Application of Machine Learning Techniques in Anomaly Detection

Lai Kai Lok
School of Computing
Asia Pacific University
Kuala Lumpur, Malaysia
tp061241@mail.apu.edu.my

Chandra Reka Ramachandiran
School of Computing
Asia Pacific University
Kuala Lumpur, Malaysia
chandra.reka@apu.edu.my

Vazeerudeen Abdul Hameed
School of Computing
Asia Pacific University
Kuala Lumpur, Malaysia
vazeer@apu.edu.my

***Abstract*—Machine learning has made tremendous improvement in terms of performance recently due to the advancement of technology and reduction in cost. This paper aims to review the application of various machine learning techniques for anomaly detection in the domain of manufacturing, finance and internet security. Abnormal activities in these domains have caused huge financial loss and the current methods used are not effective enough. In the manufacturing domain, anomaly can be in the form of abnormal activity during the production process or defects on the end product. Credit card fraud is the common anomaly in the finance domain. Cyberattack is the anomaly that needs to be addressed in the internet security domain. Various studies suggested that Random Forest is the most suitable candidate choice for anomaly detection compared with other supervised machine learning methods. Unsupervised clustering methods are performing better than supervised learning methods in detecting unseen types of anomalies. Although deep learning is showing promising results and can work well with raw data, it needs longer training time and more computational power. Hybrid methods are outperforming other techniques as each method in the modal is designed to synergize each other strengths.**

Keywords—machine learning, anomaly detection, smart-manufacturing, credit card fraud, internet security

I. INTRODUCTION

In the real world situation, there are always some instances which show abnormal characteristics from the majority samples. These unusual instances are known as anomalies. Precious and important information can usually be extracted from these anomalies. This is due to the fact that those irregular properties are the results of certain events such as system malfunction, cyber-attack and fraud transaction [1]. In Figure 1, the anomalies are labelled as O while the majority normal data are covered within the region N. Most of the data in our world have more than 3 features and it is hard to visualize it in 3 dimensional plot. Thus, it is impossible for humans to detect these anomalies without the help of computers. Machine learning is a good candidate for solving this issue as it is good at finding patterns from complex datasets. Furthermore, the advancement of computational power with lower cost and the rising availability of data are creating a perfect environment for deploying machine learning [2].

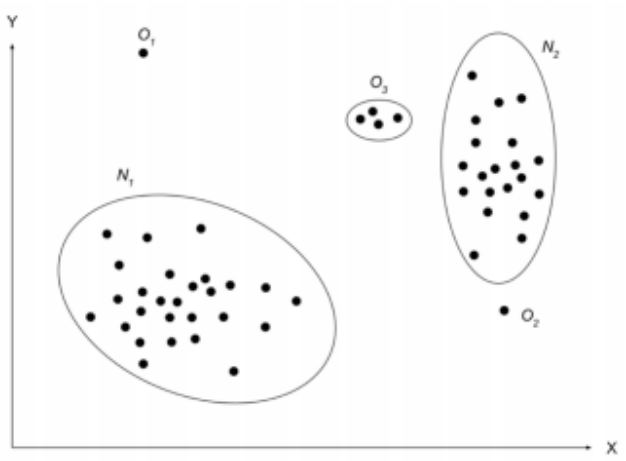

Fig. 1. Anomalies illustrated in 2 dimensional plot [1].

There are three types of anomaly [3]. The first type is point anomaly, the simplest form of anomaly, where a single data point is abnormal compared with other data. As an example in the microchip processor, by just considering one feature to simplify the condition, if the temperature of the chip is much higher than the normal range, then that point is considered as an anomaly. Contextual anomaly is the second type of anomaly. It is also known as conditional anomaly, where a data point is only considered as an anomaly in certain conditions or specific contexts. In other situations, this data point is treated as normal. For example, the high temperature of the chip is only considered as an anomaly if no intensive task is assigned to it. If the high temperature of the chip is associated with carrying out intensive tasks, it is treated as normal. The final type of anomaly is the collective anomaly. This type of anomaly only considers a collection of data points as abnormal compared to the whole dataset, while the individual data point in the collection is treated as normal. For instance, if the high temperature of the chip is occurring for a long period of time, it is treated as an anomaly while single instance of high temperature is considered normal.

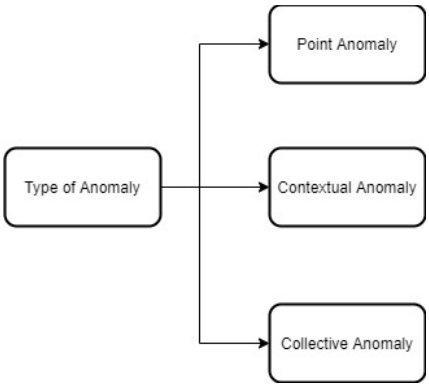

Fig. 2. Type of anomalies.

In the manufacturing domain, anomaly detection can help in preventing accidents from occurring and improve the production efficiency [4]. Credit card fraud detection in the finance sector, which is a form of anomaly detection can reduce the financial loss and create confidence among users [5]. Internet intrusion detection is crucial in ensuring the security and privacy of users are being protected. Besides, cyber-attack on important systems like the military or healthcare infrastructure can lead to dreadful consequences [6]. The main purpose of this paper is to review the research progress in machine learning based anomaly detection, particularly in the domain of manufacturing, finance and internet security.

One of the main challenges in anomaly detection is the difficulty in defining the decision boundary between normal and abnormal samples. The continuously evolving characteristics of the data add another layer of difficulty in defining the boundary [1]. Another challenge is the class imbalance problem, where the anomaly instances are way lesser than the normal samples [7]. This will create a machine learning model which is biased to the normal class during the classification training. Besides, it is difficult to differentiate between noisy data and anomaly data and result in too many false positive instances. Many machine learning algorithms failed to provide information about the root cause or the location of the anomaly even though they can perform well in detecting them [2, 8].

In Section II, various types of machine learning techniques are reviewed. Section III describes current research work regarding anomaly detection in the three main domains by using machine learning techniques. The conclusion and future research are discussed in the final Section.

II. Machine Learning Techniques

A. Decision Tree (DT)

It is a simple and fast predictive model for solving classification problems. Significant features from the dataset are used as the decision nodes to decide the class of the target variable, represented by the leaves in the decision tree. Figure 3 illustrated an example of a decision tree. In each node, there is an if-else rule which splits the data into two branches. A node with higher order implies that it has a better predictor capacity. The splitting process in each node acts as a decision boundary for one dimension feature [4].

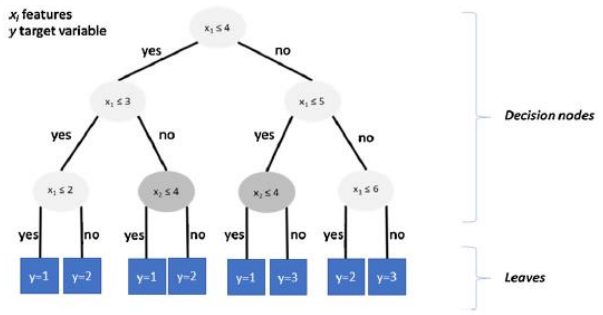

Fig. 3. Illustration of Decision Tree [4].

B. Logistic Regression (LR)

It is a conditional model which calculates the probability of a data point belonging to a class by fitting in all the features into a logistic curve [9]. The threshold probability is usually set as 0.5, where any samples that have probability of more than the threshold value is considered to belong to the same class, else the sample is treated as other classes. Given features X, weights W, bias b and classes C, the probability of a sample belonging to a class is calculated by using equation (1) [10].

$$P(y = C|X; W, b) = \frac{1}{1+exp^{-WX-b}} \quad (1)$$

C. Support Vector Machine (SVM)

As most of the dataset contains more than 3 features, it is difficult to analyse them using the current space. To solve this issue, SVM transforms these features into different domains or spaces, where it is easier to linearly classify the sample into its respective classes. Few data points are selected as support vectors and SVM's main objective is to maximize the margin or distance between the support vectors and the boundary. The boundary is formed by only using a small set of data, the support vectors, but it is able to classify for a much larger set of data. One Class SVM (OCSVM) is a special type of SVM which is commonly used for anomaly detection. In OCSVM, only the normal dataset is used in training and forms the boundary. Any sample which falls outside the boundary is considered as an anomaly [11].

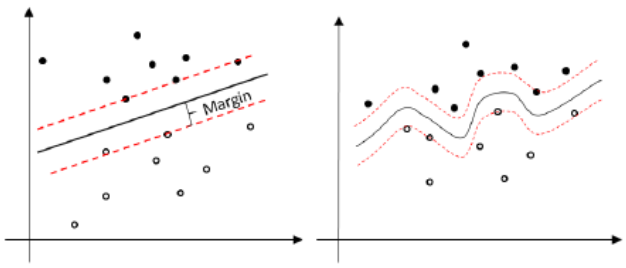

Fig. 4. Example of linear SVM (left) and non-linear SVM (right) [11].

D. Ensemble Learning

In supervised machine learning, different techniques can be used to tackle the same problem. As each technique has different properties, the best model can only be known after conducting experiments on every single model. Ensemble learning combines several models so that the disadvantages of a model can be compensated by other models, at the same time ensuring diversity in the results. Bagging, boosting and

stacking are the examples of techniques used in ensemble learning [12]. Decision Jungle and Random Forest (RF) are the two examples of ensemble learning used for classification [4].

E. Artificial Neural Network (ANN)

ANN mimics the way biological neurons function in the brain. There are three type of layer in ANN, which are the input layer, hidden layer and the output layer as shown in Figure 5. The input layer contains all the features in the dataset while the output layer shows the probability of the samples belonging to each class. Multilayer perceptron or feed-forward neural network is the simplest ANN model where the information in each node can only pass in one direction, from the input layer to the output layer. There is an activation in each node, which adds in nonlinearity into the features and helps in determining the target variable [13]. Sigmoid and RELU are examples of activation functions.

Backpropagation ANN are more widely used in the current research. In backpropagation ANN, the training goes through forward propagation to get the predicted output. After getting the differences between the desired output and the predicted output, it will go through the backpropagation process and readjust the weights of the network to reduce the error. ANN have a huge number of parameters for tuning and take longer time for optimization. It is also the backbone for deep learning algorithms like Recurrent Neural Network (RNN) and Convolutional Neural Network (CNN) [10].

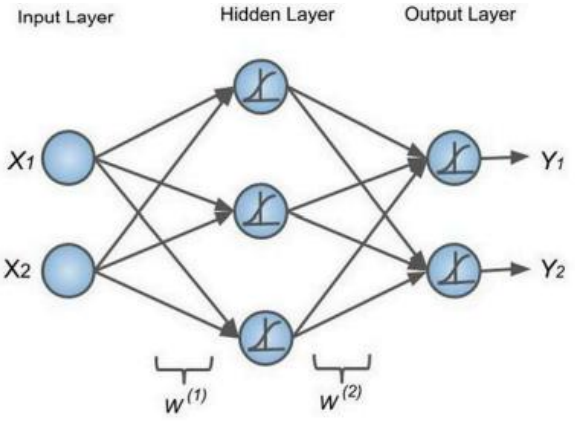

Fig. 5. Basic ANN model [13].

F. Clustering Methods

K-Nearest Neighbour (KNN) is one of the early clustering methods which uses the distance between the data point and a certain number of clusters within the train dataset for classification [7]. KNN is a supervised machine learning method widely used for classification. The K defines the number of clusters from the training set used to calculate the distance. The sample point is classified into the class where the distance is the shortest. There are five different types of distance used in KNN, which are the Euclidean distance, Hamming distance, Manhattan distance, Minkowski distance and instance-based. The computational time is shorter as this is a relatively simple algorithm [14].

K-means algorithm is an unsupervised clustering method which is simple and effective. K here refers to the number of clusters desired in the dataset, which have to be defined at the beginning. Then, K numbers of initial seeds are randomly set and all the other data points are clustered with respect to the nearest seeds. Next, the centroid of the clusters is calculated and acts as the new seeds. The steps of assigning each sample to its cluster and calculate the new centroid as the new seeds are repeated until they converge [14].

G. Hybrid

Novel methods where new ideas or concepts are added into the existing model to improve its performance. In [15], a high performance framework which applies combined feature learning and stacked de-noising auto-encoders for network anomaly detection is showing promising results. In other work [16], a multi-steps prediction was incorporated into the RNN to solve the continuously changing environment of online anomaly detection. In another approach to address the continual learning issue in the surveillance video, a method which combined the statistical module and transfer learning module was proposed [17]. To provide better predictive maintenance for trains, a system which combines the knowledge driven methods which make decisions based on the expert knowledge and data driven techniques which are mainly machine learning methods is developed [8].

III. Anomaly Detection

In this section, the application of machine learning techniques in the domain of manufacturing, finance and internet security are discussed. In each domain, a brief overview of the anomaly is presented followed by current research done on these anomaly detection.

A. Manufacturing

In this domain, anomaly detection can be in the form of detecting any unusual activity during the production process or checking the quality of the end product. Accurate anomaly detection can improve the performance of predictive maintenance which leads to reduction of the unexpected machine downtime and prevention of accidents while improving the profit [4].

As the production process is mainly monitored by using sensors, Verner and Mukherjee [18] proposed a long short-term memory (LSTM) based method to recognise abnormal reading in the sensors. The proposed method is able to achieve the same level of performance by just using raw data, compared with other machine learning methods which use specific features created by domain experts. However, more experiments need to be done by using other sensory data to confirm its efficiency. In [19], an unsupervised LSTM-based Autoencoder is developed for real-time anomaly detection in a production line which has three different chambers. The model is first trained by using data from one of the chambers then transfer learning is applied to shorten the training time for other chambers. After learning the time-based features of normal data, the model will label any data which has error larger than the threshold as anomaly. The model performed the best compared with other benchmark methods.

A metadata-driven multi-task transfer learning (M-MTL) method is developed for checking the quality of solder paste on circuit board [20]. This method combines isolation forest, k-means clustering and transfer learning to ensure the performance of different targeted tasks. This is needed as the quality of solder paste is decreasing due to the same inspection being applied on various types of circuit board. The proposed method is able to decrease 81.28% of false abnormal boards and is estimated to save $11.3 million per year. In another

study [21] which focuses on using unsupervised methods for checking the solder paste quality, generative adversarial networks (GAN) is proposed and it showed best performance among other unsupervised methods.

Similar to the case where one inspection machine needs to check the quality of solder paste on different circuit boards, it is common in industry that one machine is responsible for different production stages. Thus, a two steps real-time process anomaly detection is proposed to solve the issue of context changing within the same machine [4]. The first step is to identify the stage of the production process by implementing expert knowledge while the second step is to detect anomalies based on the identified context by using machine learning techniques. It is affirmed that RF is a good candidate for anomaly detection.

Various machine learning techniques are applied for detecting faults in the synthesis loop of an ammonia plant for unscheduled shutdown prevention [22]. Random forest showed the best performance in detecting faults. Further work can be done by incorporating the predictive maintenance into the system, using normal and abnormal as training sets.

B. Finance

In this domain, credit card fraud detection will be the main focus. Few types of credit card fraud are listed in Table I.

TABLE I. TYPE OF CREDIT CARD FRAUD [23]

Type	***Descriptions***
Theft / Stolen	Simplest and shortest detection time
Application	Use false information during application process
Bankruptcy	Spending without the ability of paying back
Internal	Illegal use by bank employee
Counterfeit	Transactions made without the consent of cardholder, hardest to detect

Eight machine learning techniques are compared and resampling techniques are applied to solve the class imbalance issue for the credit card fraud detection [23]. It is concluded that the resembling technique is ineffective as the number of false alarms is rising while a significant number of true positives remain undetected. Contradict to this study, Baabdullah et al [24] concluded that machine learning algorithm with resampling techniques is able to solve the class imbalanced problem and reduce the false positive. However, both studies are using different dataset, where [23] only has 8 features in the dataset compared with 31 features in [24]. This clearly shows that the type of data has a huge impact on the result obtained.

The performance of ensemble learning and other types of supervised machine learning methods are compared. Stacking type of ensemble learning showed the best overall performance [25]. A three stage model is proposed to handle the concept drift issue of credit card fraud detection [26]. The first step is to categorize cardholders into different spending amount groups, followed by machine learning classification. The final stage is to update the cardholder spending behaviour with non-fraud transactions.

In [27], a hybrid model which consists of Support Vector Machine Recursive Feature Elimination for best feature extraction and RF is proposed for detecting credit card fraud. Resampling using SMOTE and hyper parameter optimization is done on RF to improve the model's performance. The hybrid method performed the best compared with 7 other conventional machine learning techniques.

A deep neural network model with 3 hidden dense layers is constructed for credit card fraud detection [28]. This model showed better performance compared with Naïve Bayes (NB), LR and SVM. On the other hand, Nadim et al [29] focus on comparing conventional machine learning techniques to find out the algorithm which gives the best business value, excluding the deep learning method. After experimenting with 7 models, RF and XGB showed the best balance between accuracy and cost effective.

To solve the issue where supervised learning is unable to detect unseen types of credit card fraud, k-means clustering method is used to assign a consistency score to the samples. Any sample that has value less than the threshold consistency score is considered as an anomaly [30]. The proposed method is compared with isolation forest and showed better performance in terms of Area Under Precision-Recall Curve (AUPRC). It is claimed that AUPRC is more accurate in accessing the performance of imbalance dataset compared to Area Under Receiver Operating Characteristic Curve (AUROC).

C. Internet Security

The main anomaly detection in this domain is to recognise the pattern of cyber-attack. The examples of the cyberattack are denial of service, data type probing, malicious control, malicious operation, scan, spying and wrong setup [31].

Hassan et al [10] applied various supervised machine learning techniques for detecting cyberattack on the Internet of Things (IoT) network. The flow of the experiment is shown in Figure 6. Most of the conventional machine learning techniques are having similar flow with slight variation. This work suggested that RF is the most suitable technique in detecting cyberattack for the dataset in the experiment.

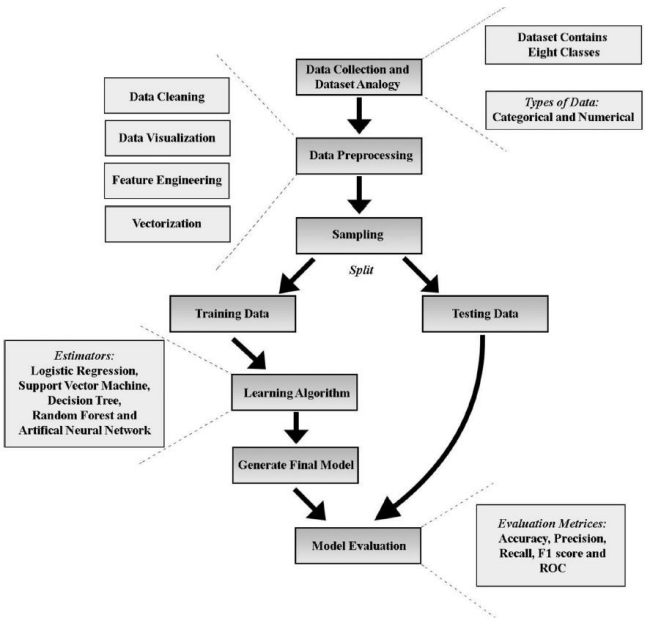

Fig. 6. The flow of conventional machine learning techniques [10].

Comparison between Deep Neural Network (DNN) and one class SVM is done by using the Swat dataset [32]. DNN has better performance by showing less false alarm while one class SVM is able to recognize slightly more anomalies. However, DNN is taking a lot more time for training. Working on the same SWaT dataset, Kravchik and Shabtai [33] showed that the 1D CNN model performed better while using shorter run time compared with LSTM and RNN model for detecting cyber-attack in the industrial control systems. This is contradict with the notion that RCC is the best method in solving sequence and series data, suggested by other researches [34], [35].

Bhatia et al [36] showed that unsupervised classifiers based on Autoencoder and PCA can perform a lot better than supervised machine learning methods in detecting new and unfamiliar attacks in the industrial network.

A vector convolutional deep learning model which consists of the vector convolutional network for feature extraction and fully connected network for feature learning is developed to detect abnormal activity in IoT devices [37]. This study used fog nodes for load distribution to solve the non-scalable issue.

An intelligent optimization method, the probability-based mutation dandelion algorithm is applied to improve the performance of Weighted Extreme Learning Machine (WELM) for solving problems with imbalanced class [38]. Various types of intelligent algorithms are applied to WELM for choosing the best parameter and compared with the proposed method. All these methods are then tested on three different credit card datasets. It is shown that the proposed method gives the best overall performance compared with other intelligent algorithms.

D. Literature Review Matrix

Author/ Date	Research Question(s)/ Objectives	Dataset	Machine Learning Methods	Results & Conclusions	Implications for Future research
Quatrini *et al.*, 2020 [4]	Apply two steps method for anomaly detection in production process. The two steps method are process phase identification and followed by anomaly detection.	• Pharmaceutical company granulation dataset	• RF • Decision jungle	• The comparison showed that the proposed method can achieve better performance compared to the method without identifying the process phase step.	• Apply training and testing continuously during new data collection • Build the two step methodology with other algorithm • Test the proposed method with other industrial data
Steenwinckel *et al.*, 2020 [8]	Develop a system which combines machine learning and expert knowledge for anomaly detection and predictive maintenance.	• Train sensor dataset from Televic Rail	• Machine learning based anomaly detection module • Machine learning based fault recognition	• The proposed method which combines semantic knowledge and machine learning methods is able to reduce the downtime and helps in analyzing the problems.	• Improve the dynamicity of the rule mining stage and let operators visually inspect the rules and knowledge. • Apply the system to other cases
Hasan *et al.*, 2019 [10]	Comparison of different machine learning models for anomaly detection in IoT systems.	• DS2OS traffic traces dataset from Kaggle	• LR • SVM • DT • RF • ANN	• RF performed best in predicting different types of cyberattacks.	• Develop a better algorithm • Work on real-time data • Apply RF for wider range of data

Author/ Date	Research Question(s)/ Objectives	Dataset	Machine Learning Methods	Results & Conclusions	Implications for Future research
Narayanan and Bobba, 2018 [11]	Develop an anomaly detection framework for robotic arms to detect abnormal activity caused by cyber-attack.	• Industrial arm dataset	• SVM	• The performance of the machine learning model to detect cyber-attack in smart manufacturing can be improved by creating labelled data using tolerance envelope technique.	• Build model that can apply in different manufacturing tasks • Build a model that can verify the robotic arm values independent from the ROS joint state values • Build a model that can detect defects of the robotic arm and differentiate it from attack problems.
Verner and Mukherjee, 2020 [18]	Apply LSTM recurrent neural networks for anomaly detection in raw sensory data, excluding the need of specifically designed feature vectors in different type of data.	• Glucose level measurements from JDRF medical dataset	• SVM • RF • NBC • SNN • LSTM	• The proposed LSTM is able to achieve the same level of performance by using raw data, compared with SVM, RF, NBC and SNN which used data with specific design features.	• Apply the LSTM model on other type of sensory data • Apply nested LSTM on more complex data
Hsieh, Chou and Ho, 2019 [19]	Apply LSTM-based unsupervised method for anomaly detection to reduce production failures.	• Manufacturing company production process sensors dataset	• LSTM Autoencoder • Vector Auto Regression • kNN • CNN	• The proposed method displayed the best performance against conventional methods used in industry.	• Improve the performance by studying the unusual pattern which gives rise to the false positive and false negative.
Zheng *et al.*, 2020 [20]	Apply metadata-driven multi-task transfer learning (M-MTL) model for different board type solder paste inspection anomaly detection.	• 3 months solder paste dataset from Huawei	• Isolation Forest • K-means clustering • Single-task learning • Feature-driven adapted transfer learning • Metadata-driven independent learning • M-MTL	• The proposed M-MTL method showed the best performance compared to other methods which can eliminate 81.28% of the false abnormal boards' detection.	• Apply cross validation in metadata-driven multi-task setting • Knowledge transfer between different applications

Author/ Date	Research Question(s)/ Objectives	Dataset	Machine Learning Methods	Results & Conclusions	Implications for Future research
Wang *et al.*, 2019 [21]	Develop a GAN based unsupervised anomaly detection model to improve the performance of detecting anomalies in high dimensional data.	• Surface Mounting Technology production line dataset from Foxconn Company	• OC-SVM • DSEBM • DAGMM • UAD-GAN	• The proposed model, UAD-GAN showed better performance in detecting abnormal samples than other common models.	• Apply the proposed model on other dataset • Improve the performance of the model by using multi-modal unsupervised learning
Qosim and Zulkarnain, 2020 [22]	Apply various machine learning classification techniques for fault detection in ammonia plant to prevent unscheduled shutdown.	• Distributed Control System history dataset	• LR • KNN • SVM • Decision Tree • Random Forest • Adaboost • XGBoost	• The machine learning classification techniques are able to detect anomaly activities during the synthesis process of ammonia plants, where RF showed the best overall performance.	• Apply neural network and deep learning • Develop predictive maintenance system
Dhankhad, Mohammed and Far, 2018 [25]	Apply ensemble learning (EL) methods for credit card fraud detection and make comparison with other supervised machine learning methods.	• European cardholder September 2013 dataset	• RF • Stacking EL • XGB • Gradient Boosting • LR • MLP • SVM • DT • KNN • NB	• Under-sampling was applied to balance the number of each class. • Stacking EL showed the best overall performance	• Apply voting classifier and increase the dataset size. • Apply feature selection to improve the performance.
Rtayli and Enneya, 2020 [27]	Develop a hybrid machine learning model for credit card fraud detection. The proposed method used RF as based, improved with recursive feature elimination, hyper parameter optimization and balancing class method.	• European dataset • PaySim dataset • Credit card transaction dataset 03	• Proposed method • DT • SVM • ANN • LR • NB • BBN • KNN	• The proposed method showed significant improvement of performance compared with other known methods.	• Apply improved model on complex, imbalanced real-world dataset • Develop a robust fraud detection system

Author/ Date	Research Question(s)/ Objectives	Dataset	Machine Learning Methods	Results & Conclusions	Implications for Future research
Nadim *et al.*, 2019 [29]	Apply various machine learning techniques for credit card fraud detection.	• European cardholder dataset from ULB	• Logistic Regression • LDA • kNN • RF • CART • SVM • XGB	• RF and XGB showed best overall performance with better accuracy and more cost effective.	• Improve the performance of the modals with substantial feature selection, stacked classifiers and genetic algorithm
Porwal and Mukund, 2019 [30]	Apply ensemble of clustering methods to assign a consistency score to each data point for credit card fraud detection.	• European cardholder dataset from Kaggle	• K-means clustering • Isolation forest	• The proposed method of assigning consistency score and use k-means clustering can detect fraud better than isolation forest.	• Apply other type of clustering algorithms and make comparison
Inoue *et al.*, 2017 [32]	Apply unsupervised machine learning techniques for anomaly detection in Cyber-Physical System.	• Secure Water Treatment testbed dataset	• Deep Neural Network with LSTM • One-class SVM	• DNN showed slightly better performance than SVM but it needs way more computational cost. • It took two weeks to train DNN while SVM only took 30 minutes.	• Improve the neural architecture and conduct feature engineering • Apply other machine learning techniques and make comparison
Kravchik and Shabtai, 2018 [33]	Apply a variety of deep neural network architectures for detecting cyber-attacks on industrial control system.	• Secure Water Treatment testbed dataset	• RNN • CNN	• A 1D convolutional neural network showed better performance and shorter run time in detecting ICS cyber-attack.	• Apply the proposed method on streaming data • Use the proposed model for faulty equipment detection

Author/ Date	Research Question(s)/ Objectives	Dataset	Machine Learning Methods	Results & Conclusions	Implications for Future research
Bhatia *et al.*, 2019 [36]	Develop unsupervised machine learning models to detect SYN floods and slow HTTP DDoS attacks in IoT network.	• Benign IoT traffic dataset • Network attack samples generated by using hping	• SVM • PCA statistical method • ANN Autoencoders	• Both the unsupervised classifiers, ANN and PCA performed way better than supervised SVM in detecting attack and anomalies in the industrial network.	• Apply the model in different size and type of dataset • Compare with other type of unsupervised methods
Bhuvaneswari Amma and Selvakumar, 2020 [37]	Apply fog based distributed vector convolutional deep learning (VCDL) to solve the non-scalable problem of anomaly detection in IoT devices.	• UNSW's Bot-IoT dataset	• VCDL • SVM • RNN • LSTM	• Shorter detection time is achieved with fog-based distributed anomaly detection compared with the centralized architecture. • VCDL showed best overall performance.	• Solve the class imbalance problem to improve the performance of classification.
Zhu *et al.*, 2020 [38]	Apply weighted extreme learning machine (WELM) enhanced by three variations of dandelion algorithm with probability-based mutation (DAPM) for credit card fraud detection.	• Loan prediction dataset • Creditcardcsvpresent dataset • Default of credit card clients dataset	• Improved particle swarm WELM • Bat algorithm WELM • Genetic algorithm WELM • DA-WELM • Self-learning DA-WELM • $DAPM_L$-WELM • $DAPM_B$-WELM • $DAPM_E$-WELM	• The three proposed methods are effective in detecting credit card fraud.	• Optimized WELMs with other algorithms and make comparison • Improve the performance of DA

IV. Conclusion and Future Research

Anomaly detection plays an important role in the domain of manufacturing, finance and internet security to ensure each process is working in normal condition. Among supervised machine learning methods, Random Forest (RF) are performing well in detecting anomalies across different experiments. However, supervised machine learning techniques do not do well in recognising new or unseen types of anomalies. Unsupervised clustering machine learning solves the issue by learning the feature of normal samples, any deviation from the learnt features larger than the threshold value is considered as anomaly. The disadvantage is the model may treat noise as an anomaly, raising false alarm. Deep learning displays promising results in anomaly detection but needs much longer time and more processing power for model training. Hybrid method is reported consistently to outperform conventional machine learning techniques as it is specifically customized to overcome the shortcoming of conventional machine learning methods in certain contexts. Therefore, to solve a problem in a specific domain, a creatively designed hybrid method is the most suitable candidate.

As there is disagreement between the effectiveness of resampling techniques, future research needs to be carried out to verify that by using a wider range of dataset and analyse the condition needed for resampling to be effective. Besides, ways to improve the performance of unsupervised machine learning techniques need to be studied especially in differentiating between noise and anomaly. Intelligent algorithms can be deployed to shorten the training time of deep learning and improve the performance of conventional machine learning techniques. Other than that, future research can be done to develop a hybrid model which can be applied and perform well across different domains.

Acknowledgment

Appreciation to Dr. Chandra Reka Ramachandiran and Dr. Vazeerudeen Abdul Hameed for their guidance in completing this review.

References

[1] R. Chalapathy and S. Chawla, "DEEP LEARNING FOR ANOMALY DETECTION: A SURVEY A PREPRINT," 2019.

[2] C. M. Ahmed, G. Raman, and A. P. Mathur, "Challenges in Machine Learning based approaches for Real-Time Anomaly Detection in Industrial Control Systems," vol. 7, no. 20, 2020, doi: 10.1145/3384941.3409588.

[3] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," ACM Comput. Surv., vol. 41, no. 15, 2009, doi: 10.1145/1541880.1541882.

[4] E. Quatrini, F. Costantino, G. Di Gravio, and R. Patriarca, "Machine learning for anomaly detection and process phase classification to improve safety and maintenance activities," J. Manuf. Syst., vol. 56, no. May, pp. 117–132, 2020, doi: 10.1016/j.jmsy.2020.05.013.

[5] I. Sadgali, N. Sael, and F. Benabbou, "Performance of machine learning techniques in the detection of financial frauds," Procedia Comput. Sci., vol. 148, no. Icds 2018, pp. 45–54, 2019, doi: 10.1016/j.procs.2019.01.007.

[6] O. Faraj, D. Megías, A. M. Ahmad, and J. Garcia-Alfaro, "Taxonomy and challenges in machine learning-based approaches to detect attacks in the internet of things," ACM Int. Conf. Proceeding Ser., 2020, doi: 10.1145/3407023.3407048.

[7] N. F. Ryman-Tubb, P. Krause, and W. Garn, "How Artificial Intelligence and machine learning research impacts payment card fraud detection: A survey and industry benchmark," Eng. Appl. Artif. Intell., vol. 76, no. June, pp. 130–157, 2018, doi: 10.1016/j.engappai.2018.07.008.

[8] B. Steenwinckel et al., "FLAGS: A methodology for adaptive anomaly detection and root cause analysis on sensor data streams by fusing expert knowledge with machine learning," Futur. Gener. Comput. Syst., vol. 116, pp. 30–48, 2020, doi: 10.1016/j.future.2020.10.015.

[9] A. Kim, Y. Song, M. Kim, K. Lee, and J. H. Cheon, "Logistic regression model training based on the approximate homomorphic encryption," BMC Med. Genomics, vol. 11, no. 4, pp. 23–31, Oct. 2018, doi: 10.1186/s12920-018-0401-7.

[10] 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, 2019, doi: 10.1016/j.iot.2019.100059.

[11] V. Narayanan and R. B. Bobba, "Learning Based Anomaly Detection for Industrial Arm Applications," in Cyber-Physical Systems Security & Privacy (CPS-SPC '18), October 19, 2018, Toronto, ON, Canada, 2018, p. 108.

[12] J. Vanerio and P. Casas, "Ensemble-learning approaches for network security and anomaly detection," Big-DAMA 2017 - Proc. 2017 Work. Big Data Anal. Mach. Learn. Data Commun. Networks, Part SIGCOMM 2017, pp. 1–6, 2017, doi: 10.1145/3098593.3098594.

[13] P. Saikia, R. D. Baruah, S. K. Singh, and P. K. Chaudhuri, "Artificial Neural Networks in the domain of reservoir characterization: A review from shallow to deep models," Computers and Geosciences, vol. 135. Elsevier Ltd, p. 104357, Feb. 01, 2020, doi: 10.1016/j.cageo.2019.104357.

[14] S. A. Abdulrahman, W. Khalifa, M. Roushdy, and A. B. M. Salem, "Comparative study for 8 computational intelligence algorithms for human identification," Computer Science Review, vol. 36. Elsevier Ireland Ltd, p. 100237, May 01, 2020, doi: 10.1016/j.cosrev.2020.100237.

[15] P. Schneider and K. Böttinger, "High-performance unsupervised anomaly detection for cyber-physical system networks," Proc. ACM Conf. Comput. Commun. Secur., pp. 1–12, 2018, doi: 10.1145/3264888.3264890.

[16] S. Saurav et al., "Online anomaly detection with concept drift adaptation using recurrent neural networks," ACM Int. Conf. Proceeding Ser., pp. 78–87, 2018, doi: 10.1145/3152494.3152501.

[17] K. Doshi and Y. Yilmaz, "Continual learning for anomaly detection in surveillance videos," IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit. Work., vol. 2020-June, pp. 1025–1034, 2020, doi: 10.1109/CVPRW50498.2020.00135.

[18] A. Verner and S. Mukherjee, "An LSTM-Based Method for Detection and Classification of Sensor Anomalies," ACM Int. Conf. Proceeding Ser., pp. 39–45, 2020, doi: 10.1145/3409073.3409089.

[19] R. J. Hsieh, J. Chou, and C. H. Ho, "Unsupervised online anomaly detection on multivariate sensing time series data for smart manufacturing," Proc. - 2019 IEEE 12th Conf. Serv. Comput. Appl. SOCA 2019, pp. 90–97, 2019, doi: 10.1109/SOCA.2019.00021.

[20] Z. Zheng et al., "Contextual Anomaly Detection in Solder Paste Inspection with Multi-Task Learning," ACM Trans. Intell. Syst. Technol., vol. 11, no. 6, pp. 1–17, 2020, doi: 10.1145/3383261.

[21] H. Wang, M. Li, F. Ma, S. L. Huang, and L. Zhang, "Poster abstract: Unsupervised anomaly detection via generative adversarial networks," in IPSN 2019 - Proceedings of the 2019 Information Processing in Sensor Networks, Apr. 2019, pp. 313–314, doi: 10.1145/3302506.3312605.

[22] H. Qosim and Zulkarnain, "Fault Detection System Using Machine Learning on Synthesis Loop Ammonia Plant," ACM Int. Conf. Proceeding Ser., pp. 74–80, 2020, doi: 10.1145/3400934.3400950.

[23] S. Makki, Z. Assaghir, Y. Taher, R. Haque, M. S. Hacid, and H. Zeineddine, "An Experimental Study With Imbalanced Classification Approaches for Credit Card Fraud Detection," IEEE Access, vol. 7, pp. 93010–93022, 2019, doi: 10.1109/ACCESS.2019.2927266.

[24] T. Baabdullah, A. Alzahrani, and D. B. Rawat, "On the Comparative Study of Prediction Accuracy for Credit Card Fraud Detection wWith Imbalanced Classifications," Proc. 2020 Spring Simul. Conf. SpringSim 2020, 2020, doi: 10.22360/SpringSim.2020.CSE.004.

[25] S. Dhankhad, E. A. Mohammed, and B. Far, "Supervised machine learning algorithms for credit card fraudulent transaction detection:

A comparative study," Proc. - 2018 IEEE 19th Int. Conf. Inf. Reuse Integr. Data Sci. IRI 2018, pp. 122–125, 2018, doi: 10.1109/IRI.2018.00025.

[26] V. N. Dornadula and S. Geetha, "Credit Card Fraud Detection using Machine Learning Algorithms," Procedia Comput. Sci., vol. 165, pp. 631–641, 2019, doi: 10.1016/j.procs.2020.01.057.

[27] N. Rtayli and N. Enneya, "Enhanced credit card fraud detection based on SVM-recursive feature elimination and hyper-parameters optimization," J. Inf. Secur. Appl., vol. 55, no. September, p. 102596, 2020, doi: 10.1016/j.jisa.2020.102596.

[28] X. Yu, X. Li, Y. Dong, and R. Zheng, "A Deep Neural Network Algorithm for Detecting Credit Card Fraud," Proc. - 2020 Int. Conf. Big Data, Artif. Intell. Internet Things Eng. ICBAIE 2020, pp. 181–183, 2020, doi: 10.1109/ICBAIE49996.2020.00045.

[29] A. H. Nadim, I. M. Sayem, A. Mutsuddy, and M. S. Chowdhury, "Analysis of machine learning techniques for credit card fraud detection," Proc. - Int. Conf. Mach. Learn. Data Eng. iCMLDE 2019, pp. 42–47, 2019, doi: 10.1109/iCMLDE49015.2019.00019.

[30] U. Porwal and S. Mukund, "Credit card fraud detection in E-commerce," Proc. - 2019 18th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. IEEE Int. Conf. Big Data Sci. Eng. Trust. 2019, pp. 280–287, 2019, doi: 10.1109/TrustCom/BigDataSE.2019.00045.

[31] M. O. Pahl and F. X. Aubet, "All Eyes on You: Distributed Multi-Dimensional IoT Microservice Anomaly Detection," in 14th International Conference on Network and Service Management, CNSM 2018 and Workshops, 1st International Workshop on High-Precision Networks Operations and Control, HiPNet 2018 and 1st Workshop on Segment Routing and Service Function Chaining, SR+SFC 2, 2018, pp. 72–80.

[32] J. Inoue, Y. Yamagata, Y. Chen, C. M. Poskitt, and J. Sun, "Anomaly detection for a water treatment system using unsupervised machine learning," IEEE Int. Conf. Data Min. Work. ICDMW, vol. 2017-Novem, pp. 1058–1065, 2017, doi: 10.1109/ICDMW.2017.149.

[33] M. Kravchik and A. Shabtai, "Detecting cyber attacks in industrial control systems using convolutional neural networks," Proc. ACM Conf. Comput. Commun. Secur., no. 1, pp. 72–83, 2018, doi: 10.1145/3264888.3264896.

[34] K. Greff, R. K. Srivastava, J. Koutnik, B. R. Steunebrink, and J. Schmidhuber, "LSTM: A Search Space Odyssey," IEEE Trans. Neural Networks Learn. Syst., vol. 28, no. 10, pp. 2222–2232, Oct. 2017, doi: 10.1109/TNNLS.2016.2582924.

[35] R. Jozefowicz and W. Zaremba, "An Empirical Exploration of Recurrent Network Architectures," PMLR, Jun. 2015. Accessed: Nov. 22, 2020. [Online]. Available: http://proceedings.mlr.press/v37/jozefowicz15.html.

[36] R. Bhatia, S. Benno, J. Esteban, T. V. Lakshman, and J. Grogan, "Unsupervised machine learning for network-centric anomaly detection in IoT," in Big-DAMA 2019 - Proceedings of the 3rd ACM CoNEXT Workshop on Big DAta, Machine Learning and Artificial Intelligence for Data Communication Networks, Part of CoNEXT 2019, Dec. 2019, pp. 42–48, doi: 10.1145/3359992.3366641.

[37] N. G. Bhuvaneswari Amma and S. Selvakumar, "Anomaly detection framework for Internet of things traffic using vector convolutional deep learning approach in fog environment," Futur. Gener. Comput. Syst., vol. 113, pp. 255–265, 2020, doi: 10.1016/j.future.2020.07.020.

[38] H. Zhu, G. Liu, M. Zhou, Y. Xie, A. Abusorrah, and Q. Kang, "Optimizing Weighted Extreme Learning Machines for imbalanced classification and application to credit card fraud detection," Neurocomputing, vol. 407, pp. 50–62, 2020, doi: 10.1016/j.neucom.2020.04.078.