Machine learning approaches to cybersecurity in the industrial internet of things: a review

Melanie Heier[1], Penatiyana W. Chandana Prasad[2], Md Shohel Sayeed[3]
[1]School of Computing, Mathematics and Engineering, Charles Sturt University, Bathurst, Australia
[2]International School, Duy Tan University, Da Nang, Vietnam
[3]Centre for Intelligent Cloud Computing, CoE for Advance Cloud, Faculty of Information Science and Technology,
Multimedia University, Melaka, Malaysia

Article Info

Article history:

Received May 5, 2024
Revised Apr 12, 2025
Accepted May 23, 2025

Keywords:

Artificial neural networks
Cybersecurity
Federated learning
Industrial internet of things
Machine learning

ABSTRACT

The industrial internet of things (IIoT) is increasingly used within various sectors to provide innovative business solutions. These technological innovations come with additional cybersecurity risks, and machine learning (ML) is an emerging technology that has been studied as a solution to these complex security challenges. At time of writing, to the author’s knowledge, a review of recent studies on this topic had not been undertaken. This review therefore aims to provide a comprehensive picture of the current state of ML solutions for IIoT cybersecurity with insights into what works to inform future research or real-world solutions. A literary search found twelve papers to review published in 2021 or later that proposed ML solutions to IIoT cybersecurity concerns. This review found that federated learning and semi-supervised learning in particular are promising ML techniques being proposed to combat the concerns around IIoT cybersecurity. Artificial neural network approaches are also commonly proposed in various combinations with other techniques to ensure fast and accurate cybersecurity solutions. While there is not currently a consensus on the best ML techniques to apply to IIoT cybersecurity, these findings offer insight into those approaches currently being utilized along with gaps where further examination is required.

Corresponding Author:

Md Shohel Sayeed
Centre for Intelligent Cloud Computing, CoE for Advanced Cloud, Faculty of Information Science and Technology, Multimedia University
Jalan Ayer Keroh Lama, 75450 Bukit Beruang, Melaka, Malaysia
Email: shohel.sayeed@mmu.edu.my

1. INTRODUCTION

Industrial internet of things (IIoT) refers to the network of interconnected devices, machines and sensors utilized in various industries for activities such as automation [1], monitoring, control, and data collection [2]–[4]. The process optimization and flexibility provided by IIoT results in reduced costs, increased production, and improved efficiency for businesses or services [3], [5], [6]. As technology has improved, IIoT has become increasingly utilized for various business and industrial processes.

The IIoT provides a unique and challenging context for cybersecurity [7]. IIoT networks comprise a large number of interconnected devices with greater lifespans than consumer devices [4], [8]. These devices may need to interact with legacy systems, putting them at risk [9]. They produce large amounts of data [5] and perform critical business tasks and safety functions [10]–[12]. Devices themselves as well as their software may be outdated, leading to risks associated with a lack of security updates [8]. IIoT devices tend to have limited resources in terms of power and memory, and so cybersecurity solutions need to have low power and low memory requirements [5], [13], [14]. These limitations mean that solutions must also be scalable and adaptable to meet business needs and have the capacity to be retrofitted [4]. Solutions must also be able to process large amounts of data quickly and accurately [15]. Traditional cybersecurity solutions can have difficulties coping with the unique challenges presented by IIoT [16]. Traditional cybersecurity solutions can also require more processing power and memory than IIoT devices possess, creating a challenging environment for device and network protection [14].

Machine learning (ML) is one of the emerging technologies being utilized to solve these cybersecurity challenges. As technology has evolved, cyber-attacks have become progressively more efficient and increasingly challenging to detect [17]. ML techniques can provide innovative, efficient, and timely methods to detect and prevent attacks [2], [17]. These techniques can be utilized in a variety of ways to provide security to IIoT systems, including anomaly detection, feature selection, analysis of networks, or risk assessment [18]. ML models can provide cybersecurity systems with increased efficiency, accuracy and automation [18] important factors in industry applications.

Many industries utilize IIoT including smart cities [19], agriculture, healthcare, power, transportation [10], [20] and manufacturing [21]. The risk to these industries from cyber-attack through IIoT devices and networks could be catastrophic. Due to the nature of IIoT, attacks may affect equipment, presenting a serious risk to personnel safety and service provision [22]. Attacks may result in financial and reputational losses associated with disruptions to service, interference with production or data breaches [5], [10], [20]. Some attacks of concern for IIoT include man-in-the-middle [23], physical, impersonation, routing, malicious code injection and data leakage [4] as well as denial-of-service, replay and deception attacks [24]. Other attacks more specific to the IIoT may include tampering with products, spear phishing or the theft of intellectual property [25]. Network monitoring and intrusion detection are possible solutions to these cybersecurity threats to IIoT, and this is an area where ML approaches have been proposed.

The field of ML is ever growing and IIoT has become increasingly prevalent, presenting unique cybersecurity challenges. It is important to review recent developments and consolidate the information available in these areas in the search for appropriate solutions. This review paper achieves this goal by consolidating and comparing the ML approaches proposed in twelve recent papers, providing an overview of the current state of ML as an approach to IIoT cybersecurity.

There were two main architectures arising from the current literature: an intrusion or attack detection architecture and a federated learning architecture. These approaches offer a way to detect cybersecurity attacks or intrusions and utilize ML approaches to process data and identify anomalies. Of those papers reviewed, ten used one of these approaches.

The main architecture utilized for proposed solutions to IIoT cybersecurity was the attack detection architecture, as displayed in Figure 1. In an attack detection approach, data is first collected, then pre-processed according to the model's needs and the composition of the data [26]. Data is then split into testing or training segments and fed into various layers of machine learning techniques to perform the attack detection and classification [27]. The model's performance is then evaluated. This architecture is utilized by seven of the twelve papers examined in this study. This attack detection approach can be applied at the network level to address IIoT network vulnerability [3], [5], [28], [29], or at the device level to address the vulnerability of physical systems [30], [31]. This architecture can also be utilized for IIoT monitoring systems [32]. These types of attack detection systems are able to successfully use various ML techniques to detect attacks and thereby protect IIoT devices and systems. However, they do not address privacy concerns as federated learning approaches do, which is an important part of IIoT cybersecurity. Attack detection solutions utilizing ML techniques can help to identify denial of service (DoS) attacks, malware and other cybersecurity threats that may cause anomalies in data or network traffic [18].

The second main type of architecture presented in the current literature is displayed by the three models using federated learning (FL) [2], [33], [34]. This architecture is displayed in Figure 2. In this type of approach IIoT clients train their own local attack or intrusion detection model. The resulting training information is then sent to a central server, which updates the global model with the local data before returning the updated global information to each client [35]. The clients then update their own local models in order to perform attack detection [1].

FL is largely used to address privacy concerns around data transmission [2], [36], as raw data is not sent, rather it is the trained parameters that are transmitted to a central server [1], [30], [37]–[39]. FL can also provide scalability and real-time detection of anomalies [39]. Li *et al.* [33] and Makkar *et al.* [34] take FL's privacy a step further by also adopting an encryption system to ensure the information being transferred has an extra layer of security. Both models utilize a Paillier encryption system, with Li *et al.* [33] also adding AES encryption. FL architecture is able to address real-world concerns such as data privacy and security [35], [38]. However, model complexity and the processing capabilities of IIoT devices must be considered as they need to be able to perform their own model training and these devices may not have the required processing power [40]. As well as processing load considerations, federated learning techniques also face challenges of devices reconnecting after being offline and protect each facet of the process, including the centralized data collection point and information transfers between device and central server [38].

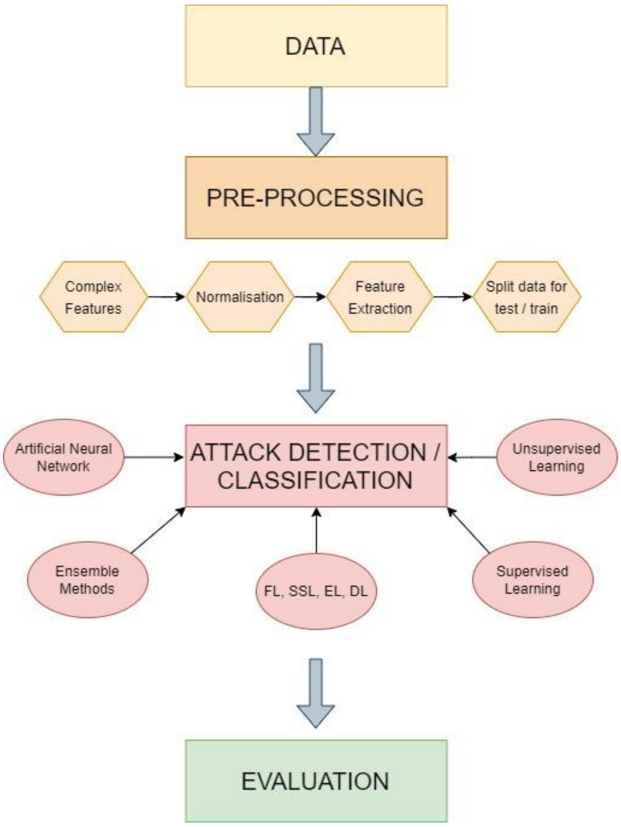

Figure 1. General flow of attack detection approaches. Based on diagrams from Fu *et al.* [28], Shahin *et al.* [30], Tran *et al.* [31], and Chakraborty *et al.* [32]

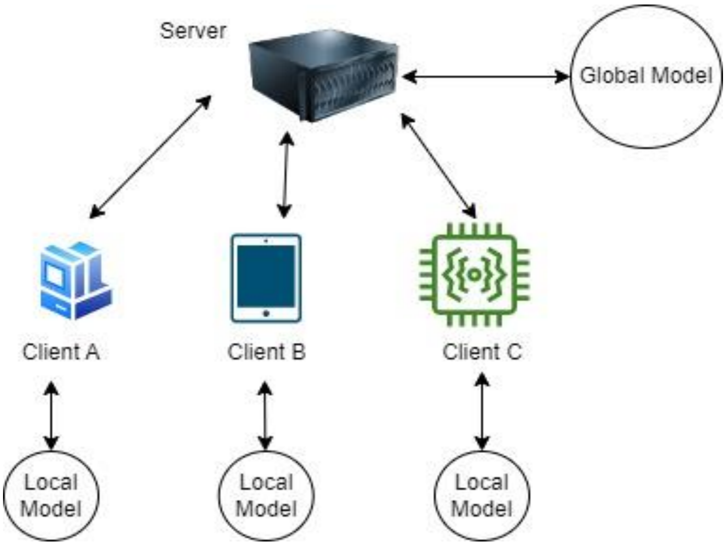

Figure 2. General flow of federated learning approaches. Based on diagrams from Aouedi *et al.* [2] and Li *et al.* [33]

Table 1 summarizes the most commonly proposed techniques and their categories. Table 2 summarizes the components present in the reviewed literature. Components are comprised of the software related tools used by researchers, the datasets used to evaluate the ML models, the attack types included in those data sets, the techniques used in the proposed models, the metrics used to measure model performance, and the variables that were adjusted to examine the performance of the proposed models. These components are organized into four categories of tools, input, techniques and output. Table 3 breaks down these components by paper. As can be seen in Table 2 techniques section as well as Table 3, the current literature proposes many different ML techniques used in various combinations for cybersecurity in IIoT. Broadly, these techniques include categories of artificial neural networks, supervised, unsupervised and semi-supervised learning, deep learning, ensemble learning, and ensemble methods. Due to the limited scope of this review, the focus will be on the common techniques as presented in Table 1. One paper did not specify their technique, merely stating machine learning (ML) and deep learning (DL) algorithms [33], making its comparison incompatible with others presented here.

Table 1. Most common ML techniques

Category	Abbr.	Technique
Artificial neural network (ANN)	CNN	Convolutional neural networks
	FCNN	Fully convolutional neural networks
	MLP	Multilayer perceptron
	LSTM	Long short-term memory
Supervised learning	DT	Decision tree
	RF	Random forest
Ensemble methods	XGBoost	Extreme gradient boosting

Table 2. Components

Factors	Attributes	Instances
Tools	Software	OPNet Network simulation, Netflow, Redis, Anaconda Navigator, Tensorflow, Google Colab, LabVIEW, CONTACT Element Platform
	Frameworks, libraries, languages	Pytorch, Flask, Keras, Scikit-Learn, Python
Input	Dataset	Gas pipeline SCADA system, water storage tank control system, Secure Water Treatment, CIC-IDS-2018, DS2OS, UNSW-NB15, SCADA power system, XIIoTID, BoT-IoT, ToN-IoT, Glitches, Bot attack samples, induction motor bearing conditions
	Attack type	NMRI, CMRI, MSCI, MPCI, MFCI, DoS, DDoS, Recon., Heartbleed, web attacks, botnet, INFI, UtR, MC, MO, WS, spying, scan, DTP, fuzzers, backdoor, analysis, exploit, generic, shellcode, worm, weaponization, LM, C&C, ransom DoS, exfiltration, crypto-ransomware/ransomware, keylogging, injection, MITM, password, XSS, SS-SPASSMPA, MS-SPA, MS-MPA, Botnet, IRF, ORF, cyber-attack
	Dataset type	Sourced, self-created
Techniques	Machine learning approaches	FL, SSL, EL, DL, ML, AE, FCN, MLP, ELM, CNN, GRU, LSTM, FCNN, ALSTM, RF, XGBoost, LightGBM, AdaBoost, LR, SVM, k-NN, DT, CA, HCA, PRU, RaNN
	Other techniques	FSA, FPCA, Paillier, AES
Output	Evaluation metrics	Accuracy, precision, recall, F1 score, log loss, communication overhead, AUC/ROC, safety factor, MCC, TPR, TNR, FPR, FNR, TP, FP, TN, FN, detection time
	Variables	Number of clients, local client epochs, communication rounds, amount of unlabeled data, Segment size, Time allocated for decision making, linear/non-linear sensors, Number of features, Learning rate, Time slots, Binary classification /multiclassification, dataset, learners, model, type of attack, training/testing, device

Summary of instances of attributes from papers included in the literature review. Abbreviations used in table are listed in the Appendix.

Artificial neural networks (ANN) are part of DL, a subsection of ML. They can be utilized in models for cybersecurity to detect malware or analyze network behavior [16]. ANN techniques can also be utilized for time series prediction or speech recognition [41]. In the reviewed papers, ANNs were largely used for data classification [42] and to extract features [30]. This process of classification and feature extraction allows new data to be easily classified or filtered based on previously processed information [42]. ANNs generally consist of a number of connected nodes that each perform data processing [43]. ANN nodes consist of three layers: one for input, one for output and one hidden layer for processing [30], [43], [44].

The most commonly proposed ANNs in the literature include convolutional neural networks (CNN) [29], [33], [34], fully convolutional neural networks (FCNN) [29], [30], [34], multilayer perceptron (MLP)

[5], [33] and long short-term memory (LSTM) [3], [29]. As seen in Table 3, the datasets used to test these models included: UNSW-NB15, BoT-IoT, ToN-IoT, a gas pipeline system, a supervisory control and data acquisition (SCADA) system, and XIIoTID. Also shown in Table 3, these datasets addressed a range of attack types, including but not limited to: DoS, backdoor, ransomware, man-in-the-middle (MITM), cross site scripting (XSS), reconnaissance (recon.) and worms.

Table 3. Classification

Ref	Tools	Input			Techniques	Output	
[#]	SW, FW, Libs, Langs.	Dataset	Attack type	Dataset type	ML and other approaches	Evaluation metrics	Variables
[2]	Pytorch, Scikit-Learn, Python	Gas pipeline SCADA system dataset, water storage tank control system	NMRI, CMRI, MSCI, MPCI, MFCI, DoS, Recon.	Sourced	AE, FCN, FL, SSL	Accuracy, precision, recall, F1 score, communication overhead	Num. clients, local client epochs, CR, amount of unlabeled data
[3]	Pytorch, Python	SCADA power system datasets (15 datasets)	Unspecified (thousands of distinct attacks)	Sourced	PRU, DT, LSTM, EL	Accuracy, FPR, TP, FP, TN, FN	Binary/ multiclassification, dataset, learners
[5]	Anaconda Navigator, Tensorflow, Keras	DS2OS, UNSW-NB15	DoS, MC, MO, WS, spying, scan, DTP, fuzzers, backdoor, analysis, exploit, generic, shellcode, worm	Sourced	MLP, RaNN	Accuracy, precision, recall, F1 score, log loss, AUC-ROC	Learning rate
[45]	Google Colab	Glitches	Glitches (8890 over 12 hours)	Self-Created	HCA, ELM, SSL	Accuracy, precision, recall, F1 score	Time slots
[46]	Unspecified	Bot attack samples	Botnet	Self-Created	DL, ML	Accuracy, precision, recall, F1 score, MCC, FPR	
[28]	Opnet, Netflow, Redis	CIC-IDS-2018	DoS, Recon., Heartbleed, web attacks, botnet, inside, UtR	Sourced	CA	Safety factor, TP, FP, detection time	Number of features
[29]	Scikit-Learn	UNSW-NB15, BoT-IoT, ToN-IoT	Fuzzers, backdoor, analysis, exploit, generic, shellcode, worm, DoS, DDoS, Recon., scan, exfiltration, ransomware, keylogging, injection, MITM, password, XSS	Sourced	CNN, LSTM, FCNN	Accuracy, precision, recall, log loss	Dataset, model
[30]	Scikit-Learn	ToN-IoT	DoS, DDoS, Recon., scan, backdoor, ransomware, injection, MITM, password, XSS	Sourced	XGBoost, AdaBoost, FCNN, ALSTM	Accuracy, precision, recall, F1 score	Model, device, attack type
[31]	CONTACT Element, LabVIEW	induction motor bearing conditions	IRF, ORF, cyberattack	Self-created	DT, RF, XGBoost,	Accuracy, AUROC, TPR, FPR, TP, FP, FN	Model, motor status (attack type)
[32]	Unspecified	SWaT	SS-SPA, SS-MPA, MS-SPA, MS-MPA	Sourced	LR, SVM, k-NN, RF, FSA, FPCA	Accuracy, precision, recall, F1 score, TP, FP, TN, FN	Segment size, Time for decision making, linear/ non-linear sensors, Model
[33]	Flask, Keras, Python	Gas pipeline SCADA system	NMRI, CMRI, MSCI, MPCI, MFCI, DoS, Recon.	Sourced	MLP, CNN, GRU, FL, Paillier, AES	Accuracy, precision, recall, F1 score	Num. clients, CR, local/ideal/proposed model, type of attack
[34]	Google Colab, Pytorch	XIIoTID	Recon., exploit, weaponization, LM, C&C, ransom DoS, exfiltration, ransomware	Sourced	RF, XGBoost, LightGBM, CNN, LSTM, FL, Paillier	Precision, recall, F1 score, TPR, TNR, FPR, FNR	Num. clients, model, training/testing

The contents of the component table broke down by paper. Abbreviations used in the table are listed in the Appendix.

CNNs are often used for visual recognition activities [41], [47], and are able to extract features automatically [29]. CNNs consist of a number of convolutional layers used to extract features and a number of fully connected layers used to classify these features, thereby providing the combined output [28], [41], [44], [47]. As with other ANNs, CNN algorithms can be used in combination with other ML techniques.

An FCNN is an CNN comprised only of convolutional layers [30], [48]. FCNN in particular is able to perform well in terms of time and resources when there are many variations in the data [29], [30], [49], [50]. This is because the neurons in each layer are not fully connected [29].

The MLP is also known as a feed-forward fully-connected multi-layer neural network [51]. An MLP creates correlations between the input and output data by adjusting the neurons in its layers [30]. Continuing investigation into the use of MLP discovered that performance was able to be improved by sequentially pre-training layers [51].

LSTM is a type of recurrent neural network that is able to recall prior information, learn feature dependencies [52] and learn order dependency in sequence prediction [29], [30]. LSTM utilizes gates for input, output and forgetting to process memory data [29], [41], [52]. LSTM is able to be utilized with other ML techniques to assist with accurate attack prediction. LSTM techniques have been applied in IIoT systems in industries such as finance, healthcare, and transportation [41].

These ANN techniques have been combined with various other ML approaches to formulate models. These models have been compared in different ways in the reviewed literature. Shahin *et al.* [29] compared two models: one combining LSTM with CNN and the other combining LSTM with FCNN. Makkar *et al.* [34] compared four models within a federated learning architecture: CNN, LSTM and two ensemble method models. Each of these models used random forest (RF) for feature organization, and ensemble methods for training. These kinds of model comparisons are useful in the analysis of specific technique performance.

Others in the reviewed literature formed their models with a combination of ANN and non-ANN ML approaches. Huma *et al.* [5] and Khan *et al.* [3] both combined ANN techniques with deep learning, though in different ways. Huma *et al.* [5] utilized a deep random neural network (RaNN) with MLP. Khan *et al.* [3] proposed a pyramidal recurrent unit (PRU) model that incorporated LSTM. In this way, ANN techniques have the flexibility to be applied in many different model types.

Li *et al.* [33] utilized ANN approaches within a federated learning architecture alongside other techniques. They proposed a model utilizing both MLP and CNN along with another ANN technique-gated recurrent unit (GRU). GRU methods offer an efficient option that requires less computational resources [53]. ANN appear to be a popular ML method for IIoT cybersecurity, and these techniques have the flexibility to be applied in different ways and with different ML and non-ML techniques. Neural network techniques do have drawbacks however when it comes to application in IIoT. These techniques can have a high computational cost and be susceptible to overfitting [14]. Neural network models also take time to complete their training phase, and can require large amounts of data [14].

The two most common supervised learning techniques utilized in the reviewed papers were decision tree (DT) [3], [31] and RF [32], [34]. As can be seen in Table 3, datasets used to test these models included multiple SCADA power system datasets, a self-created equipment-based dataset, SWaT and XIIoTID datasets. Also shown in Table 3, these datasets covered a range of attacks including but not limited to cyberattack, DoS, ransomware, reconnaissance, and single and multi-point attacks.

The DT technique builds its training models by learning rules for decision making [54], [55]. This technique begins with a single node and then branches out to create more nodes for each possibility [56]. Each new node has the potential to branch out further [56]. DT is able to train models quickly and with less required memory [31]. DT can be utilized in a number of ways, including image processing, classifying data and pattern recognition [16]. RF is a classifier consisting of a number of decision trees [57]. The use of RF offers accuracy to a model [57] as well as speed of learning [58].

Khan *et al.* [3] utilized DT along with ensemble-learning to process the output of previous layers of the model before making the final decision on whether the data signified an attack. Tran *et al.* [31] compared a standalone DT model with an RF model and another model using extreme gradient boosting (XGBoost). Conversely to other models presented here, Chakraborty *et al.* [32] primarily utilized non-ML techniques for their model, but utilized different supervised learning techniques for attack classification. They compared logistic regression (LR), support vector machine (SVM), k-nearest neighbor (k-NN) and RF. Like ANN techniques, supervised learning approaches provide some flexibility to be utilized in different ways with different ML techniques.

There were three ensemble methods utilized in the reviewed literature, all of which were gradient boosting algorithms. Gradient boosting algorithms calculate the mistakes of earlier models by creating a new model [59]. They then make a choice based on the amalgamation of the new and old models. Generally, the inclusion of a boosting algorithm can improve performance [59]. The most common ensemble method proposed was XGBoost [30], [31], [34]. This algorithm is considered to have low resource dependency and a fast speed [60]–[62]. Shahin *et al.* [30] confirmed these observations, while also stating that it performed well in terms of network intrusion detection. Tran *et al.* [31] similarly stated that this method has performed well in terms of fault detection, though can, if not used with other processes, increase the resources required. It is apparent from the literature that in terms of ensemble methods, gradient boosting algorithms in particular are popular methods to use in ML approaches to IIoT cybersecurity.

Semi-supervised learning can process both unlabeled and labelled data [2], [63]. This technique utilizes unsupervised learning with unlabeled data to extract features from it. It then uses supervised learning to incorporate a small amount of labelled data to calibrate the features and construct the model for use in attack detection [2], [63]. This technique is used by Aouedi *et al.* [2] within their federated learning model to solve the issue in IIoT cybersecurity of needing to examine large amounts of unlabeled data to determine whether an attack would have occurred. Conversely, Jiang [45] utilizes semi-supervised learning in their model to detect voltage glitch attacks (VGA) from glitches in power signals from an IIoT machine. Table 3 shows the datasets utilized by these approaches to examine performance. These datasets included both network or device data and equipment glitches, covering a range of potential attack surfaces in IIoT. These differing applications of semi-supervised learning demonstrate that it is a versatile and flexible approach suitable for cybersecurity applications in IIoT.

As can be seen in Tables 2 and 3, proposed solutions in the current literature use not just a multitude of ML techniques, but test against many different datasets, covering a wide range of attack scenarios. They also utilize many different evaluation metrics and variables, making it difficult to draw comparisons between the performance of different models as this paper attempts. There were some commonalities among the programming languages, tools and libraries where these were mentioned in the studies.

In terms of datasets, there were three most common in use in the literature: a gas pipeline SCADA system dataset [2], [33] UNSW-NB15 [5], [29] and ToN-IoT [29], [30]. These datasets are all based on IIoT and cover a wide range of attack scenarios, as can be seen in Tables 2 and 3. Using the same datasets can make it easier to make comparisons between different approaches [64]. For example, Huma *et al.* [5] and Shahin *et al.* [29] both use the UNSW-NB15 dataset, making it easier to compare the results achieved by their respective models.

Similarly, differing evaluation metrics make models difficult to compare. For example, Fu *et al.* [28] proposed a hierarchical abnormal traffic detection method utilizing an unsupervised clustering algorithm. This model was able to detect anomalies in the shortest amount of time in comparison to other selected models. However, as this model did not use any of the metrics common to other reviewed models, its performance is not easily comparable in this review. Their data was also mainly presented in the form of bar graphs, rather than numerically, making score interpretation potentially inaccurate.

The range of variables shown in Tables 2 and 3, while providing excellent data within single papers, can again make comparison troublesome between separate experiments. As can be seen in Table 3, model comparisons were the most prominent variable [29]–[34]. Comparing models using the same variables can be very useful to determine the performance of different ML techniques. Comparing performance based on dataset or attack type was also common [3], [29]–[31]. When it came to actual parameters of the models, the number of clients was the most common variable for comparing performance [2], [3], [34]. This is an important point of comparison, as the number of devices within an IIoT environment could vary.

While input and output components were many and varied, tools used by the different approaches were fewer. Of those that mentioned the programming language used, all utilized python [2], [3], [46]. The most commonly used tool was Google Collaboratory [34], [45]. Of the frameworks and libraries mentioned, Pytorch [2], [3], [34] and Scikit-Learn [2], [29], [30] were most common. Some tools and libraries were unspecified in the reviewed literature [32], [46].

The most recently proposed solutions to IIoT cybersecurity that utilize ML approaches have not yet been consolidated and evaluated. This paper will review these solutions to provide an overview of the current state of ML approaches to cybersecurity in IIoT. The key research questions include:

a. What are the cybersecurity concerns within the IIoT?
b. What are the most recent machine learning approaches being proposed to solve these cybersecurity concerns?
c. What are the advantages and disadvantages of these approaches?
d. What software and programming languages are being used to implement machine learning approaches to cybersecurity for IIoT?

2. METHOD

This review utilized Charles Sturt University library resources, specifically *https://primo.csu.edu.au* to locate appropriate articles for the topic. Inclusion criteria: i) Published in 2021 or later, ii) Peer reviewed,

iii) Have a journal rating of Q1 or Q2 according to Scimago Journal and Country Rank (SJR) journal rankings, and iv) Propose a ML approach to cybersecurity in IIoT.

The research methodology for this project is outlined in Figure 3 and is as follows. First, searches were performed in order to formulate the topic. Initial keywords used were “software design OR software development” and “cyber security”. The results of this search were then grouped into common topics, and additional keywords added including “machine learning OR deep learning” and “IIoT OR Industrial Internet of Things OR industry 4.0”. The topic of ML approaches to cyber security was then selected based on the common topics of articles found. The resulting collection of articles was then screened and selected according to the inclusion criteria outlined above and their suitability for the topic. The scope for this review was limited to twelve papers due to assignment requirements.

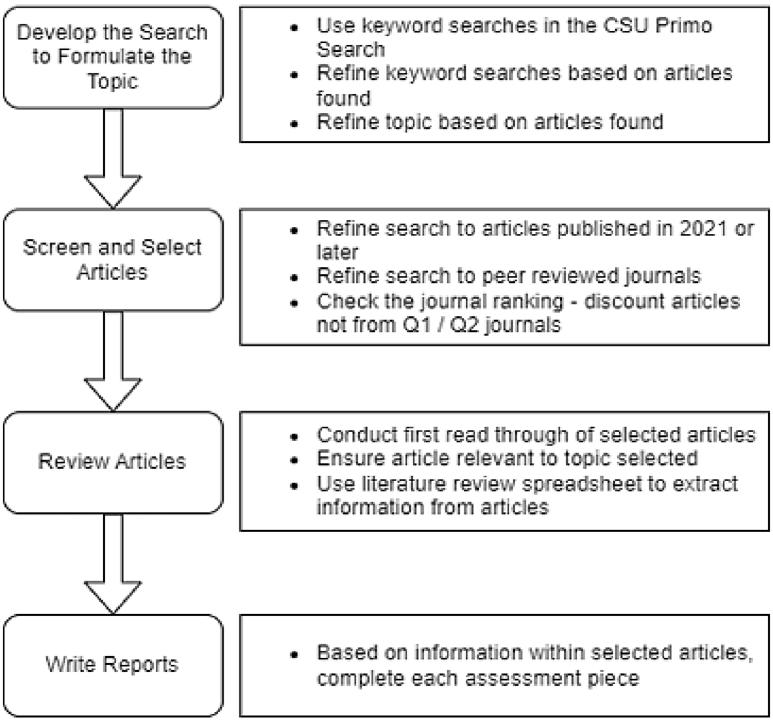
Develop the Search to Formulate the Topic
Use keyword searches in the CSU Primo Search
Refine keyword searches based on articles found
Refine topic based on articles found
Screen and Select Articles
Refine search to articles published in 2021 or later
Refine search to peer reviewed journals
Check the journal ranking - discount articles not from Q1 / Q2 journals
Review Articles
Conduct first read through of selected articles
Ensure article relevant to topic selected
Use literature review spreadsheet to extract information from articles
Write Reports
Based on information within selected articles, complete each assessment piece

Figure 3. Research methodology. Adapted from Deakin University [65]

Data extraction was performed with the use of Excel spreadsheets. A broad feature analysis was completed, which involved summarizing the following features of each paper: i) problem definition, ii) proposed solution, iii) advantages and disadvantages, iv) method, steps, and/or stages, v) limitations and justifications, vi) challenges, vii) hardware, software and programming languages, viii) models used for comparison to the proposed solution, and ix) future work suggested. The specific techniques used in the reviewed articles were consolidated, as were the datasets, implementation procedures, evaluation criteria and results. Finally, this extracted data was utilized to complete this final report.

The consolidated techniques were reviewed to determine those that were most used by the papers under review. These common techniques were grouped into the categories of ANN, supervised learning and ensemble methods as shown in Table 1. These common techniques were used for discussion and comparison in order to maintain the focus and scope of the paper. For example, Chakraborty *et al.* [32] utilized LR, SVM and k-NN, however it was the only paper among the twelve reviewed to use these techniques, and so they were excluded from in-depth discussion.

3. RESULTS AND DISCUSSION

3.1. Results

Table 4 displays the accuracy, precision, recall and/or F1 scores for each paper’s best scoring model. Where models were compared to state-of-the-art techniques within the paper, these comparison scores were taken for Table 4. The variables column shows any variables associated with the achievement of those best scores. Fu *et al.* [28] was the only paper that did not use any of these common evaluation metrics as noted in the table. Scores were only included in Table 4 where the precise score was stated by the authors; scores displayed only in graph form were excluded.

Accuracy is the metric most utilized by literature and so is discussed here in further detail. Accuracy is described as the percentage or ratio of correct predictions [5], [29], [46]. As can be seen in Table 4, the highest accuracy of 100% was achieved by Shahin *et al.* [29] on the BoT-IoT and UNSW-NB15 datasets with their model using LSTM and FCNN techniques. Shahin *et al.* [30] did also achieve a 100% accuracy for one of the devices in their study, however as both of their models achieved 100% in that case, the next highest score would have been taken that differentiated the models. Unfortunately, since their accuracy scores were presented only in bar graph form, a specific accuracy score was not able to be discerned for inclusion in the table. The lowest accuracy score of .78 was achieved by the model utilizing primarily non-ML techniques, suggesting that ML techniques generally have superior performance in this area. Techniques utilized in models achieving 99% or above accuracy include FL [33], ANN [5], [29], [33], ensemble methods [31], supervised learning [31], and deep learning [5]. The only ML technique used by more than one of these high accuracy achieving models was MLP. These results demonstrate that ANN techniques in particular are successfully being utilized in ML solutions to IIoT cybersecurity.

Table 4. Evaluation

Best model	Ref [#]	Techniques	Accuracy	Precision	Recall	F1	Variables
Federated semi-supervised learning scheme	[2]	AE, FL, FCN, SL	95.84%	97.89	87.15		Overall Scores
DL based SCADA network based cyberattack detection scheme	[3]	PRU, DT, LSTM, EL	98.89%				binary classification with dataset 1
HDRaNN	[5]	MLP, RaNN	0.9919	0.9907	0.9898	0.9902	dataset: UNSW-NB15
Heuristic semi-supervised learning method	[45]	CA, ELM, SSL	90.7	90.7	90.7	90.7	Timeslot: 10
Secure network model	[46]	DL, ML	0.87	0.907	0.864	0.881	Overall Scores
Secure clustering algorithm for complex attribute features	[28]	CA					used only TP and FP evaluation metrics and only presented in bar graph form
LSTM-FCN and LSTM-FCN 5-folds CV	[29]	LSTM, FCNN	100%				datasets: BoT-IoT and UNSW-NB15
Deep hybrid learning model	[30]	ALSTM, FCNN, AdaBoost		99.90%	99.90%	99.90%	booster: AdaBoost, device: GPS
Online fault diagnosis with RF	[31]	RF	99.03%				Overall Scores
FM4: functional position and velocity model	[32]	FSA, FPCA, RF	0.78		1	0.78	segment size 40 or 200
DeepFed	[33]	MLP, CNN, GRU, FL, Paillier, AES	99.20%	98.85%	97.47%	98.14%	num clients: 7, comm. Rounds: 10
SecureIIoT - CNN model	[34]	FL, CNN, RF		0.51	0.97	0.67	testing, train: 0

Selected results of each paper's best performing model including associated variables if alternative variable values were associated with different scores. Abbreviations used in table are listed in the Appendix.

3.2. Discussion

The aim of this review was to provide an overview of the current state of ML solutions to cybersecurity in IIoT by examining the proposed solutions from recent years. By undertaking this examination, this review provides insights into what works in order to inform future research or the development of real-world solutions. The most commonly proposed ML techniques were discussed and compared, along with other aspects of studies into IIoT cybersecurity solutions such as data sets and evaluation metrics. This review showed that some of the most promising ML techniques for application in IIoT cybersecurity include FL, FCNN, RF and semi-supervised learning.

It is clear from the current literature that cybersecurity in IIoT is of growing concern due to the potential consequences of an attack [2], [5], [34], and the vulnerability of IIoT devices and networks [2], [3], [5], [29], [32]–[34]. The literature identifies that industries utilizing IIoT are increasingly being targeted by cyber-attacks of varying forms [5], [29], [30], [32] and that the data being stored in and transferred between these devices requires privacy protection [2], [3], [5], [32]–[34]. In terms of intrusion and attack mechanisms for IIoT, the literature agrees that accuracy [3], [28], [32] and efficiency [2], [3], [32] are very important.

3.2.1. Architecture

In order to achieve accuracy, efficiency, and security in IIoT cybersecurity solutions, various machine learning techniques are proposed in the literature. The solutions proposed are divided into two types of architecture: attack detection architecture and FL architecture. An attack detection architecture provides flexible application, as it can be applied at the network level [3], [5], [28], [29], at the device level [30], [31], or within monitoring systems [32]. The downside of this approach is that data is often sent from devices and processed elsewhere. This raises concerns about data privacy, as well as data security in transmission. Depending on the industry utilizing the solution, there may also be legalities to consider in this area of data safety. The FL architecture approach addresses this limitation through training a model on the device itself and sending training model parameters rather than the raw data to a central location. Some models in the reviewed papers also including data encryption to improve security [2], [33], [34]. The downside of this approach, however, is the processing power required to complete training and processing on the device itself, which IIoT devices may not have capacity for.

3.2.2. Techniques

It was clear from the literature that many different ML techniques are being utilized in proposed IIoT security solutions. It is also apparent from the literature that at this stage there are no agreed upon best methods for IIoT cybersecurity solutions. As different algorithms can be combined in different ways, there are a multitude of possibilities in this space.

The most commonly proposed ML techniques fell into four categories: ANN, supervised learning, ensemble methods and semi-supervised learning. Of the ANN techniques, the most commonly utilized were CNN [29], [33], [34], FCNN [29], [33], [34], MLP [5], [33], and LSTM [2], [12]. FCNN in particular provided good processing time with a low level of resources required [29], [30].

The comparisons included in some papers provided insight into the performance of specific ML techniques, particularly within the ANN category. Makkar *et al.* [34] compared models using CNN, LSTM and two ensemble methods, and found that the CNN model had the best performance, as captured in Table 4. However, they found that an increase in the number of devices correlated with an increase in the time taken to process data as well as the time taken to detect attacks [34]. Shahin *et al.* [29] compared two models, one combining LSTM with CNN and the other combining LSTM with FCNN. As displayed in Table 4, they found that the model utilizing FCNN outperformed the one using CNN across two different datasets. From these comparisons, it can be surmised that in terms of attack detection for IIoT, models utilizing CNN techniques outperform LSTM models, and FCNN models outperform those using CNN techniques.

These comparisons, along with the best model results from Table 4, assist in drawing conclusions about which techniques stand out in the current literature. The results in Table 4 show that the ANN technique most commonly used by the models that achieved an accuracy above 99% was MLP. Therefore, it is clear that FCNN and MLP are particularly promising ANN techniques for IIoT cybersecurity solutions.

Supervised learning techniques in the current literature can be evaluated in a similar manner. Chakraborty *et al.* [32] compared their model using different supervised learning techniques for classification, finding that RF outperformed LR, SVN and k-NN approaches. Similarly, Tran *et al.* [31] found that an RF model outperformed models using DT and XGBoost. It can be seen then, from these comparisons that RF is the popular and best performing supervised learning technique within the current literature.

Contrary to MLP, RF was not among the most utilized technique in the top-scoring solutions shown in Table 4. However, it did feature in several of the models that performed the best in their particular study [31], [32], [34]. This supports the results of those studies that found improved performance by including RF in their models and shows that RF is a promising ML technique for IIoT cybersecurity solutions.

Gradient boosting algorithms were the main methods utilized in the category of ensemble methods, with XGBoost being the most commonly used [30], [31], [34] and shown to be a good technique for network intrusion detection [30] as well as fault detection [31]. However, when Shahin *et al.* [30] compared their Attention based LSTM (ALSTM)- FCNN model with XGBoost and AdaBoost, the model using AdaBoost actually provided better performance in terms of precision, recall and F1 score.

Semi-supervised learning techniques were utilized by Aouedi *et al.* [2] and Jiang [45] in different ways. This type of learning was well suited to dealing with large amounts of unlabeled data along with some labelled data as often exists in IIoT environments [2]. However, IIoT environments may also have amounts of purely unlabeled data, which would not be able to be processed by these types of models [2]. Despite this limitation, being able to process the combined labelled and unlabeled data suggests that semi-supervised learning is a good option for IIoT cybersecurity solutions.

More recent papers have looked at reinforcement learning (RL) as an adaptive and flexible ML tool in cybersecurity, though this technique can also have a high computational cost [18]. RL seeks to train an agent in how to behave in its environment in a way that will maximize rewards [18]. There are many different techniques and combinations of techniques that could be further considered for future research in IIoT cybersecurity.

3.2.3. Implementation and evaluation

Datasets, evaluation metrics and variables are areas in the IIoT cybersecurity literature with not a lot of commonalities. The three most commonly used datasets were a gas pipeline dataset [2], [33], UNSW-NB15 [5], [29] and ToN-IoT [29], [30]. As models can perform differently across different datasets, this could provide an area of future research to determine the best datasets to use in the evaluation of ML approaches to IIoT cybersecurity. More recent papers have applied ML models to Virtual Power Plants, offering a focus on more concrete implementations of ML solutions [36] that future reviews could examine and contrast. Alternatively, future reviews could focus on models that utilize the same datasets in order to compare performance.

Similarly, variables used to evaluate proposed solutions in the literature were numerous. This makes comparisons between models from different papers difficult, though it can provide detailed evaluation of models within their own experiments. Model comparisons in particular were the most prominent [29]–[31], [33], [34] and provided good comparisons of different ML techniques, contributing to an evaluation of their performance. In terms of model parameters, the number of clients was the most common variable used to evaluate a model's performance [2], [3], [34]. This is an important point of comparison for IIoT solutions due to the potential number of devices or sensors providing data.

The other facet of implementation important to this study was the use of software tools, frameworks, libraries, and languages. It was clear from the literature that Python is the most used programming language for implementing ML solutions to IIoT cybersecurity [2], [3], [33] and several of the libraries or frameworks used were Python based. In terms of software tools, Google Collaboratory was the only tool used by more than one paper [34], [45]. Not all papers specified their software tools, frameworks, libraries, or languages however, so it is difficult to determine what, if any impact these aspects of implementation may have on a model's performance.

These findings show that IIoT cybersecurity is an increasingly important field for research and development given the current concerns around increased attacks and potential consequences. The vast amount of potential ML techniques that are being utilized in this area suggest that there is a lot of work still to do in terms of finding the best approach for IIoT applications. The focus on techniques which preserve privacy such as federated learning are promising, as is the attention paid to accuracy and efficiency of solutions. These points of focus will ensure that models that are proposed will be more likely to be viable for real-world application. The findings of this review also show that there is more work to be done to narrow down those specific techniques and implementation factors that offer the best performance.

3.2.4. Limitations

This paper was limited in the number of papers selected for review as well as in its scope. Given these limitations, the paper was not able to completely represent or review the vast amount of research being conducted in this field, nor cover the range of impacting factors such as regulation and compliance concerns. These limitations also prevented more in-depth discussion of real-world applications of ML solutions and issues associated with this such as computational requirements and the comparison of used datasets to real-world cases. As discussed above, the evaluation metrics were not standard across reviewed papers, which hampered their comparison, however the use of a proven meta-analysis technique, along with additional analysis of results and used algorithms would have allowed for a more statistically accurate and in-depth analysis. More in-depth and standardized investigation of reviewed papers' methods and variables would have provided a more conclusive analysis as to model performance.

4. CONCLUSION

The current literature agrees that IIoT systems are being targeted more often by cyberattacks, and that the consequences of these attacks are of great concern. The vulnerability of IIoT devices and networks mean that solutions must be found to better protect these systems and data. As IIoT may process confidential data, privacy and encryption are also important considerations for cybersecurity solutions.

Of those ML techniques proposed in the current literature, the most common were FL, RF, CNN, LSTM and XGBoost, with the ML category of ANN being the most utilized type of ML technique. Given the varying combinations of techniques, it is difficult to determine which individual techniques are best suited to a ML solution. FL and supervised learning offer solutions to real world concerns of data privacy and largely unlabeled data, while FCNN, MLP and RF show improved results over other techniques. The difficulty of an IIoT environment is the potential number of devices. Several models found that processing and training time increased depending on devices, and so this is something to take into account when considering cybersecurity solutions.

This review concludes that there is no particular best ML solution to IIoT cybersecurity at present. Future reviews in this area could focus on comparing models that use the same core ML technique paired with different ensemble methods. This type of comparison could provide further insight into the impact of ensemble methods on the performance of specific ML techniques. Another focus for future reviews could be a comparison of the performance of different ML models against the same data set to better contrast the performance of specific techniques. However, one limitation of using created test data sets is that a model may then perform differently in a real-world scenario. Therefore, applying ML solutions in real-world conditions or scenarios could be another interesting direction for future research. In particular, examining models' ability to detect zero-day attacks would present a worthwhile avenue for research.

Two techniques in particular, semi-supervised learning and FL provide solutions to real world concerns of data privacy and large amounts of unlabeled data needing to be processed. These techniques could be considered for implementation in real-world solutions for IIoT cybersecurity. However, there are still drawbacks to these techniques. Semi-supervised learning does still require the use of some labelled data, which may or may not exist in a real world IIoT cybersecurity scenario. There can also be a high resource need in terms of power and time for model training, which IIoT devices may not have. Therefore, another direction for future research could be unsupervised learning, as well as experimenting with different combinations of methods to reduce the amount of processing power and time required for training.

The current literature is varied when it comes to ML techniques, datasets, and variables. Further examination of the impact of different variables on the performance of different ML algorithms could provide further insight into the performance of specific ML techniques. This could also help us to understand which factors are important in determining the best performance for a model or which variables may help to reduce processing times and resources. Similarly, the impact and performance of ensemble methods could be further reviewed, particularly gradient boosting methods. It is clear that there are many different areas of focus for future research and reviews which would provide deeper insights into the application of ML to IIoT cybersecurity.

Further reviews could provide a more extensive comparison of ML models in the area of IIoT cybersecurity or could focus more in depth on any particular aspect or ML technique within this review. For example, a more thorough examination of the impact of variable choice, software or tools, hardware choices or a focus on data privacy could be pursued in future reviews. Future reviews could also look at concrete examples of the implementation of machine learning solutions for a better examination of real-world results.

ACKNOWLEDGMENTS

The authors acknowledge the support from the Charles Sturt University for the facilities provided to carry out the research.

FUNDING INFORMATION

Authors state no conflict of interest.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the contributor roles taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Melanie Heier	✓	✓			✓	✓	✓	✓	✓	✓	✓		✓	
Penatiyana W. Chandana Prasad	✓									✓		✓		
Md Shohel Sayeed										✓				✓

C	:	**C**onceptualization	I	:	**I**nvestigation	Vi	:	**Vi**sualization
M	:	**M**ethodology	R	:	**R**esources	Su	:	**Su**pervision
So	:	**So**ftware	D	:	**D**ata Curation	P	:	**P**roject administration
Va	:	**Va**lidation	O	:	Writing - **O**riginal Draft	Fu	:	**Fu**nding acquisition
Fo	:	**Fo**rmal analysis	E	:	Writing - Review & **E**diting			

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

DATA AVAILABILITY

Data availability is not applicable to this paper as no new data were created or analyzed in this study.

REFERENCES

[1] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010, doi: 10.1016/j.comnet.2010.05.010.

[2] O. Aouedi, K. Piamrat, G. Muller, and K. Singh, "Federated semisupervised learning for attack detection in industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 1, pp. 286–295, Jan. 2023, doi: 10.1109/TII.2022.3156642.

[3] F. Khan, R. Alturki, M. A. Rahman, S. Mastorakis, I. Razzak, and S. T. Shah, "Trustworthy and reliable deep learning-based cyberattack detection in industrial IoT," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 1, pp. 1030–1038, Jan. 2023, doi: 10.1109/TII.2022.3190352.

[4] M. Serror, S. Hack, M. Henze, M. Schuba, and K. Wehrle, "Challenges and opportunities in securing the industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 5, pp. 2985–2996, May 2021, doi: 10.1109/TII.2020.3023507.

[5] Z. E. Huma *et al.*, "A hybrid deep random neural network for cyberattack detection in the industrial internet of things," *IEEE Access*, vol. 9, pp. 55595–55605, 2021, doi: 10.1109/ACCESS.2021.3071766.

[6] M. A. Ferrag, O. Friha, D. Hamouda, L. Maglaras, and H. Janicke, "Edge-IIoTset: A new comprehensive realistic cyber security dataset of IoT and IIoT applications for centralized and federated learning," *IEEE Access*, vol. 10, pp. 40281–40306, 2022, doi: 10.1109/ACCESS.2022.3165809.

[7] S. F. Tan and A. Samsudin, "Recent technologies, security countermeasure and ongoing challenges of industrial internet of things (IIoT): A survey," *Sensors*, vol. 21, no. 19, p. 6647, Oct. 2021, doi: 10.3390/s21196647.

[8] T. Gueye, A. Iqbal, Y. Wang, R. T. Mushtaq, and M. I. Petra, "Bridging the cybersecurity gap: A comprehensive analysis of threats to power systems, water storage, and gas network industrial control and automation systems," *Electronics*, vol. 13, no. 5, p. 837, Feb. 2024, doi: 10.3390/electronics13050837.

[9] P. Priller, A. Aldrian, and T. Ebner, "Case study: From legacy to connectivity migrating industrial devices into the world of smart services," in *Proceedings of the 2014 IEEE Emerging Technology and Factory Automation (ETFA)*, Sep. 2014, pp. 1–8, doi: 10.1109/ETFA.2014.7005136.

[10] N. Mishra and S. Pandya, "Internet of things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review," *IEEE Access*, vol. 9, pp. 59353–59377, 2021, doi: 10.1109/ACCESS.2021.3073408.

[11] O. K. Sahingoz, E. Buber, O. Demir, and B. Diri, "Machine learning based phishing detection from URLs," *Expert Systems with Applications*, vol. 117, pp. 345–357, Mar. 2019, doi: 10.1016/j.eswa.2018.09.029.

[12] A. Alsaedi, N. Moustafa, Z. Tari, A. Mahmood, and A. Anwar, "TON_IoT telemetry dataset: A new generation dataset of IoT and IIoT for data-driven intrusion detection systems," *IEEE Access*, vol. 8, pp. 165130–165150, 2020, doi: 10.1109/ACCESS.2020.3022862.

[13] A. Diro, N. Chilamkurti, V.-D. Nguyen, and W. Heyne, "A comprehensive study of anomoly detection schemes in IoT networks using machine learning algorithms," *Sensors*, vol. 21, no. 24, p. 8320, Dec. 2021, doi: 10.3390/s21248320.

[14] S. Ruiz-Villafranca, J. Roldán-Gómez, J. M. C. Gómez, J. Carrillo-Mondéjar, and J. L. Martinez, "A TabPFN-based intrusion detection system for the industrial internet of things," *The Journal of Supercomputing*, vol. 80, no. 14, pp. 20080–20117, Sep. 2024, doi: 10.1007/s11227-024-06166-x.

[15] W. G. Hatcher and W. Yu, "A survey of deep learning: platforms, applications and emerging research trends," *IEEE Access*, vol. 6, pp. 24411–24432, 2018, doi: 10.1109/ACCESS.2018.2830661.

[16] A. Houkan *et al.*, "Enhancing security in industrial IoT networks: machine learning solutions for feature selection and reduction," *IEEE Access*, vol. 12, pp. 160864–160883, 2024, doi: 10.1109/ACCESS.2024.3481459.

[17] R. Rudenko, I. M. Pires, P. Oliveira, J. Barroso, and A. Reis, "A brief review on internet of things, industry 4.0 and cybersecurity," *Electronics*, vol. 11, no. 11, p. 1742, May 2022, doi: 10.3390/electronics11111742.

[18] J. Yu, A. V. Shvetsov, and S. Hamood Alsamhi, "Leveraging machine learning for cybersecurity resilience in industry 4.0: challenges and future directions," *IEEE Access*, vol. 12, pp. 159579–159596, 2024, doi: 10.1109/ACCESS.2024.3482987.

[19] N. Moustafa, "A new distributed architecture for evaluating AI-based security systems at the edge: Network TON_IoT datasets," *Sustainable Cities and Society*, vol. 72, 2021, doi: 10.1016/j.scs.2021.102994.

[20] M. Mudassir, D. Unal, M. Hammoudeh, and F. Azzedin, "Detection of botnet attacks against industrial IoT systems by multilayer deep learning approaches," *Wireless Communications and Mobile Computing*, vol. 2022, pp. 1–12, May 2022, doi: 10.1155/2022/2845446.

[21] A. E. Elhabashy, L. J. Wells, and J. A. Camelio, "Cyber-physical security research efforts in manufacturing – a literature review," *Procedia Manufacturing*, vol. 34, pp. 921–931, 2019, doi: 10.1016/j.promfg.2019.06.115.

[22] U. Tariq, "Combatting ransomware in ZephyrOS-activated industrial IoT environments," *Heliyon*, vol. 10, no. 9, p. e29917, May 2024, doi: 10.1016/j.heliyon.2024.e29917.

[23] M. Zolanvari, M. A. Teixeira, L. Gupta, K. M. Khan, and R. Jain, "Machine learning-based network vulnerability analysis of industrial internet of things," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6822–6834, Aug. 2019, doi: 10.1109/JIOT.2019.2912022.

[24] M. S. Mahmoud, M. M. Hamdan, and U. A. Baroudi, "Modeling and control of cyber-physical systems subject to cyber attacks: A survey of recent advances and challenges," *Neurocomputing*, vol. 338, pp. 101–115, Apr. 2019, doi: 10.1016/j.neucom.2019.01.099.

[25] A. Angelopoulos *et al.*, "Tackling faults in the industry 4.0 era – a survey of machine-learning solutions and key aspects," *Sensors*, vol. 20, no. 1, p. 109, Dec. 2019, doi: 10.3390/s20010109.

[26] M. Abdel-Basset, V. Chang, H. Hawash, R. K. Chakrabortty, and M. Ryan, "Deep learning approaches for human-centered IoT applications in smart indoor environments: a contemporary survey," *Annals of Operations Research*, vol. 339, no. 1–2, pp. 3–51, Aug. 2024, doi: 10.1007/s10479-021-04164-3.

[27] H. Hanif, M. H. N. Md Nasir, M. F. Ab Razak, A. Firdaus, and N. B. Anuar, "The rise of software vulnerability: Taxonomy of

software vulnerabilities detection and machine learning approaches," *Journal of Network and Computer Applications*, vol. 179, p. 103009, Apr. 2021, doi: 10.1016/j.jnca.2021.103009.

[28] L. Fu, W. Zhang, X. Tan, and H. Zhu, "An algorithm for detection of traffic attribute exceptions based on cluster algorithm in industrial internet of things," *IEEE Access*, vol. 9, pp. 53370–53378, 2021, doi: 10.1109/ACCESS.2021.3068756.

[29] M. Shahin, F. F. Chen, H. Bouzary, A. Hosseinzadeh, and R. Rashidifar, "A novel fully convolutional neural network approach for detection and classification of attacks on industrial IoT devices in smart manufacturing systems," *The International Journal of Advanced Manufacturing Technology*, vol. 123, no. 5–6, pp. 2017–2029, Nov. 2022, doi: 10.1007/s00170-022-10259-3.

[30] M. Shahin, F. F. Chen, A. Hosseinzadeh, H. Bouzary, and R. Rashidifar, "A deep hybrid learning model for detection of cyber attacks in industrial IoT devices," *The International Journal of Advanced Manufacturing Technology*, vol. 123, no. 5–6, pp. 1973–1983, Nov. 2022, doi: 10.1007/s00170-022-10329-6.

[31] M.-Q. Tran, M. Elsisi, K. Mahmoud, M.-K. Liu, M. Lehtonen, and M. M. F. Darwish, "Experimental setup for online fault diagnosis of induction machines via promising IoT and machine learning: towards industry 4.0 empowerment," *IEEE Access*, vol. 9, pp. 115429–115441, 2021, doi: 10.1109/ACCESS.2021.3105297.

[32] S. Chakraborty, A. Onuchowska, S. Samtani, W. Jank, and B. Wolfram, "Machine learning for automated industrial IoT attack detection: an efficiency-complexity trade-off," *ACM Transactions on Management Information Systems*, vol. 12, no. 4, pp. 1–28, Dec. 2021, doi: 10.1145/3460822.

[33] B. Li, Y. Wu, J. Song, R. Lu, T. Li, and L. Zhao, "DeepFed: Federated deep learning for intrusion detection in industrial cyber-physical systems," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 8, pp. 5615–5624, Aug. 2021, doi: 10.1109/TII.2020.3023430.

[34] A. Makkar, T. W. Kim, A. K. Singh, J. Kang, and J. H. Park, "SecureIIoT environment: Federated learning empowered approach for securing IIoT from data breach," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 9, pp. 6406–6414, Sep. 2022, doi: 10.1109/TII.2022.3149902.

[35] D. Preuveneers, V. Rimmer, I. Tsingenopoulos, J. Spooren, W. Joosen, and E. Ilie-Zudor, "Chained anomaly detection models for federated learning: An intrusion detection case study," *Applied Sciences*, vol. 8, no. 12, p. 2663, Dec. 2018, doi: 10.3390/app8122663.

[36] S. Taheri, M. Davoodi, and M. Ali, "Mitigating cyber anomalies in virtual power plants using artificial-neural-network-based secondary control with a federated learning-trust adaption," *Energies*, vol. 17, no. 3, p. 619, Jan. 2024, doi: 10.3390/en17030619.

[37] Y. Lu, X. Huang, Y. Dai, S. Maharjan, and Y. Zhang, "Blockchain and federated learning for privacy-preserved data sharing in industrial IoT," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4177–4186, Jun. 2020, doi: 10.1109/TII.2019.2942190.

[38] J. O. Odeh, X. Yang, C. I. Nwakanma, and S. Dhelim, "Asynchronous privacy-preservation federated learning method for mobile edge network in industrial internet of things ecosystem," *Electronics*, vol. 13, no. 9, p. 1610, Apr. 2024, doi: 10.3390/electronics13091610.

[39] S. S. Sefati, R. Craciunescu, B. Arasteh, S. Halunga, O. Fratu, and I. Tal, "Cybersecurity in a scalable smart city framework using Blockchain and federated learning for internet of things (IoT)," *Smart Cities*, vol. 7, no. 5, pp. 2802–2841, Oct. 2024, doi: 10.3390/smartcities7050109.

[40] X. Liu, X. Dong, N. Jia, and W. Zhao, "Federated learning-oriented computing framework for the IIoT," *Sensors*, vol. 24, no. 13, p. 4182, Jun. 2024, doi: 10.3390/s24134182.

[41] P. Dini, L. Diana, A. Elhanashi, and S. Saponara, "Overview of AI-models and tools in embedded IIoT applications," *Electronics*, vol. 13, no. 12, p. 2322, Jun. 2024, doi: 10.3390/electronics13122322.

[42] M. Wu, Z. Song, and Y. B. Moon, "Detecting cyber-physical attacks in CyberManufacturing systems with machine learning methods," *Journal of Intelligent Manufacturing*, vol. 30, no. 3, pp. 1111–1123, Mar. 2019, doi: 10.1007/s10845-017-1315-5.

[43] D. Svozil, V. Kvasnicka, and J. Pospichal, "Introduction to multi-layer feed-forward neural networks," *Chemometrics and Intelligent Laboratory Systems*, vol. 39, no. 1, pp. 43–62, Nov. 1997, doi: 10.1016/S0169-7439(97)00061-0.

[44] X. Zhou, J. Feng, and Y. Li, "Non-intrusive load decomposition based on CNN–LSTM hybrid deep learning model," *Energy Reports*, vol. 7, pp. 5762–5771, Nov. 2021, doi: 10.1016/j.egyr.2021.09.001.

[45] W. Jiang, "Machine learning methods to detect voltage Glitch attacks on IoT/IIoT infrastructures," *Computational Intelligence and Neuroscience*, vol. 2022, 2022, doi: 10.1155/2022/6044071.

[46] V. A. Memos, K. E. Psannis, and Z. Lv, "A secure network model against bot attacks in edge-enabled industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 11, pp. 7998–8006, Nov. 2022, doi: 10.1109/TII.2022.3162837.

[47] D. Gibert, C. Mateu, J. Planes, and R. Vicens, "Using convolutional neural networks for classification of malware represented as images," *Journal of Computer Virology and Hacking Techniques*, vol. 15, no. 1, pp. 15–28, Mar. 2019, doi: 10.1007/s11416-018-0323-0.

[48] F. Karim, S. Majumdar, and H. Darabi, "Insights into LSTM Fully convolutional networks for time series classification," *IEEE Access*, vol. 7, pp. 67718–67725, 2019, doi: 10.1109/ACCESS.2019.2916828.

[49] Z. Wang, W. Yan, and T. Oates, "Time series classification from scratch with deep neural networks: A strong baseline," in *2017 International Joint Conference on Neural Networks (IJCNN)*, May 2017, pp. 1578–1585, doi: 10.1109/IJCNN.2017.7966039.

[50] E. Park, X. Cui, T. H. B. Nguyen, and H. Kim, "Presentation attack detection using a tiny fully convolutional network," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 11, pp. 3016–3025, 2019, doi: 10.1109/TIFS.2019.2907184.

[51] Y. Yin, "Deep learning with the random neural network and its applications," *arXiv preprint arXiv:1810.08653*, 2018.

[52] M. M. Hassan, A. Gumaei, A. Alsanad, M. Alrubaian, and G. Fortino, "A hybrid deep learning model for efficient intrusion detection in big data environment," *Information Sciences*, vol. 513, pp. 386–396, Mar. 2020, doi: 10.1016/j.ins.2019.10.069.

[53] T. D. Nguyen, S. Marchal, M. Miettinen, H. Fereidooni, N. Asokan, and A.-R. Sadeghi, "DÏoT: A federated self-learning anomaly detection system for IoT," in *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*, Jul. 2019, pp. 756–767, doi: 10.1109/ICDCS.2019.00080.

[54] Y. Zhao, L. Yang, B. Lehman, J.-F. de Palma, J. Mosesian, and R. Lyons, "Decision tree-based fault detection and classification in solar photovoltaic arrays," in *2012 Twenty-Seventh Annual IEEE Applied Power Electronics Conference and Exposition (APEC)*, Feb. 2012, pp. 93–99, doi: 10.1109/APEC.2012.6165803.

[55] R. Benkercha and S. Moulahoum, "Fault detection and diagnosis based on C4.5 decision tree algorithm for grid connected PV system," *Solar Energy*, vol. 173, pp. 610–634, Oct. 2018, doi: 10.1016/j.solener.2018.07.089.

[56] M. Hasan, M. M. Islam, M. I. I. Zarif, and M. M. A. Hashem, "Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches," *Internet of Things*, vol. 7, p. 100059, Sep. 2019, doi: 10.1016/j.iot.2019.100059.

[57] N. Farnaaz and M. A. Jabbar, "Random forest modeling for network intrusion detection system," *Procedia Computer Science*, vol. 89, pp. 213–217, 2016, doi: 10.1016/j.procs.2016.06.047.

[58] D. Rani, N. S. Gill, P. Gulia, and J. M. Chatterjee, “An ensemble-based multiclassifier for intrusion detection using internet of things,” *Computational Intelligence and Neuroscience*, vol. 2022, pp. 1–16, May 2022, doi: 10.1155/2022/1668676.

[59] R. Avnimelech and N. Intrator, “Boosted mixture of experts: an ensemble learning scheme,” *Neural Computation*, vol. 11, no. 2, pp. 483–497, Feb. 1999, doi: 10.1162/089976699300016737.

[60] J. Friedman, T. Hastie, and R. Tibshirani, “Additive logistic regression: a statistical view of boosting (With discussion and a rejoinder by the authors),” *The Annals of Statistics*, vol. 28, no. 2, Apr. 2000, doi: 10.1214/aos/1016218223.

[61] J. H. Friedman, “Greedy function approximation: A gradient boosting machine,” *The Annals of Statistics*, vol. 29, no. 5, Oct. 2001, doi: 10.1214/aos/1013203451.

[62] T. Chen and C. Guestrin, “Xgboost: A scalable tree boosting system,” in *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, Aug. 2016, pp. 785–794, doi: 10.1145/2939672.2939785.

[63] K. Hara and K. Shiomoto, “Intrusion detection system using semi-supervised learning with adversarial auto-encoder,” in *NOMS 2020 - 2020 IEEE/IFIP Network Operations and Management Symposium*, Apr. 2020, pp. 1–8, doi: 10.1109/NOMS47738.2020.9110343.

[64] T. M. Booij, I. Chiscop, E. Meeuwissen, N. Moustafa, and F. T. H. den Hartog, “ToN_IoT: The role of heterogeneity and the need for standardization of features and attack types in IoT network intrusion data sets,” *IEEE Internet of Things Journal*, vol. 9, no. 1, pp. 485–496, Jan. 2022, doi: 10.1109/JIOT.2021.3085194.

[65] Deakin University, “Systematic and systematic-like review toolkit,” *Deakin University*, 2023. https://deakin.libguides.com/systematicreview/step1 (accessed Dec. 17, 2022).

APPENDIX

Abbreviations:

AdaBoost	Adaptive boosting	LM	Lateral movement
AE	Autoencoder	LSTM	Long short-term memory
ALSTM	Attention-based long short-term memory	MC	Malicious control
C&C	Command and control	MCC	Matthew's correlation coefficient
CA	Clustering algorithm	MFCI	Malicious function command injection
CMRI	Complex malicious response injection	MITM	Man-in-the-Middle
CNN	Convolutional neural network	ML	Machine learning
CR	Communication rounds	MLP	Multi-layer perceptron
DDoS	Distributed denial of service	MO	Malicious operations
DL	Deep learning	MPCI	Malicious parameter command injection
DoS	Denial of service	MSCI	Malicious state command injection
DT	Decision tree	MS-MPA	Multi stage, multi point attack
DTP	Data type probing	MS-SPA	Multi stage, single point attack
EL	Ensemble learning	NMRI	Naïve malicious response injection
ELM	Extreme learning machine	ORF	Outer ring fault
FCN	Fully connected network	PRU	Pyramidal recurrent unit
FCNN	Fully convolutional neural network	RaNN	Random neural network
FL	Federated learning	Recon.	Reconnaissance
FN	False negative	RF	Random forest
FNR	False negative rate	SSL	Semi supervised learning
FP	False positive	SS-MPA	Single stage, multi point attack
FPCA	Functional principal component analysis	SS-SPA	Single stage, single point attack
FPR	False positive rate	SVM	Support vector machine
FSA	Functional shape analysis	SW	Software
FW	Framework	SWaT	Secure water treatment
GRU	Gated recurrent unit	TN	True negative
HCA	Heuristic clustering algorithm	TNR	True negative rate
INFI	Infiltration of network from Inside	TP	True positive
IRF	Inner ring fault	TPR	True positive rate
k-NN	K-nearest neighbour	UtR	User to root
Langs.	Languages	WS	Wrong setup
LG	Logistic regression	XGBoost	Extreme gradient boosting
Libs.	Libraries	XSS	Cross site scripting

BIOGRAPHIES OF AUTHORS

Melanie Heier is a recent graduate of Charles Sturt University, Australia. She has no prior publications. This report was completed as the final project of her Master of Information Technology degree and adapted for publication. The combination of machine learning techniques with cybersecurity provided a topic within the realms of both master’s specializations: cybersecurity, and software design and development. Melanie now works within a software development role. She can be contacted at email: melheier@gmail.com.

Penatiyana W. Chandana Prasad is an associate professor with the School of Computing and Mathematics at Charles Sturt University, Australia and also an adjunct associate professor at Duy Tan University, Vietnam. Prior to this, he was a lecturer at the United Arab Emirates University in UAE, Multimedia University in Malaysia, and the Informatics Institute of Technology (IIT), Sri Lanka. He gained his undergraduate and postgraduate degrees from St Petersburg State Electrotechnical University in the early 90s and completed his PhD studies at the Multimedia University in Malaysia. He is an active researcher in the areas of computer architecture, digital systems, and modeling and simulation”. He has published more than 260 research articles in computing and engineering journals and conference proceedings. He has co-authored two books entitled ‘Digital Systems Fundamentals and Computer Systems Organization and Architecture’ published by Prentice Hall. He is a senior member of the IEEE Computer Society. He can be contacted at email: chandana.withana@duytan.edu.vn.

Md Shohel Sayeed has been a member of Multimedia University since 2001 and now he serves as a professor of the Faculty of Information Science and Technology. Dr. Shohel’s core research interest is in the area of biometrics, information security, image and signal processing, pattern recognition and classification. Till date, he has published over 100 research papers in international peer-reviewed journals and international conference proceedings as a result of his research work. His research works have been accepted by journals such as IEEE Transactions on Pattern Analysis and Machine Intelligence (TPAMI), International Journal of Pattern Recognition and Artificial Intelligence (IJPRI), Discrete Dynamics in Nature and Society (DDNS). He has been appointed technical paper reviewer for Journal of Pattern Recognition Letters, IEEE Transaction on Neural Networks, IEEE Transactions on Automation Science and Engineering, Journal of Computer Methods and Programs in Biomedicine and International Journal of Computer Theory and Engineering. He has also been invited to review technical papers for several international conferences. In recognition of his professional contribution, he has obtained recognition as a Senior member of IEEE Computer Society, IEEE Communication Society and International Association of Computer Science and Information Technology (IACSIT). He can be contacted at email: shohel.sayeed@mmu.edu.my.