1969
Automation, Computer, Electronics
Industry 4.0
IoT, Cyber Security

Figure 1.2 The industrial revolutions.

any colour as long as it is black." Although mass production is becoming increasingly popular, there is still room for product customization if mass production is not used. It is the third industrial revolution, which began with the introduction of microelectronics and automation and has continued to the present day [14]. Module manufacturing is encouraged as a result of this, in which a variety of items is created on flexible production lines by employing programmable machines as well as various materials [15].

These manufacturing processes, on the other hand, are limited in their ability to accommodate varying output volumes, which is a disadvantage. The fourth industrial revolution has begun as a result of the advancement of information and communications technology (ICT). Intelligent automation of cyber-physical systems with decentralized control and advanced networking is the technological foundation for artificial intelligence-based systems. Intelligent automation of cyber-physical systems with decentralized control and advanced networking is based on decentralized control and advanced networking (IoT functionalities) [25, 26]. A self-organizing cyber-physical production structure was created by reorienting this new industrial production technology using classical hierarchical automation systems. As a result of this new manufacturing technology, scalable mass-customized production as well as flexibility in terms of production volume are now possible.

Research Gap

The existing security researchers have handled the different types of attacks on the IIoT network by adopting the deep learning and incremental learning models; however, the incremental learning-based security models have been confronted with several shortcomings particularly, in the IIoT network, which are discussed as follows.

- Applying the available existing IIoT security solutions is critical due to the primary concern of the resource constraints in the IIoT network.
- Owing to the need for cross-layer design and optimization algorithms for the security mechanisms, the available security solutions are inappropriate for the IIoT model.
- The DDoS or intrusion detection models often confront the increased probability of false positives, leading to ineffective attack detection [16].
- Lack of modification in the machine learning model while adopting the security solution leads to an increased number of false positives and true negatives.
- Traditional deep learning models lack the development of a reliable, robust, and intelligent security mechanism over the massive scale deployment of the IIoT.
- Static machine learning and deep learning models lead to inaccurate decision-making due to the continuously arriving data streams from different IIoT data sources [17].
- Incrementally identifying the potential features and making the decisions from the extracted set of features over the continuously arriving data streams is critical.
- Traditional preprocessing methods lack to support the effective incremental learning results due to the variations in the inherent relationships of the arriving data [18].
- Incremental learning models lead to inaccurate decision-making without handling the drift data in the

IIoT applications due to the enormous availability of the continuously changing data.

- Modeling the deep learning algorithm with the appropriate parameter values is quite critical for detecting known and unknown attacks in the dynamic IIoT environment.

Challenges in IIoT Security

In the real-world, the IIoT applications often demand both the speed and accuracy ensured data stream mining methods. The IIoT platform confronts major security issues due to the ever-increasing complexity of the attacks, zero-day vulnerabilities, the nature of connected IIoT devices, and the lack of detection of new threats. The existing IIoT security models lack in providing suitable security solutions over the continuous arrival of the IIoT data. Owing to the resource-constrained IIoT environment, modeling the heavy-weight security solution is inappropriate. Even though traditional machine learning and deep learning techniques have been adopted to model the IIoT security solutions, effectively detecting over the continuously arriving IIoT data and developing the lightweight security solution is challenging [19]. The continuous arrival of IIoT data leads to the inaccurate detection or classification of the malicious activities due to the existence of the noisy data, which also leads to the increased computational time. Besides, detecting the new malware or attacks in the IIoT environment with a large number of training samples by the traditional learning model is ineffective [20]. To overcome this obstacle, the incremental learning models have been utilized by the IIoT security researchers. However, training the massive amount of arriving data streams and detecting both the known and unknown malware without selecting the potential features is critical. Hence, there is an essential need to preprocess the massive data streams and protect the IIoT environment from both the known and unknown malware-based attacks [21].

1.3 Literature Review

Several progressive and online algorithms have been written, mostly adapting the existing batch techniques to the progressive environment. Massive theoretical work was done in the stationary environment to test their capacity for generalization and convergence speed, often followed by assumptions such as the linear details. While progress and online learning are well developed and well founded, some publications are only generally aimed at the elder, especially in the context of big data or the Internet of Things technology. Most of these are surveys that classify available methods and certain fields of application.

The principle of progressive learning with a certain motivation for incremental learning is included in Giraud-Carrier and Christophe [15]. They promote progressive learning approaches to incremental projects and also illustrate problems such as e-effects ordering or a trustworthiness query. Gepperth and Hammer recently conducted a survey. Usually, the number of measurements and the number of incoming data instances can be approximated. It can also be presumed how critical the rapid response of the system is. It can also be guessed if a linear classifier is suitable for such tasks.

Challenges in the Environment

An overview of commonly used algorithms with relevant implementation of the real world is also given see Table 1.1.

Incremental learning is done more broadly in streaming environments, but much of the work is geared towards drifting ideas.

Main Properties for Incremental Algorithms for Domingos and Hulten

To sustain the increasingly growing data rate, production, they emphasize the importance of combining models with theoretical performance guarantees, which are strictly limited in time and space processing.

Batch-incremental methods were contrasted and evaluated with examples-incremental methods. The inference is, for example, that incremental algorithms are equally effective, but use less energy and that the lazy strategies function especially well with a slider.

Fernandez *et al.* conducted a big test of 179 batch classes on 121 datasets. This comprehensive analysis also included several implementations trendy various toolboxes and languages. The best results were achieved with the Random Forest algorithm [24] and the Gaussian supporting kernel vector Machine (SVM) [25]. However, for incremental algorithms such work is still desperately missing. In this chapter, we take a qualitative approach and examine in depth the main approaches in stationary settings, instead of a broad comparison. We also track the complexity of the model, which takes time and space to draw the required resources, in addition to accuracy. Our analysis ends with some unknown considerations, such as convergence speed and HPO.

In machine learning, deep learning is a subfield that is concerned with learning a hierarchy of data inputs. Many areas such as image detection, speech recognition, signal processing, and natural language processing

Table 1.1 Comparison charts.

Author name and year	Methodology	Techniques	Security type	Application area	Limitations
Ullah, F. *et al.* (2019)	Detects the malware affected files and software piracy in the IoT through source code plagiarism and color image visualization	TensorFlow deep convolutional neural network	Software piracy and malware detection	IoT software source code	Fails to support the detection of unknown malware
Shafiq, M., *et al.* (2020)	Effectively selects the machine learning algorithm and identifies the Bot-IoT attacks traffic	Bijective soft set approach	Malicious and anomaly traffic	Smart city	Lacks to select the potential features for the continuous arrival of data

(*Continued*)

Table 1.1 Comparison charts. (*Continued*)

Author name and year	**Methodology**	**Techniques**	**Security type**	**Application area**	**Limitations**
Qiu, H., *et al.* (2020)	Eliminates the adversarial perturbations by utilizing the pixel drop operation and employs the sparse signal recovery method and wavelet-based denoising method	Deep neural network	Adversarial attacks	Image classification in smart applications	Lack of consideration on the parameter tuning leads to inaccurate detection over the dynamic data
Parra, G.D.L.T., *et al.* (2020)	Detects the URL attacks, SQL injection, phishing, and DDoS attacks in the IoT through cloud-based distributed deep learning	Convolutional neural network and Long short-term memory	Phishing and Botnet attacks	IoT applications	Training the massively arriving input data leads to time inefficiency

(*Continued*)

Table 1.1 Comparison charts. (*Continued*)

Author name and year	**Methodology**	**Techniques**	**Security type**	**Application area**	**Limitations**
Deshmukh, R. and Hwang, I. (2019)	Detects different types of aviation anomalies over air traffic variations by recursively updating the learning model with the mini-batch of surveillance data	DBSCAN-based clustering and Temporal-logic-based anomaly detection	Anomaly Detection	Terminal Airspace Operations	Fails to detect the surface anomalies in the airspace
Constantinides, C., *et al.* (2019)	Efficiently as well as effectively mitigates both the known and unknown attacks regardless of the signatures or rules	Self-Organizing Incremental Neural Network and Support Vector Machine	Known and unknown intrusion prevention	Internet of Things and Industrial Applications	Leads to increased false positives
Fan, X., *et al.* (2019)	Combines the unsupervised learning with the visualization technology to identify the network behavior patterns in real-time	Deep auto-encoder and Self Organizing Incremental Neural Network	Anomaly detection in a big market	Real-time network traffic	Fails to select the significant features and consider the variations in the features

(*Continued*)

Table 1.1 Comparison charts. (*Continued*)

Author name and year	**Methodology**	**Techniques**	**Security type**	**Application area**	**Limitations**
Reis, L.H.A., *et al.* (2020)	Integrates the incremental learning and unsupervised learning and detects the threats that affect the control loops in the plant	One-class support vector machine	Zero-day attacks and threats	Water treatment plants	Fails to reduce the false positive rate
Li, J., *et al.* (2020)	Performs opcode sequence extraction and selection to detect malware samples	Multiclass support vector machine	Known and unknown malware	Information security in small scale data	Fails to support the large-scale imbalanced data
Zhao, W., *et al.* (2020)	Identifies the changes in the flight operations by detecting the outliers through incremental clustering	Gaussian Mixture Model and Expectation-maximization algorithm	Anomaly detection	Flight Security	Fails to assign the number of clusters and fails to update the parameters

have now been enriched by deep learning algorithms, which have been learned by researchers in order to solve problems.

Deep learning methods are a category of learning methods that can hierarchically learn characteristics from the lower to higher level by constructing a deep architecture. The deep learning methods are able to learn features on several levels automatically, which enable the algorithm to learn complex mapping functions directly from data without human characteristics.

The key characteristic of profound methods of learning is that their models are all profoundly architectured. A deep architecture means that the network has many secret layers. A shallow architecture, in comparison, has only few hidden layers (one to two layers).

Deep neural networks are effectively implemented in different fields: regression, classification, size reduction, movement modeling, texture modeling, information retrieval, processing of natural languages, robotics, error diagnosis and road cracks.

In the ML model, a set of 21 feed profound neural networks was created, which included a variety of DNN values, such as the number of hidden layers, the number of processing units per layer, the triggering of functions, and methods of optimization and regulation. The permutation method [22] has been used to determine the relative value in the ensemble's accuracy of the various biochemical markers. Standardization batch [23] was used to minimize overfit effects and improve the stability of the model's convergence.The best results were obtained by using a DNN with five hidden layers and the regularised mean squared error (MES) function for loss estimation in the loss estimation, the activation PReLU function (PReLU) [24] for each layer and the loss optimization AdaGrad [25] for each layer. The highest DNN score with 82% accuracy was β = 10, i.e. when the predicted age was ±10 years of true age, it found the sample to be correctly accepted, exceeding many groups of the competing ML models. Several models were evaluated for the combination of each DNN into an ensemble (stacking), and the elastic net model was most successful [26]. Albumin, glucose, alkaline phosphatase, urea and erythrocyte have been the most effective blood markers.

This model should be incremental learning as well deep learning in industrial IoT.

1.4 The Proposed Methodology

In recent years, the Industrial Internet of Things (IIoT) has become a popular technology among Internet users for transportation, business, education, and communication development. With the rapid adoption of IIoT technology, individuals and organizations easily communicate with each other without great effort from the remote location. However, the IIoT technology often confronts the unauthorized access of sensitive data, personal safety risks, and different types of attacks. Hence, it is essential to model the IIoT technology with proper security measures to cope with the rapid increase of IIoT-enabled devices in the real-time market. In particular, predicting security threats is significant in the Industrial IIoT applications due to the huge impact on production, financial loss, or injuries. Also, the heterogeneity of the IIoT environment necessitates the inherent analysis to detect or prevent the attacks over the voluminous IIoT-generated data. Even though the IIoT network employs machine learning and deep learning-based security mechanisms, the resource constraints create a setback in the security provisioning especially, in maintaining the trade-off between the IIoT device's capability and the security level. Hence, in-depth analysis of the IIoT data along with the time efficiency is crucial to predict the cyber-threats proactively. Despite, relearning the new environment from scratch leads to the time-consuming process in the large-scale IIoT environment when there are minor changes in the learning environment while applying the static machine learning or deep learning models. To cope with this constraint, incrementally updating the learning environment is essential after learning the partially changed environment with the knowledge of previously learned data. Hence, to provide security to the resource-constrained IIoT environment, selecting the potential input data for the incremental learning model and fine-tuning the parameters of the deep learning model for the input data is vital, which assists towards the proactive prediction of the security threats by the time-efficient learning of the dynamically arriving input data.

Figure 1.3 illustrates the processes involved in the proposed IIoT security methodology. The proposed approach incorporates the contextual preprocessing and the proactive prediction processes with the help of the deep incremental learning model and the optimization method. Initially, to effectively clean the continuously arriving data streams, the proposed approach explores the noisy and misclassified instances in the arrival of data and then incrementally selects the features within a particular timeframe based on the impact on the classification performance. In subsequence, it optimizes

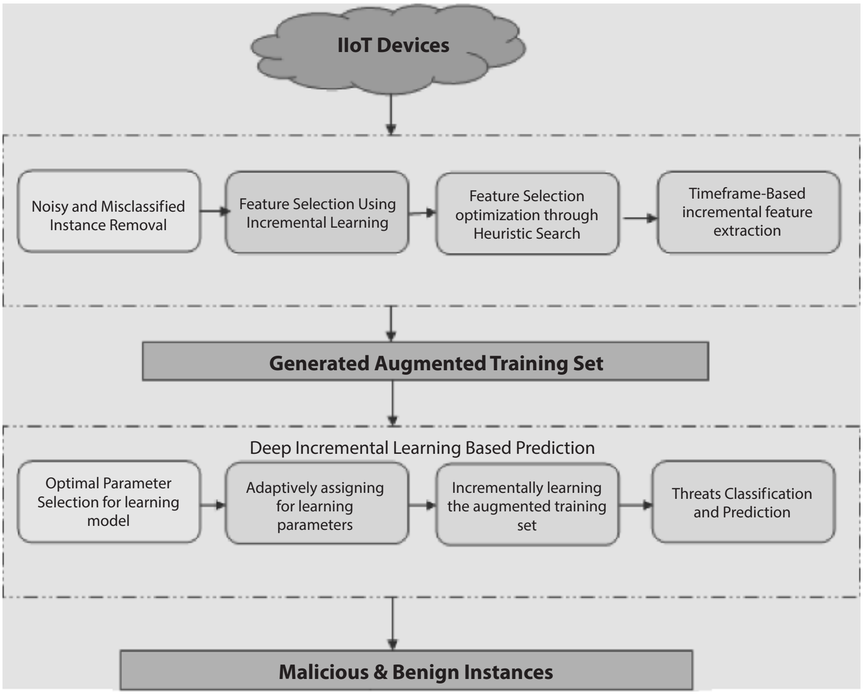
IIoT Devices
Noisy and Misclassified Instance Removal
Feature Selection Using Incremental Learning
Feature Selection optimization through Heuristic Search
Timeframe-Based incremental feature extraction
Generated Augmented Training Set
Deep Incremental Learning Based Prediction
Optimal Parameter Selection for learning model
Adaptively assigning for learning parameters
Incrementally learning the augmented training set
Threats Classification and Prediction
Malicious & Benign Instances

Figure 1.3 Deep incremental learning-based IIoT security model.

the feature selection process through the heuristic search strategy that targets improving the time efficiency in the attack detection process. Moreover, it assists in augmenting training data generation with the optimal features alone, which leverages the improved classification performance. The proposed approach applies the deep incremental learning model with the fine-tuning of the learning parameters for the input data in the IIoT environment. The adaptive updating of the learning parameters associated deep incremental learning model ensures the classification or prediction of the malicious instances in the IIoT platform based on the learning knowledge from the augmented training set. Thus, the proposed approach effectively protects the IIoT environment with improved time efficiency with the help of the deep incremental learning model along with the heuristic model.

1.5 Experimental Requirements

It is necessary to have an i7 processor with 32 GB or extended memory and a 500 GB hard drive in order to run the experimental framework on

Ubuntu 18.04 LTE. The experimental model makes use of the IIoT dataset, which combines the normal data with the data collected during the attack release. Furthermore, in order to run the deep incremental learning algorithm, the experimental framework makes use of the python libraries, which are running on the Python 3.6.8 platform.

Evaluation Metrics

Detection Rate: It is the ratio of the number of correctly detected attacks to the total number of attacks in the IIoT environment. It is also termed as the recall.

Accuracy: It measures the overall detection accuracy of the IIoT security model, which considers the accurate detection performance on both the attacks and normal activities.

Both true positive and true negative refer to the number of malicious activities that were correctly classified or predicted as attacks, as well as the number of normal activities that were correctly classified or predicted as normal. A false positive represents a malicious activity that was incorrectly classified or predicted as normal, while a false negative represents a legitimate activity that was incorrectly classified or predicted as an attack.

1.6 Conclusion

This work presented the incremental learning-based security model for the IIoT environment. The proposed IIoT security mechanism has focused on the classification and prediction of the cyber threats through contextual preprocessing and the deep incremental learning-based prediction. With the target of proactively predicting the malicious instances or activities in the IIoT, this work has outlined the processes of the generation of the augmented training set for the deep increment learning model. The contextual preprocessing involves removing the noisy and misclassified instances, incremental feature selection, and heuristic search-based feature selection optimization. The deep incremental learning-based prediction involves the optimal and adaptive learning parameters selection, learning the augmented training data with the fine-tuned values, and incremental classification and prediction. Thus, the proposed security mechanism proactively protects the IIoT environment from malicious activities through the lightweight and time-efficient intelligence model.

References

1. Alaba, F.A., Othman, M., Hashem, I.A.T., Alotaibi, F., Internet of Things security: A survey. *J. Netw. Comput. Appl.*, 88, 10–28, 2017.
2. Van Oorschot, P.C. and Smith, S.W., The Internet of Things: Security Challenges. *IEEE Secur. Priv.*, 17, 5, 7–9, 2019.
3. Haddadpajouh, H. and Parizi, R., A Survey on Internet of Things Security: Requirements, Challenges, and Solutions. *Internet of Things,* 14, 100129, 2019. doi: 10.1016/j.iot.2019.100129
4. Khraisat, A., Gondal, I., Vamplew, P., Kamruzzaman, J., Survey of intrusion detection systems: techniques, datasets and challenges. *J. Cybersecur.*, 2, 1, 20, 2019.
5. Hussain, F., Hussain, R., Hassan, S.A., Hossain, E., Machine learning in IoT security: Current solutions and future challenges. *IEEE Commun. Surv. Tutor.*, 22, 3, 1686–1721, thirdquarter 2020, doi: 10.1109/COMST.2020.2986444.
6. Al-Garadi, M.A., Mohamed, A., Al-Ali, A., Du, X., Ali, I., Guizani, M., A survey of machine and deep learning methods for Internet of Things (IoT) security. *IEEE Commun. Surv. Tutor.*, 22, 3, 1646–1685, 2020, doi: 10.1109/comst.2020.2988293.
7. Losing, V., Hammer, B., Wersing, H., Incremental on-line learning: A review and comparison of state of the art algorithms. *Neurocomputing*, 275, 1261–1274, 2018.
8. Bhuyan, M.H., Bhattacharyya, D.K., Kalita, J.K., Survey on incremental approaches for network anomaly detection. *Int. J. Commun. Netw. Inf. Sec. (KUST),* 3, 3, 226–239, 2011, 2012. arXiv preprint arXiv:1211.4493.
9. Gepperth, A. and Hammer, B., Incremental learning algorithms and applications. European Symposium on Artificial Neural Networks (ESANN), Bruges, Belgium, ffhal-01418129f, 2016.
10. Dawoud, A., Shahristani, S., Raun, C., Deep learning and software-defined networks: Towards secure IoT architecture. *Internet Things J.*, 3, 82–89, 2018.
11. Guo, W., Mu, D., Xu, J., Su, P., Wang, G., Xing, X., Lemna: Explaining deep learning-based security applications, in: *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pp. 364–379, 2018.
12. Sagduyu, Y.E., Shi, Y., Erpek, T., IoT network security from the perspective of adversarial deep learning, in: *2019 16th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*, pp. 1–9, 2019.
13. Ullah, F., Naeem, H., Jabbar, S., Khalid, S., Latif, M.A., Al-Turjman, F., Mostarda, L., Cybersecurity threats detection in internet of things using deep learning approach. *IEEE Access*, 7, 124379–124389, 2019.
14. Shafiq, M., Tian, Z., Sun, Y., Du, X., Guizani, M., Selection of effective machine learning algorithm and Bot-IoT attacks traffic identification for internet of things in smart city. *Future Gener. Comput. Syst.*, 107, 433–442, 2020.

15. Qiu, H., Zheng, Q., Zhang, T., Qiu, M., Memmi, G., Lu, J., Towards secure and efficient deep learning inference in dependable IoT systems. *IEEE Internet Things J.,* 2020.
16. 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.,* 102662, 2020.
17. Rezvy, S., Luo, Y., Petridis, M., Lasebae, A., Zebin, T., An efficient deep learning model for intrusion classification and prediction in 5G and IoT networks, in: *2019 53rd Annual Conference on Information Sciences and Systems (CISS),* pp. 1–6, 2019.
18. Ibitoye, O., Shafiq, O., Matrawy, A., Analyzing adversarial attacks against deep learning for intrusion detection in IoT networks, in: *2019 IEEE Global Communications Conference (GLOBECOM)*, pp. 1–6, 2019.
19. Deshmukh, R. and Hwang, I., Incremental-Learning-Based Unsupervised Anomaly Detection Algorithm for Terminal Airspace Operations. *J. Aerosp. Inf. Syst.*, 16, 9, 362–384, 2019.
20. Constantinides, C., Shiaeles, S., Ghita, B., Kolokotronis, N., A novel online incremental learning intrusion prevention system, in: *IEEE 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS),* pp. 1–6, 2019.
21. Fan, X., Li, C., Dong, X., A real-time network security visualization system based on incremental learning (ChinaVis 2018). *J. Vis.*, 22, 1, 215–229, 2019.
22. Reis, L.H.A., Murillo Piedrahita, A., Rueda, S., Fernandes, N.C., Medeiros, D.S., de Amorim, M.D., Mattos, D.M., Unsupervised and incremental learning orchestration for cyber-physical security. *Trans. Emerg. Telecommun. Technol.,* e4011, 2020.
23. Li, J., Xue, D., Wu, W., Wang, J., Incremental Learning for Malware Classification in Small Datasets. *Secur. Commun. Netw.,* 2020.
24. Zhao, W., Li, L., Alam, S., Wang, Y., An Incremental Clustering Method for Anomaly Detection in Flight Data. *Transp. Res. Part C: Emerg. Tech.,* 132, 103406, 2021. arXiv preprint arXiv:2005.09874.
25. Almusaylim, Z.A. and Zaman, N., A review on smart home present state and challenges: linked to context-awareness internet of things (IoT). *Wirel. Netw.*, 25, 6, 3193–204, 2019 Aug.
26. Jha, S., Kumar, R., Chatterjee, J.M., Khari, M., Collaborative handshaking approaches between internet of computing and internet of things towards a smart world: a review from 2009–2017. *Telecommun. Syst.*, 70, 4, 617–34, 2019 Apr.