HIGH ACCURACY ANOMALY DETECTION FOR CYBER PHYSICAL SYSTEM USING SELF-ORGANIZING MAP BASED ALGORITHM

KWAN CHAK YIN

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

A report submitted in partial fulfilment of the requirements for the degree of Bachelor of Mechatronics Engineering

Faculty of Electrical Engineering
UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2018

"I hereby declare that I have read through this report entitle "**HIGH ACCURACY ANOMALY DETECTION FOR CYBER PHYSICAL SYSTEM USING SELF-ORGANIZING MAP BASED ALGORITHM**" and found that it has complied with requirement for the partial fulfilment for awarding the degree of Bachelor of Mechatronics Engineering."

Signature : .....

Supervisor's Name : ASSOC. PROF. DR. MUHAMMAD FAHMI BIN MISKON

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

Date : .....

I declare that this report entitles "**HIGH ACCURACY ANOMALY DETECTION FOR CYBER PHYSICAL SYSTEM USING SELF-ORGANIZING MAP BASED ALGORITHM**" is the result of my own research except as cited in the references. The report has not been accepted for any degree and is not concurrently submitted in the candidature of any other degree.

Signature : .....

Name : KWAN CHAK YIN

Date : .....

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

To my beloved family

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

ACKNOWLEDGEMENT

First, I would like to express my sincere thanks and greatest appreciation to my supervisor, Associate Professor Dr. Muhammad Fahmi Bin Miskon for the expertise sharing, truthful and treasured guidance and encouragement extended to me during the undergoing of FYP.

I would like to express my greatest gratitude to my FYP panels, Pn. Nurdiana Bt. Nordin @ Musa and Dr Mohd. Shahrieel B. Mohd. Aras for the valuable yet attentive advice given during the undergoing of FYP. Apart from that, I would like to express my deep sense of gratitude to all the coursemates and friends for being kind and helpful in completing the FYP.

I would like to take this opportunity to express greatest appreciation to my family for their continuous shower of love, unceasing encouragement and support throughout my life. I derived inspiration from their sacrifice, encouragement from their faith, found happiness in their pride and the strength from their unconditional love.

Besides that, my grateful thanks are also extended to Universiti Teknikal Malaysia Melaka (UTeM) for the resources offered in running FYP. Without the help of the particulars that I mentioned above, I might face difficulties during the FYP. Last but not least, my sense of gratitude is recorded to the one and all who, directly or indirectly, have offered their helping hand during the entire period of FYP.

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

ABSTRACT

In order to embrace challenges of Industry 4.0 (I4.0), failure prediction on the machinery in the Cyber-Physical System (CPS) is important which gives rise to the research in anomaly detection. Recent studies on anomaly detection generally applied to the network security, fraud system and image processing. However, anomaly detection in I4.0 have difficulty in ensuring the designed algorithm is self-adaptive without compromising the accuracy of the prediction. Hence, this project addresses this problem by proposing a habituating SOM-based algorithm to predict the possible failure faced in the system. In the proposed method, the SOM and k-means act as the clustering network for the mechanism, while the habituation function take role as set of habituating synapses that form connection among the network neurons to the output. Weight vector for the neurons is initialized via k-means clustering to ensure reasonable number of cluster and proper distribution of weight vector. Receiver Operating Characteristic (ROC) curve is used to optimize threshold value of Euclidean distance. Accuracy test is carried out by execute the algorithm to different dataset that contain various number of anomalies. The performance of the algorithm is evaluated via the application of confusion matrix in term of accuracy. The proposed algorithm can detect the anomalies occur in the data accurately with minimum accuracy of 98.5% and maximum accuracy of 99.2%. This indicates that there is possibility to use the proposed anomaly detection technique to predict the possible failure in CPS' machinery.

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

ABSTRAK

Demi untuk menyahut cabaran dalam menerajui I4.0, ramalan ketidakfungsian mesin dalam dalam CPS sangat penting yang mana membangkitkan penyelidikan terhadap pengesanan keganjilan. Kajian yang sedia ada terhadap pengesanan keganjilan kebanyakannya digunakan untuk sistem keselamatan rangkaian, pengesanan penipuan dan pemprosesan imej. Walau bagaimanapun, pengesanan keganjilan dalam I4.0 mengalami kesulitan dalam menjamin algoritma yang direka mempunyai kebolehan pembelajaran kendiri tanpa mengabaikan ketepatannya dalam mengesan keganjilan. Oleh itu, kajian ini menangani masalah ini dengan mencadangkan algoritma berasaskan pembiasaan SOM untuk meramalkan kemungkinan kegagalan yang dialami oleh mesin. Dalam kaedah yang dicadangkan, SOM dan k-means bertindak sebagai rangkaian cluster untuk mekanisme, manakala fungsi pembiasaan memainkan peranan sebagai set sinapsis pembiasaan yang membentuk sambungan antara neuron rangkaian ke hasilannya. Vektor berat untuk neuron diasaskan melalui k-means clustering untuk menjaminkan bilangan neuron dan pengagihan vektor berat yang munasabah. Lengkungan ROC digunakan untuk mengoptimumkan nilai ambang jarak Euclidean. Ujian ketepatan dijalankan dengan melaksanakan algoritma dengan set data yang mempunyai bilangan keganjilan yang berbeza. Prestasi algoritma dinilai melalui aplikasi matriks confusion dari segi ketepatan. Algoritma yang dicadangkan boleh mengesan keganjilan yang terdapat dalam set data dengan tepat dengan ketepatan yang sekurangnya 98.5% dan sebanyaknya 99.2%. Ini menunjukkan bahawa ada kemungkinan untuk menggunakan teknik pengesanan keganjilan yang dicadangkan untuk meramal kegagalan yang mungkin wujud dalam mesin CPS.

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

TABLE OF CONTENTS

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

LIST OF TABLES

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

LIST OF FIGURES

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

LIST OF ABBREVIATIONS

ACC	–	Accuracy
AI	–	Artificial Intelligence
ANN	–	Artificial Neural Network
BMU	–	Best Matching Unit
BPNN	–	Backpropagation ANN
CNN	–	Convolutional ANN
CPI	–	Continuous Process Improvement
CPS	–	Cyber-Physical System
DBM	–	Deep Boltzmann Machine
DBN	–	Deep Belief Network
DNN	–	Deep ANN
DWT	–	Discrete Wavelet Transform
FN	–	False negative
FP	–	False positive
FPR	–	False Positive Rate
GGSOM	–	Growing Grid SOM
GHSOM	–	Growing Hierarchical SOM
GNG	–	Growing Neural Gas
I4.0	–	Industry 4.0
IDS	–	Intrusion Detection System
IoT	–	Internet of Things
IR4.0	–	Industrial Revolution 4.0
MCC	–	Matthews Correlation Coefficient
MLP	–	Multilayer Perceptron
PHM	–	Prognostic and Health Management
PPV	–	Precision/ Positive Predictive Value
PSO	–	Particle Swarm Optimization
PSOM	–	Periodic SOM
RBFNN	–	Radial Basis Function ANN

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

RBM	–	Restricted Boltzmann Machine
RNN	–	Recurrent ANN
ROC	–	Receiver Operating Characteristic
SOM	–	Self-organizing Map
SSOM	–	Scalable SOM
TN	–	True negative
TNR	–	True Negative Rate
TP	–	True positive
TPR	–	True Positive Rate
WEF	–	World Economic Forum

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

The Industry 4.0 (I4.0) is introduced in German Hannover Fair. It ignites the start of the Industrial Revolution 4.0 (IR4.0) with the improvement in the Cyber-Physical System (CPS) and the Internet of Things (IoT) [1]. I4.0 become the main concern in World Economic Forum (WEF) 2016 Conference. Executive chairperson of WEF 2016, Prof. Klaus Schwab state that I4.0 is mainly described the CPS and mainly build on the third industrial revolution that uses electronic and information technology system as basic of the automated production line [2]. Hence, the basic principle of I4.0 is to connect machines, processes, systems as well as business via an intelligent network to control each other autonomously [3]. The main design principles of I4.0 are interoperability that concern about integration that acts as the root of IoT and CPS and cognizance that originated from artificial intelligence (AI) that leads to the decision-making and prognostic maintenance of the system [4].

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

CPS is the transformative technologies to manage the interconnected system between its physical resources and computational capabilities. Jay Lee et. al. [5, 6] proposed CPS structure consist of five levels, basically known as 5C architecture. The structure of CPS is mainly build up by the advanced connectivity that ensures good interfacing between physical space and cyberspace and the intelligent data analytic that built up the cyberspace. The levels of 5C architecture including smart connection level that provides seamless and tether-free methods for data acquisition system management, data transfer to the central server; data-to-information conversion level that analysed and transformed data collected into valuable information; cyber level that acts as central information hub; cognition level that good in decision-making as well as configuration level that give feedback from cyberspace to physical space as well as take the role of advisory control . [5, 6].

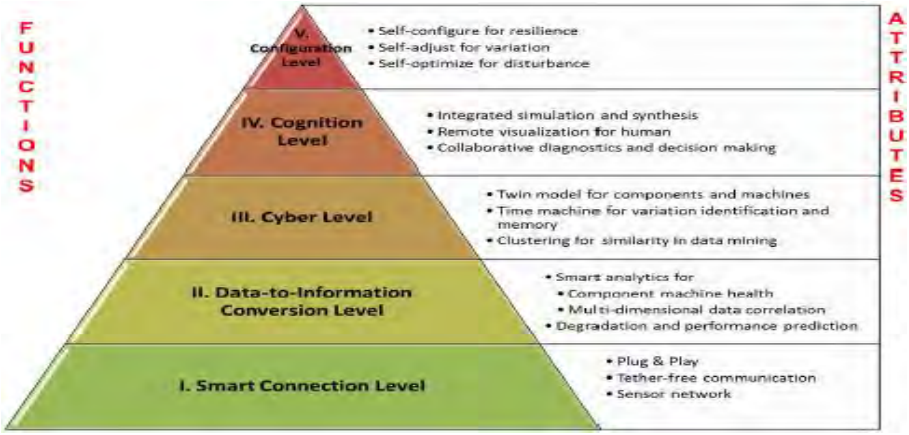

Figure 1.1: The implementation of 5C architecture in CPS. [5, 6]

The IR4.0 is concerned to the self-adaptive of the CPS which involve the concept of machine learning that related to the system changes that complete task given via artificial intelligent through techniques such as recognition, prediction and others [7]. It also allows the complex mathematical calculation can be automatically apply to the big data in the cloud for the analysis [8]. Hence, the CPS in I4.0 should not be tied to any fixed program and the changes on the program is allowed in order to enhance the CPS function. Anomaly detection describing a technique of finding patterns in data that do not follow a priori expected behaviour [9]. It is a useful tool to increase productivity with monitoring and failure prevention. Besides, it is also providing an essential way for the machine manufacturers to complete the technology improvement in the continuous improvement process.

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

1.1 MOTIVATION

Industry 4.0 is unavoidable and bound to happen by TN50 that aimed to rise up the usage of broadband and mobile connectivity, IoT, robotics and Artificial Intelligence (AI) incorporation of formation of “smart city” [10]. The concept of the smart factory had been implement in some country such as United States of America, Germany, Japan, Singapore as well as South Korea, but in terms of automating, Malaysia is still in the infancy stage and back end of the line [11]. According to research on the readiness to embrace challenges of Industry 4.0 by WEF 2016, Malaysia got a relatively low rating on the aspect of infrastructure readiness and legal protection. The relatively low rating on the infrastructure readiness due to the lack of

new technology implementation in the industry and the ready facilities and machine in the industry cannot meet the cyber-physical system requirement. Hence, the WEF 2016 evaluated Malaysia as an emerging market. The low maturity level of required technology also became the main concerned challenges in the nine challenges need to face in order to succeed in this industrial revolution [12].

Global competitiveness rankings for the fourth industrial revolution.
Source: UBS (2016), WEF (2017), IMD (2017).

Rank	Nation	UBS	WEF	IMD	Average
1	Singapore	2	1	1	1.3
2	Finland	4	2	4	3.3
3	U.S.A.	5	5	3	4.3
4	Netherland	3	6	6	5.0
5	Switzerland	1	7	8	5.3
	Sweden	11	3	2	5.3
7	Norway	8	4	10	7.3
8	United Kingdom	7	8	11	8.3
	Denmark	9	11	5	8.3
10	Hong Kong	7	12	7	8.7
11	Canada	15	14	9	12.7
12	New Zealand	10	17	14	13.7
13	Germany	13	15	17	15.0
14	Taiwan	16	19	12	15.7
15	Japan	12	10	27	16.3
16	Australia	17	18	15	16.7
17	Austria	18	20	16	18.0
18	Israel	21	21	13	18.3
19	Korea	25	13	19	19.0
20	Ireland	14	25	21	20.0
21	Belgium	19	23	22	21.3
22	France	20	24	25	23.0
23	Malaysia	22	31	24	25.7
24	Portugal	23	30	33	28.7

Figure 1.2: Global competitiveness rankings for IR4.0 [12]

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

Based on a report by EdgeMarket, 97.3% of business establishment in Malaysia is Small and Medium Enterprise. Only 10% of ICT adoption by SME compared to the ICT adoption in developed countries, which have 50% according to Malaysia Productivity Corporation [13]. Most of the SME are still in the industrial revolution 2.0 that based on mass production empowered by electrically driven [11].

The continuous process improvement (CPI) is important to the industry as a continuing action to improve the processes, services as well as the products of the industry through justifiable changes over a period. The traditional CPI method cannot deal with the current challenges faced that mainly due to the increased of sensors and actuators that lead to multi-parameter production space, big data environment as well as complex dependencies in the production space [14]. Hence, maintenance of the physical assets became the concerned problem in the industry nowadays. Anomaly detection is concerning the cognition level in the CPS to provide continuous

improvement process as well as the predictive maintenance. Hence, in order to ensure the completeness in the Industry 4.0, with the use of the anomaly detection algorithms, the anomaly happened can be automatically detect by the CPS itself and making decision once, the anomalies are detect as well as predict in advance the potential failures of the physical system.

1.2 PROBLEM STATEMENT

Anomaly detection consists of two steps, which are learning the normal behaviour from the previous data and identifying the abnormalities in the presence data [14]. Hence, the detection in the CPS based on the big data analytic, which the analysis of data will be done in the cyber-space. In addition, the self-adaptive of the algorithm used as the detection also need to be done in the data-driven orientation. In order to define the metric for maintenance, the algorithm also should be able to predict the performance and predict the possible failure that would occur. Besides, the amount of data in the cloud is very large and lead to the difficulties in clustering the data as well as looking for the anomalies in the data set.

However, anomaly detection in CPS was relatively new. An investigation on the approach to anomaly detection and its accuracy in the existing applications is needed to provide a useful ground for this project.

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

As the IR4.0 is mainly concerned about the autonomous system, hence the challenge faced in the anomaly detection for IR 4.0 is the self-adaptive of the machine in learning the normal behaviour, comparing the previous with presence, detect the anomalies as well as giving the best decision in the rapid changing manufacturing line in the smart factory. Hence, a neural network algorithm needed to be designed to solve the problem.

Besides, the performance of anomaly detection algorithm is been evaluated in different way in the existing application. The investigation on the method of evaluation for anomaly detection for the existing method is needed in order to choose the most suitable method to evaluate algorithm.

Therefore, an anomaly detection algorithm that is created using the neural network is proposed to solve the problem faced.

1.3 OBJECTIVES

The objectives of this research project are:

i. To investigate the self-adaptive and accuracy of anomaly detection for the cyber-physical system.
ii. To design and develop an anomaly detection algorithm using self-organizing map (SOM).
iii. To validate the anomaly detection algorithm based on the confusion matrix and receiver operating characteristic (ROC) curve.

1.4 SCOPE

The research is focused on creating and design an anomaly detection algorithm that use to detect the unusual performance of the manipulator. Hence, the designed anomaly detection algorithm is used to evaluate the performance of manipulator and define the metric of maintenance of the manipulator via detecting the anomalies present in the manipulator's behaviour.

Hence, the scopes and limitations of this project are stated as below:

- The CPS investigated in this study is restricted to a manufacturing system with known resources and processes.
- The sample and dataset used in the simulation of algorithm is generated from the V-Rep Robot Simulator.
- The algorithm is mainly designed based on the SOM, while k-means clustering only act as the neuron and neuron weight finder.
- The performance of the algorithm is evaluated based on the accuracy of the algorithm in detecting the true anomalies present in the presence data.
- The algorithm aims to detect the point anomalies.

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

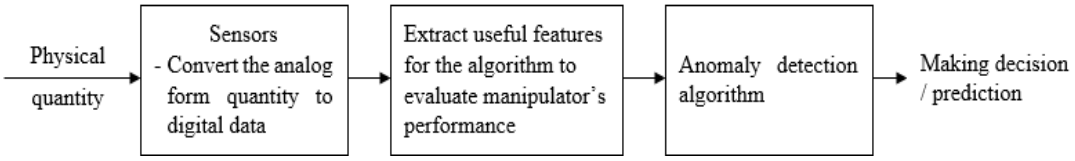

Figure 1.3: The basic block diagram of the system

1.5 OUTLINE OF THE REPORT

This part discusses the role of the rest of the report with a brief explanation on the part of the report. The report is organized as follows:

Chapter 2: Literature Review

This chapter discusses the theoretical background and basic principles that involved for the completion of the report. This part describes the type of anomalies as well as the type of anomaly detection method. This part also reviews and summaries the previous works about the anomaly detection in different applications.

Chapter 3: Research Methodology

This chapter brief the working principle of the method that had been chose to solve the problem of the project. This chapter also discusses the theory related to project solution as well as the method used for the development of the anomaly detection algorithm. The chapter also shows the approach to evaluate the performance of the designed anomaly detection algorithm.

Chapter 4: Result and Discussion

This chapter describes the result that had been achieve in the project. The chapter also gives the analysis and discussion on the result that had been obtained throughout the project.

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

Chapter 5: Conclusion and Recommendation for Future Work

This chapter summarizes the progress of the project by review all the information obtained for the project. The chapter also provides the recommendation for the future work.

CHAPTER 2

LITERATURE REVIEW

2.1 THEORETICAL BACKGROUND

2.1.1 Cyber-Physical System (CPS)

CPS is a heterogeneous strategy that includes computation and communication devices that link together with sensors and actuators. Reddy [15, 16] state that CPSs is the control system that is distributed, smart, real-time response, self-learning and have the possibility to be connected in a loop. While Ribeiro [17] define CPS as an embedded system with good communication capabilities and the intelligent and permanent connection between the cyber-space which is the logical component and the physical system. With the existence of the CPS, the automated continuous improvement cycle is created.

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

The existence of preventive maintenance concept and Total Productive Maintenance in 1951 made the Prognostic and Health Management (PHM) start to develop. PHM has the capability to convert data into desired information about the pattern of inefficient performance. Fusion of advanced analytic with communication and the physical machinery leads to CPS and make PHM step closer to completion. Jay Lee et. al. [6] [5] state that increases of usage of sensors and interacted machinery require the system to handle big data. In order to achieve the intelligent and self-adaptive, big data management and leveraging machines' interoperability is necessary.

At the stage of the component, the sensor is not just for the use of precision, but also responsible in capture the sensory data from component and convert it into useful information to offer self-prediction and self-awareness to the system. For the machine stage, the advanced machine data such as controller parameter is not only to supervise the performance of the machine, but also give the self-comparison to the machine by aggregated the advanced machine data to the component information from

sensors in order to monitor the status of the machine. For the production stage of the CPS, the aggregated information from the sensors and machines provides the self-maintainability and self-configurability to the factory in order to offer worry-free production with near-zero downtime and improved manufacture scheduling [5].

	Data source	Today's factory		Industry 4.0	
		Attributes	Technologies	Attributes	Technologies
Component	Sensor	Precision	Smart sensors and fault detection	Self-aware Self-predict	Degradation monitoring & remaining useful life prediction
Machine	Controller	Producibility & performance	Condition-based monitoring & diagnostics	Self-aware Self-predict Self-compare	Up time with predictive health monitoring
Production system	Networked system	Productivity & OEE	Lean operations: work and waste reduction	Self-configure Self-maintain Self-organize	Worry-free productivity

Figure 2.1: Comparison between the elements of today's factory and I4.0 [5]

The CPS should can communicate with the integration between the control system, software as well as the communication linkage; uniquely identified, as CPS is part of Internet of Everything (IoE) that can be uniquely addressed with the identifier; have controller, sensors and actuators as the basis of the system to operate; act as the basic building block of I4.0 as well as the enabler of the extra capabilities; have the capabilities to enable smart factory [18].

اونيۏرسيتي تيكنيكل مليسيا ملاك
UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2.1.2 Anomaly Detection

Anomaly detection is the technique that identifies the data point or pattern that do not follow the expected or normal behaviour, called anomalies or outliers [19]. Anomaly detection is similar to, but have some differences compared to noise removal and novelty detection. Novelty detection is focus on identify the unnoticed pattern in new observation that system is not alert during the training session [20] while noise removal is defined as the process that removing noise from the wanted signal [21]. Major goals of anomaly detection in IR4.0 are automatic monitoring and detect the abnormal events and points on the collected data [22]. Anomaly detection is important to increase the productivity in the manufacturing line, provide continuous improvement to achieve mastery of the technology as well as define the metric for maintenance to detect the malfunction or abnormality in the running machine [23].

2.2 THEORY AND BASIC PRINCIPLE

2.2.1 Type of Anomaly Detection Setup

The mode of the anomaly detection setup is differentiate based on the labels available in the dataset. Hence, the mode is categorized into 3 types whereas:

2.2.1.1 Supervised anomaly detection

Supervised anomaly detection defines the mode that uses the training data contains fully categorized data which is the normal behaviours and anomalies as well as test data. The algorithm is trained first with a set of input with equivalent accurate output and then learned by comparing the actual output with the desired to find an error in order to identify the anomaly [8]. Goldstein and Ushida [24] state that the setup is irrelevant due to the statement that all the outliers are identified and labelled properly as the anomalies for most of the application are unknown in advance. Chandola et. al. [25] state that the supervised method has issues that the number of anomalies is far fewer than the normal data in the training data which the occurrence of imbalanced distribution of data and follow with the high difficulty in getting an accurate label on the unlabelled data.

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

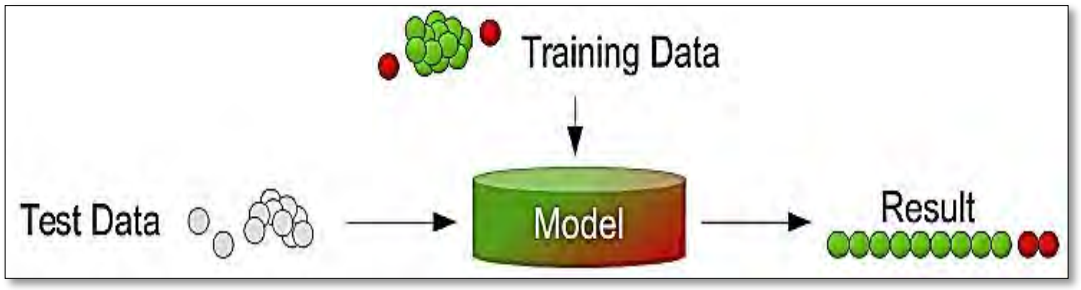

Figure 2.2: The model for supervised anomaly detection mode [24]

2.2.1.2 Semi-supervised anomaly detection

Semi-supervised anomaly detection describes the mode that uses the training data that have normal instances and anomalies to train the algorithm and the test datasets [24]. Chandola et. al. [25] describe the possibility to train the algorithm with the data that only consist of outliers, but this method is not commonly being used due to the difficulty in obtaining the training data that have every possible outlier that might appear in the data.

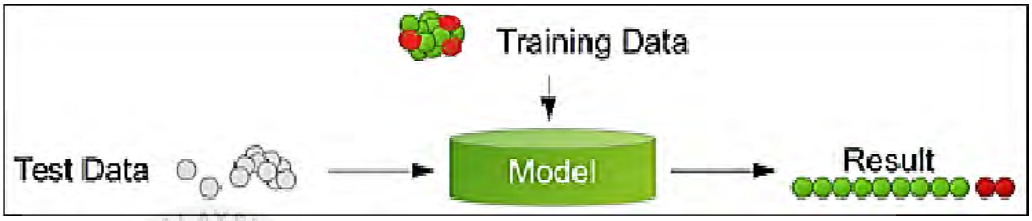

Figure 2.3: The model for semi-supervised anomaly detection mode [24]

2.2.1.3 Unsupervised anomaly detection

Unsupervised anomaly detection is the most widely used method as no training data required. The method is applicable to the data set that has no historical labels to explore the structure of the data [8]. The algorithm estimate the data score based on the fundamental properties of the dataset. Most of the data are labelled based on the distances and densities [24]. If the assumption that the normal data is far more common than an anomaly in the data is false, then resulted in the high false alarm rate. Semi-supervised mode can adapt to an unsupervised mode with the use of a sample of unlabelled data as the training data. The adaptation assumes that very little of outliers contain in the test data and the learning of the algorithm during the training is robust to the outliers appeared in the test data.

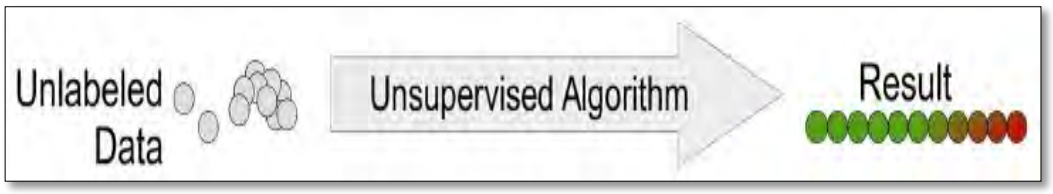

Figure 2.4: The model for unsupervised anomaly detection mode [24]

2.2.2 Type of Anomalies

Anomaly, also known as an outlier is the data or instance that do not follow the prior data behaviour [26] or the instance that occurs rarely in the data set [24]. Anomalies can be differentiated to three group:

2.2.2.1 Point Anomalies

Point anomalies, also known as the global anomalies define as the single data that is different from the dense area of data [24]. It is the simplest type of outlier and the main focus in the research in anomaly detection [25].

2.2.2.2 Contextual Anomalies

Contextual anomalies, also known as the local anomalies or conditional anomalies define as the data that seen like normal but act like anomalous when compared with its nearest neighbourhood or a specific environment [24]. The data is determined based on two set of attributes which are contextual attributes that estimate the neighbourhood for that data and behavioural attributes that describe the non-contextual characteristic of the data. The effect of anomalies to the target application and accessibility of contextual attributes greatly affect the application of local outlier detection method [25].

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2.2.2.3 Collective Anomalies

Collective anomalies, also known as micro clusters describe a little set of data collection that is anomalous to the entire data. The algorithm should allocate scores to its members greater than normal data, but less significant value than the noticeable outliers [24]. The single data in the collective anomaly might not be anomalous to each other, but the collection of the single data is anomalous to the entire dataset [25].

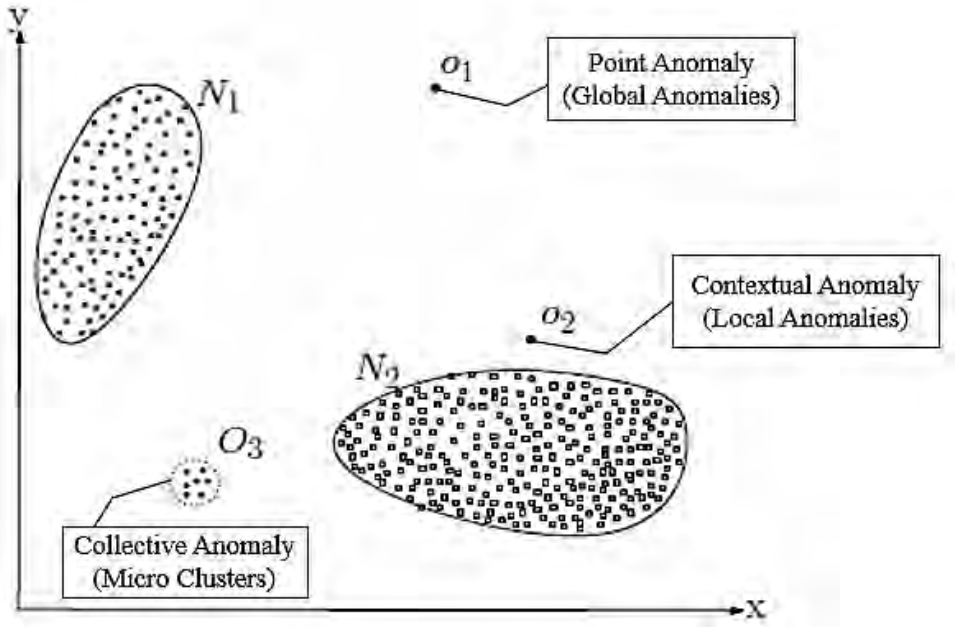

Figure 2.5: Type of anomalies [25]

The point anomaly and collective outliers can also act as the contextual anomalies once the data is analysed with respect to the context. A global outlier or collective outlier detection can convert to contextual anomaly detection by interfacing it to respective information [25]. A pre-processing is needed for the practical anomaly detection in order to produce suitable data view. Hence, the dataset needs to be set carefully to avoid the preprocessing and can straight away determine the performance of the algorithm [24].

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2.2.3 Type of Anomaly Detection Output

The anomalies can be reported in two ways.

First, the label can straight away specify either the data is an outlier or not. Due to the availability of the detection algorithm, most of the supervised detection use the label as output. Second, the score is an output that uses degree of irregularity.

Scores more commonly used in the semi-supervised and unsupervised anomaly detection technique as most of the application ranked the anomalies frequently.

The score can be transformed into label via a suitable threshold application.

2.2.4 Type of Distance Measurement in Clustering

In order to cluster the data set, there are few of the basic distance measurement to be applied to the algorithm to calculate the distance between two data. Distance measurement is for the ease of clustering as well as determine the anomaly in the data [27]. Han and Kamber [28] summarise few of the basic distance measurement techniques which are:

- Euclidean distance

$$D(x,y) = \sqrt{\sum(x_i - y_i)^2} \quad (2.1)$$

- Manhattan distance / City-block distance [29]

$$D(x,y) = \sum|x_i - y_i| \quad (2.2)$$

- Chebychev distance / Sup distance [29]

$$D(x,y) = |x_i - y_i| \quad (2.3)$$

- Categorical data distance

$$D(x,y) = (number\ of\ x_i - number\ of\ y_i) / \mathrm{N} \quad (2.4)$$

N = Total number of categorical characteristics

- Minkowski distance

It can be assumed as the simplification of Manhattan and Euclidean distance.

$$D(x,y) = (\sum_i^n |x_i - y_i|^p)^{1/p}, p \geq 1 \quad (2.5)$$

The latter is Euclidean distance, while former is Manhattan distance. By limiting p to infinity, Chebychev distance is obtained. [29]

- Mahalanobis distance [29]

$$D(x,y) = (x_i - y_i)^T S^{-1}(x_i - y_i) \quad (2.6)$$

- Kernel-based function

The distance between two data point is measured by mapping the data obliquely into high dimensional space that linearly separates the data. [30]

$$\left\|\varphi(\overrightarrow{x_i}) - \varphi(\overrightarrow{x_j})\right\|^2 = 2\left(1 - K(\overrightarrow{x_i}, \overrightarrow{x_j})\right) \quad (2.7)$$

Where the $K(\overrightarrow{x_i}, \overrightarrow{x_j})$ is the Gaussian Kernel function as it is good accuracy in linear and polynomial kernels classification. The Gaussian function is:

$$K(\overrightarrow{x_i}, \overrightarrow{x_j}) = e^{-\frac{\|\overrightarrow{x_i} - \overrightarrow{x_j}\|^2}{2\sigma^2}}, \sigma > 0 \quad (2.8)$$

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2.3 REVIEW OF RELATED PREVIOUS WORK

Anomaly Detection is classified the anomaly detection into two main categories, which is the self-learning anomaly detection and the programmed anomaly detection. The self-learning category is further breakdown into cognition based anomaly detection, computation intelligent, data mining method and machine learning based anomaly detection. While the programmed anomaly detection is divide to a simple rule-based and the statistical based.

The main concern in this research is the machine learning based anomaly detection as mentioned in Chapter 1. The machine learning based anomaly detection is further separate into few more category, which are: Bayesian Network method that use the directed acyclic graph that indicate dependencies between the child node and parent node with associated conditional probabilistic tables [26, 31]; Generic algorithm that use the principle of genetic and natural selection to detect anomalies and allows evolution of certain population under specified selection rules to maximise the fitness value [32]; Fuzzy logic that capable to calculate and make decision with presence of only ambiguous information [33]; Support Vector Machine that develop a hyperplane that produce maximum size of separating margin between the normal and anomaly classes [31, 34]; Artificial Neural Network (ANN) that going to explain in Section 2.3.1.

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

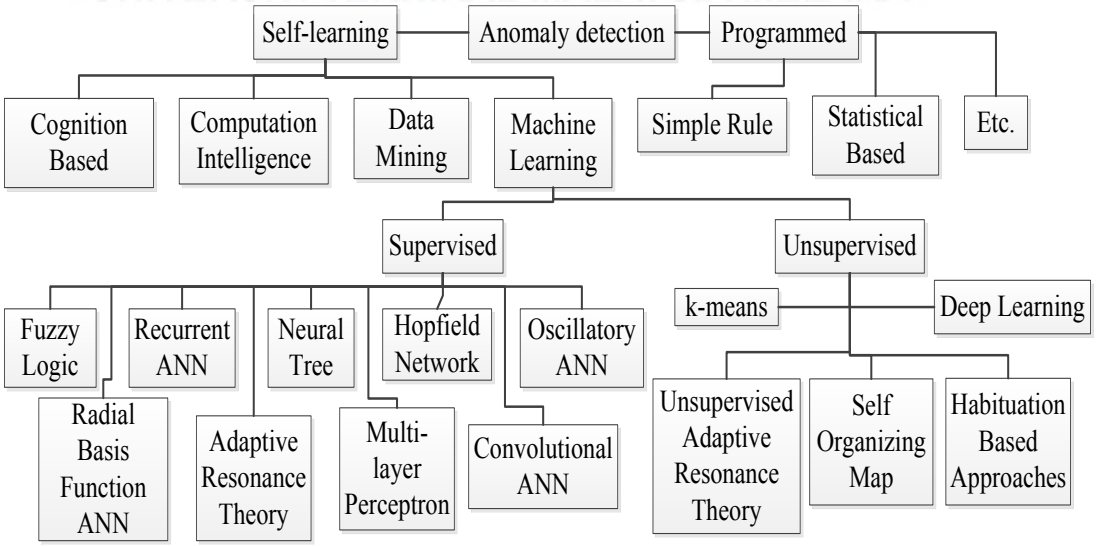

Figure 2.6: Classification of the anomaly detection technique

2.3.1 Artificial Neural Network (ANN)

ANN is defined a group of interconnected neurons that learn useful linear and non-linear tendencies in complex data from their environment [35]. Haykin [36] define ANN as a parallel-dispersed processor that has a natural tendency for keeping empirical knowledge and making it available for use. It imitates the brain in the aspect that knowledge is obtained by the network through the learning process and store the knowledge in synaptic weight (interconnection between neurons).

The ANN-based anomaly detection is further divided into two categories based on the need of training data in the application, which is the supervised ANN anomaly detection and unsupervised ANN anomaly detection.

Multilayer feed-forward neural network, known as multilayer perceptron (MLP) network is one type of the supervised ANN. Callegari et al. [37] used the MLP architecture for the Intrusion Detection System (IDS). Threshold-based evaluation and common decision making with various aggregates are used for the attacks or anomalies identification. The performance of the algorithm is evaluated based on the false positive rate, false negative rate and convergence speed. Convolutional ANN (CNN) is the type of supervised feed-forward ANN that has a different combination of the convolutional layer, average-pooling layer and local correlation behaviour by enhancing the interconnectivity of neurons. Li et al. [38] combine CNN with deep learning method to detect the outlier in the hyperspectral imagery. The algorithm is the first to train with the reference data and then determine the anomalies with a dual-window strategy that assumes the presence of an anomaly is rare and most of the data are normal. The performance of the algorithm determines the use of ROC for the quantitative assessment.

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

Backpropagation ANN (BPNN) consists of input layer, hidden layer and output layer and been widely used due to the simplicity, ease of use and strong capacity of the method. Radial Basis Function ANN (RBFNN) is a three-layer network where the hidden layer consists the radial basis function and less vulnerable to moving inputs. Lokman and Yilmaz [39] made a fusion of BPNN and RBFNN for the use target recognition and anomaly detection in HSI for unmanned aerial vehicles. Multi-layered ANN is used where the ANN-1 for the anomaly detection and ANN-2 for target recognition. The binary number is used as the output. The performance of the algorithm is evaluated through the amount of true positive and false positive detected.

Recurrent ANN (RNN) allows the output of hidden layer feedback and acts as the input to the hidden layer that makes the network able to understand the chronological nature of data through the past result. Nanduri and Sherry [40] use RNN to detect the anomalies in the aircraft data. The performance of the method is evaluated through the precision, recall rate and F1 score of the algorithm. RNN more suitable in handle multivariate time series data and more delicate to short-term outliers.

The main concept of the deep learning is unsupervised machine learning, AI and multiple layers. The deep learning can use for both supervised and unsupervised, or even hybrid mode which is semi-supervised based on the application. Example of unsupervised deep learning is Deep Boltzmann Machine (DBM), Restricted Boltzmann Machine (RBM), Deep ANN (DNN) and Deep Belief Network (DBN). Kwon et. al. [41] compare the performance of DBM, RBM, DNN and DBN on the IDS. The four method tests using the KDDCup 1999 and NSL-KDD data test. The performance of the method is evaluated via the accuracy, precision, recall and F1 score of the method on the test data.

2.3.2 Self-Organizing Map (SOM)

SOM, also known as Self-Organizing Feature Map or Kohonen Network is introduced by Kohonen in 1988. This method is unsupervised and hence no prior information on the data label of samples is required [20]. In SOM, the winner neuron and neurons that neighbourhood to the winner adjusts the weight vector together to ensure the sensitivity of neighbourhood neuron to a specific input. This feature helps the topology preservation of the inputs that ensure the organized region is similar in nature and spatial proximity to each other [35].

Kohonen [42] propose single layer neurons to the input layer of branching nodes. The neural layer contains neurons that have parametric weight vector, $v^{(m)}$, which same as the input vector, $x^{(q)}$. The weight vector is first randomly initialized and then calculate the square distance of the $v^{(m)}$ and $x^{(q)}$ using the equation:

$$D_{qm} = D_{qm}\left(x^{(q)}, v^{(m)}\right) = \sum_{(n=1,N)} \left(x_n^{(q)} - v_n^{(m)}\right)^2 \qquad (2.9)$$

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

The minimum value determines the winner neuron. The weight vector of the winning neuron is updated via the equation:

$$v^{(m^*)} = v^{(m^*)} + \eta\left(x^{(q)} - v^{(m^*)}\right) \quad (2.10)$$

where η is the learning rate.

Lateral inhibition, also known as "Mexican sombrero" can be used for SOM clustering by reinforcing the winning neuron and the neighbourhood of winning neuron and extinguish the neuron that further away from the winning neuron. The reinforcement region is reduced steadily over the iterations [43].

SOM does not depend on the input space and efficient in handling the large dataset as the ability of SOM to convert the high-dimensional data into low-dimensional simple data group. However, SOM is not able to provide the precise clustering result, fixed number and arrangement of the neurons in the SOM architecture that lead to the possibility of drastic dimension reduction and generation of folded SOFM and the lack of interpretability of the trained SOM. SOM is a good technique for a detect anomaly in huge data, thus disadvantages of SOM are overcome via the improvement on SOM or fusion to other anomaly detection technique.

Lee et al, [44] propose the combination of SOM and k-means clustering to overcome the disadvantages of SOM. K-means clustering is effective in process large data and widely used due to its simplicity, low time complexity and fast convergence, but it depends seriously on the initial value set which is the patterns and synaptic weight of the data set and the difficulty to find the centre of the cluster. The proposed method is used for the IDS. The method is tested on the offline model and the online model by using the KDDCup 1999 dataset. The performance is evaluated on detection rate and the false positive rate. The proposed method is discussed based on the time overhead, intelligent knowledge overhead and degree of automation and resulted in the increase of detection rate until 96.6% and decrease the false positive rate till 13% and allows the prediction on the occurrence in the new attack. The same method also used in the Huai-bin et al. [45] for IDS. SOM is used to determine number of clusters and the k-means to refine the final SOM topology. The method also achieved 92% detection rate and 35% false positive rate, but only applicable to three type of attacks.

Tian et al. [46] recommend SOM based k-nearest neighbour algorithm that used to detect anomalies in PHM of the mechanical and electronic system to predict the possible failure of the system. The proposed method is semi-supervised where the method is trained by SOM to get the BMUs and acts as healthy references for the k-

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

nearest neighbour algorithm. The algorithm aims to reduce the influence of the noise in the data and resulted in the algorithm is applicable to the non-convex data.

Zhang et al. [47] propose unsupervised periodic SOM (PSOM) for the anomaly detection for periodic and aperiodic time series data. The performance of the algorithm is evaluated through the false positive rate, true positive rate and the ROC curve. The algorithm results in the high accuracy in one-dimensional data and correlated multi-dimensional data, but the PSOM need to properly set the number of row in advance.

Siripanadorn et al. [48] propose the combination of SOM and discrete wavelet transform (DWT) that have time-frequency localization property for signal and multi-resolution representation for detecting the anomalies in a wireless sensor network. DWT is used as the pre-processor and SOM as data size reduction and anomaly detection. The performance of the algorithm is determined using true alarm rate and false alarm rate. The algorithm resulted in an acceptable accuracy of detection rate, which is minimum of 65% and a maximum of 80%.

Shahreza et al. [49] propose the anomaly detection that combines SOM and particle swarm optimization (PSO) that is effective in solving nonlinear optimization and easy implementation. The algorithm is used on a case study on forest fire detection. The method updates the weight vector of SOM by using PSO. The method has low time and space complexity, applicable to various domain anomaly detection and is unsupervised anomaly detection. The performance of the algorithm is evaluated with false positive rate, false negative rate, Huang's accuracy measure and Ward's minimum-variance. The proposed method have 83.2% accuracy on real data and 99% on simulated data, which is more accurate than the original SOM, Bayesian estimation and Dempster-Shafer anomaly detection.

Liu et al. [50] proposed a SOM-based anomaly detection algorithm for the virtual machine in cloud platform. The virtual machines are partition based on the similarity to reduce need and time for SOM modelling. The performance of the algorithm is determined based on the detection accuracy. The detection accuracy is tested on different SOM net size, initial training neighbourhood size and initial learning rate. The bigger SOM net size, larger initial training neighbourhood size and higher initial learning rate resulted in higher detection accuracy that reached until 97.5%. The proposed idea resulted in high accuracy on detecting the failure in a virtual machine of cloud platform compared to a k-nearest neighbour and cluster-based anomaly detection and fast training speed.

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

Habituating SOM is proposed by Miskon [51] by linking the neuron to output via a habitable synapse to detect the anomaly in the certain area via mobile area. The performance of the algorithm is evaluated in term of the sensitivity of the algorithm. The method proposed has the limitation in finding BMU that even poor match become BMU. Spatial habituating SOM is introduced by Miskon et al. [52] to allow the continuous learning and adaption to change in the situation by apply habituation principle that considers spatial information. The algorithm is used for the underwater pipe and cable inspection application. The algorithm is tested on different learning rate.

Growing Hierarchical SOM (GHSOM) is the improvement of SOM that the model is a hierarchical structure with different layers to overcome the disadvantages of SOM. Emiro et al. [53] apply GHSOM to detect the anomalies in IDS. The algorithm is tested with the KDDCup 1999 and the performance of the algorithm is tested using the detection rate, false positive rate and the ROC curve of the algorithm. The algorithm resulted in high detection rate which is 99.2%. Chiu et al. [54] used GHSOM to cluster and detect the malware in the big data environment. The research resulted in the possibility of using k-means with a random number of the cluster might make the presence of a useless cluster. False positive rate and false negative rate are used by Chiu for the performance evaluation. The proposed method resulted in low false positive rate and false negative rate. GHSOM is useful in the map size reduction and provides a detail view of the complicated clustering task. The number and size of the layer are determined during the training phase and the training is faster. Although the training is fast, GHSOM requires time to obtain a result and have limited visualisation on the result as well as the limitation on static topology where unnecessary neuron occurs in some case.

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

Albayrak et al. [55] proposed the combining SOM algorithm for a robust and scalable IDS that combine Scalable SOM (SSOM), Hierarchical SOM, GHSOM, Growing Grid SOM (GGSOM), original SOM and Growing Neural Gas (GNG). The proposed method aims to reduce training cost in order to cope with the real-time situation. The selection of operating SOM algorithm depends on the rules set such as the number of zero elements, number of features, memory resources, processor resources, level of importance for the node, the need of visualisation. SSOM is used when the zero-elements is more than 40% and no limitation on memory. Otherwise, SSOM with compressed vectors is used. Original SOM is used when the features are less than 10. Otherwise, if features are more than 500 or limited memory resources or

no need visualization, then Hierarchical SOM is used. Furthermore, if no limitation on memory and limited resources in CPU, then GHSOM is used. Additionally, if the high importance of node, then the original SOM is used. Fast winner search technique is used whenever real-time processing is important. The method resulted in the optimization on the training cost without abandon the accuracy of anomaly detection.

Table 2.1: Summary on anomaly detection technique

Method	Nature of CPS	Attribute of anomaly	Advantages	Disadvantages
SOM	• Virtual machine anomaly detection	• Point anomalies	• Does not depend on the input space • unsupervised learning • Efficient in handling large datasets • Transform high-dimensional data into simple group of data with low-dimension	• Cannot provide precise clustering results • Fixed network architecture • Drastic dimension reduction • Generate folded feature map • Lack of interpretability of trained SOM
k-means	• Network intrusion detection	• Point anomalies	• Process large data effectively • Simple, low time complexity • Fast convergence	• Depend seriously on initial value Difficult to find centre of cluster
Hierarchical SOM	• Network intrusion detection	• Point anomalies	• Useful in reducing map size	• Need to determine threshold that

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

			• Faster in training SOM	creates child SOM
GGSOM	• Intrusion detection	• Point anomalies	• Unnecessary predefined SOM's size	• Obtain uneven growth of map
GHSOM	• Network intrusion detection	• Point anomalies	• Useful in reducing map size • Provide detail view on complicated clustering task • Determination of number and size of layer during training phase • Faster training	• Require time to obtain result • Limited visualisation
SOM + k-means	• Network intrusion detection	• Point anomalies	• Increase detection rate • Increase false positive rate	• Only can detect 1 type of intrusion
PSOM	• Periodic time series • Aperiodic time series	• Point anomalies	• No labelled training data required to capture normal data patterns • Applicable to multi-dimensional data	• Only applicable to time series dataset • Needs to set number of rows in advanced properly

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2.4 SUMMARY

The basic theory on the anomaly detection such as the type of detection, type of anomalies and others is studied. The application of SOM on the previous work is reviewed. Most of the anomaly detection is applied in the field of IDS, fraud detection and system failure prediction. The advantages and limitation of the present type of SOM are summarised. The methods and parameter used for the performance determination are reviewed. Most of the work determined their algorithm based on the detection rate, false positive rate, accuracy and ROC curve. In order to fulfill the requirement of I4.0, the detection rate and accuracy of the algorithm are important. Hence, the SOM+k-means is used for the project implementation. The disadvantages that only can detect one type of intrusion can solve by implementing the threshold mechanism to the data. To overcome the problem due to a large amount of data, Habituating SOM is used as good in reducing map size and faster training. Therefore, the proposed idea is a fusion of the two methods, Habituating SOM+kmeans.

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

CHAPTER 3

RESEARCH METHODOLOGY

3.1 INTRODUCTION

The chapter described the methodology that is being used throughout the research in order to achieve the research objective in the research. The chapter provide the guide on the way for implementation of proposed method to the research.

First, the chapter discussed the proposed research methodology for the research application through the flowchart shown in Figure 3.1 and then follow with the brief explanation on the flow of the proposed method, theory or principle that involved in the proposed idea and the equation that involved in the algorithm completion. The technique for the system to detect the anomaly is discussed further in the chapter.

Next, the chapter also describe the methods used for analyzing the performance of the algorithm. Lastly, few of experiments is proposed to validate the performance of the designed algorithm. The objective and the experimental set-up for the proposed experiments also described in the chapter.

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

3.2 PROPOSED RESEARCH METHODOLOGY

The proposed research methodology is the habituating SOM with the implementation of k-means as mentioned in the Section 2.4. Hence, the flowchart is created on behalf the proposed method to provide a glance on the proposed method and make the operation of the method become clearer as well as for the ease of design algorithm.

Habituation SOM is a neural network based anomaly detection algorithm that can be easily adapt to new environment. Little number of runs is enough for the mechanism to learn new pattern. The application and functionality of Habituating SOM is proven in Miskon et.al. [51, 52]. The flows for the operation of the designed algorithm is shown in Figure 3.1.

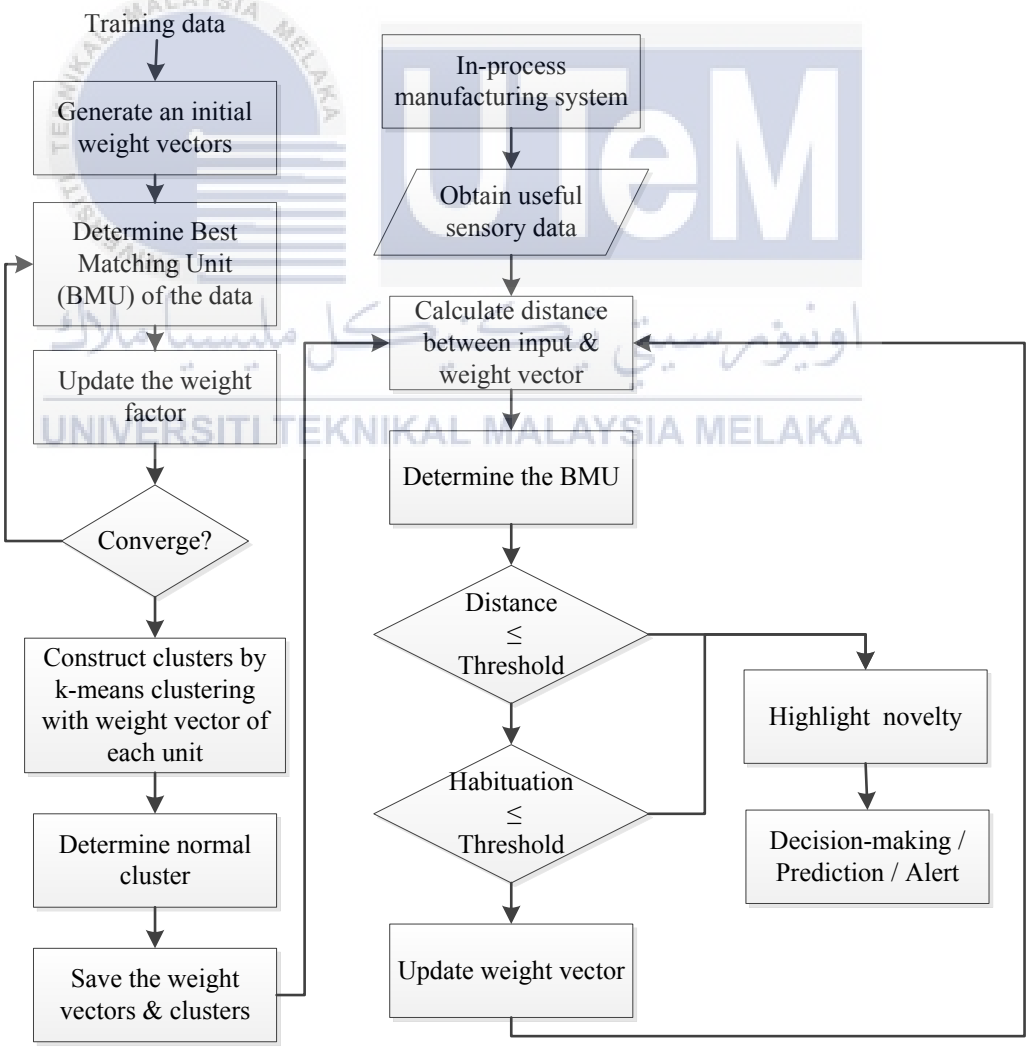

Figure 3.1: Flowchart of the proposed method

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

3.3 DISCUSSION ON PROPOSED METHODOLOGY

The proposed anomaly detection that based on the Habituating SOM with implementation of k-means clustering. In the proposed method, the SOM and k-means act as the clustering network for the mechanism, while the habituation function take role as set of habituating synapses that form connection among the network neurons to the output as shown in Figure 3.2.

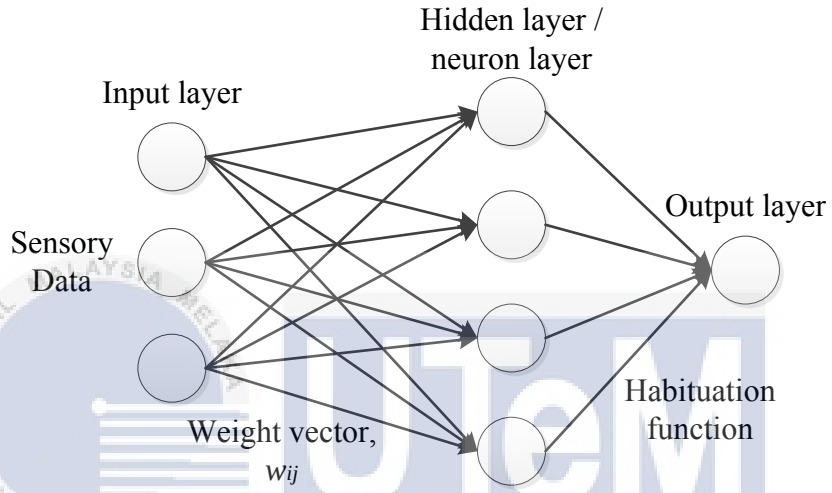

Figure 3.2: The simple layout of the Habituating SOM

The weight vector need to be initialized beyond the clustering process. If the weight vectors are not initialized properly, the network will need longer time to produce the result. Besides, the performance of SOM greatly depends on the initialization of the weight vector for the data. Hence, the weight vector for the neurons is initialized via k-means clustering mechanism to ensure reasonable number of cluster and proper distribution of weight vector.

1 *initialize* $\mathbf{m}_k$;
2 **repeat**
3 | Assign each data point to its closest cluster center: $z_i = \arg\min_k ||\mathbf{x}_i - \boldsymbol{\mu}_k||_2^2$;
4 | Update each cluster center by computing the mean of all points assigned to it: $\boldsymbol{\mu}_k = \frac{1}{N_k} \sum_{i:z_i=k} \mathbf{x}_i$;
5 **until** *converged*;

Figure 3.3: The procedure of the k-means clustering [45]

SOM clustering is used after the initialization of SOM. There always have three key assumptions that need to be made when detect the anomalies using the clustering mechanism, which are [44, 25]:

- Any new data that implement into the algorithm is considered as an anomaly if the data cannot fit well with the existing clusters of the normal data when cluster only have normal data.
- The normal data instances is lies close to the centre of nearest clusters, while the anomalies outlying far away from the nearest clusters centroid when the cluster consists of normal data and anomalies. Distance score is used to detect the outliers.
- From the clusters that have different size, the normal data is appeared in big and dense clusters, while the small or sparse size of cluster can considered as outliers. Hence, the new instance that belong to the cluster size and density below threshold is considered as an anomaly.

Hence, the assumptions need to be made in order to succeed in detect the anomalies.

When new input, i, is implement to the algorithm, the distance of i with every neuron in the hidden layer, j is calculated via Euclidean distance measure, d_{ij} as mentioned in Section 2.2.4 that shown in Equation (3.1) where v_i is the input vector, w_{ij} is weight vector of neuron, t is the number of iteration.

$$d_{ij} = \sqrt{\sum_{i=1}^{N} \left(v_i(t) - w_{ij}(t)\right)^2} \quad (3.1)$$

The neuron with minimum Euclidean distance measurement, $d_{ij(min)}$ is choose as the winning neuron, or known as Best Matching Unit (BMU), w_{ij}^*. The weight vector of the BMU, $w_{ij}^*(t+1)$ is then updated via Equation (3.2) where $\eta(t)$ is the learning rate and $\vartheta(t)$ is the neighbourhood strength function.

$$w_{ij}^*(t+1) = w_{ij}^*(t) + \eta(t)\vartheta(t)\left(v_i(t) - w_{ij}^*(t)\right) \quad (3.2)$$

Neighbourhood strength function, $\vartheta(t)$ and learning rate function, $\eta(t)$ control the adaptation of the weight vector of BMU in order to ensure the topology preservation of the SOM. $\vartheta(t)$ determine the influences of BMU to its neighbourhood and the way that the weight adaptation decays with distance from the winner [35]. $\vartheta(t)$ is in the Gaussian form to ensure the smoothness of decay between the weight adjustment and distance as given in Equation (3.3) where σ is the neighbourhood radius and d is the distance between winning neuron and other neuron.

$$\vartheta(t) = e^{-\frac{d^2}{2\sigma^2}} \quad (3.3)$$

The neighbourhood radius also shrinking over the iteration in order to stabilise the network. Smaller initial neighbourhood can resulted in the metastable status correlate to local minima. Therefore, a larger initial neighbourhood is required for initial clustering. The decay of the neighbourhood size also in the form of exponential as given in Equation (3.4) where σ_o is initial neighbourhood radius, σ_t is the neighbourhood radius at iteration, *t*, while *T* is the constant to allow the function decay to zero with iterations.

$$\sigma_t = \sigma_0 e^{-\frac{t}{T}} \quad (3.4)$$

The value of $\vartheta(t)$ depends on the similarity of BMU to nearby neuron. The increase in the similarity of BMU to nearby neuron resulted in the increase in the value of $\vartheta(t)$. The similarity of BMU to nearby neurons, d also determine via Euclidean distance as shown in Equation (3.5) where w_{ij}^* is the weight vector for BMU and w_{ij} is the weight vector of other neurons except BMU.

$$d = \sqrt{\sum_{i=1}^{N} \left(w_{ij}(t) - w_{ij}^*(t)\right)^2} \quad (3.5)$$

The learning rate, $\eta(t)$ also decay with the iterations. [35] suggest to start with a higher learning rate and decreased gradually based on the Equation (3.6) where η_0 is initial learning rate factor, $\eta(t)$ is the learning rate factor at iteration, *t*, while *T* is the constant to allow the function decay to zero with iterations., but stay at or above 0.01.

$$\eta(t) = \eta_0 e^{-\frac{t}{T}} \quad (3.6)$$

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

The SOM converts to Habituating SOM by connect the neurons in hidden layer to the output via habitable synapse. The synapse adjusts when the respective neuron become BMU. Marsland [56] found that the habituation behaviour can be simulated via a curve that decay gradually as the number of insights increases. Hence, an exponential function is used for the habituation of synapse as stated in Equation (3.7) where *o* indicate the times of the neuron become BMU and T_2 is is the constant that manages the rate of habituation.

$$\Upsilon_j(o) = e^{-\frac{o}{T_2}} \quad (3.7)$$

The input is consider as anomalies when it does not match any neuron in hidden layer within the allowed distance threshold or the habituation synapse, $\Upsilon_j(o)$ is larger compared to the allowed habituation threshold, h_T.

3.4 EVALUATION FOR PERFORMANCE

The outcome from algorithm can be positive (anomaly is present) or negative (anomaly is absent), while the actual outcome may resulted in different answer in the experiment. The parameter for performance evaluation is define as the following:

- True positive (TP): Situation that an anomaly is present is correctly observed as an anomaly is detected.
- False positive (FP): Situation that an anomaly is absence is incorrectly observed as an anomaly is detected.
- True negative (TN): Situation that an anomaly is absence is correctly identified as no anomaly is detected.
- False negative (FN): Situation that an anomaly is present is wrongly observed as no anomaly is detected.

Table 3.1: Possible outcome for anomaly detection via confusion matrix

Anomalies?		**Actual**	
		Yes	No
Prediction	Yes	TP	FP
	No	FN	TN

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

Based on the confusion matrix and the parameter to determine performance, the performance measures as below can be carry out. The performance measures are given equation as below:

- Sensitivity/ True Positive Rate (TPR)/ Recall

$$TPR = \frac{number\ of\ TP}{number\ of\ TP + number\ of\ FN} \quad (3.8)$$

- Specificity (SPC)/ True Negative Rate (TNR)

$$SPC = \frac{number\ of\ TN}{number\ of\ TN + number\ of\ FP} \quad (3.9)$$

- Fall-out/ False Positive Rate (FPR)/ False Alarm Rate

$$FPR = \frac{number\ of\ FP}{number\ of\ TN + number\ of\ FP} = 1 - SPC \quad (3.10)$$

- Accuracy (ACC)

$$ACC = \frac{number\ of\ TP + number\ of\ TN}{number\ of\ TP + number\ of\ FP + number\ of\ TN + number\ of\ FN} \quad (3.11)$$

- Precision/ Positive Predictive Value (PPV)

$$PPV = \frac{number\ of\ TP}{number\ of\ TP + number\ of\ FP} \quad (3.12)$$

- F1 Score (Harmonic mean of precision and sensitivity)

$$F1 = \frac{2(number\ of\ TP)}{2(number\ of\ TP) + number\ of\ FN + number\ of\ FP} \quad (3.13)$$

- Matthews Correlation Coefficient (MCC)

$$MCC = \frac{TP(TN) - FP(FN)}{\sqrt{(TP+FP)(TP+FN)(TN+FP)(TN+FN)}} \quad (3.14)$$

Receiver Operating Characteristic (ROC) curve is a graphical plot to represent the analysis ability of the binary classifier by varying the threshold. ROC curve is the plot of sensitivity against false positive rate [57]. The sensitivity and specificity is greatly depend on the criterion value. If a high criterion value is selected resulted in the increase in specificity and decrease in sensitivity. The points in ROC curve indicate the sensitivity/specificity pair with respect to particular threshold. The overall accuracy of system can be determine through the distance of ROC curve to the top left corner of the graph. A ROC curve that passes through the upper left corner which is 100% sensitivity and 100% specificity indicate perfect discrimination that no intersection in the two distribution at respective threshold. Hence, the nearer the ROC curve to the upper left corner, the higher the overall accuracy for the algorithm [58].

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

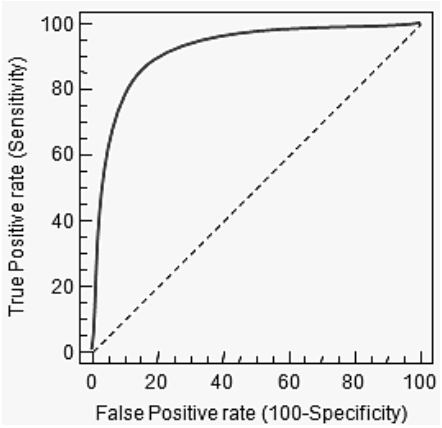

Figure 3.4: The representation of ROC curve [58]

3.5 DATA FOR ANALYSIS

The data used for the simulation and evaluating the performance of the designed algorithm was collected from the V-rep robot simulator. The application of the mini CPS was set to pick-and-place application as shown in Figure 3.5. The data collected from V-rep for the simulation was the initial position and the final position of the pick-and-place application of the robotic arm, linear velocity and angular velocity.

It was found that it is hard to have anomaly occur in the simulator, thus the anomalies that were present in the test data were created randomly. The random anomalies was ensure that it was within the working range of the robot manipulator. The simulated data set was attained using the following requirements:

- Tolerance and sensitivity is taken into account as real situation will not work in ideal condition and having deviation [59].
- Precision of sensor is taken into account as the sensory data that obtained from real situation will deviated even though the actual remain unchanged [59] .

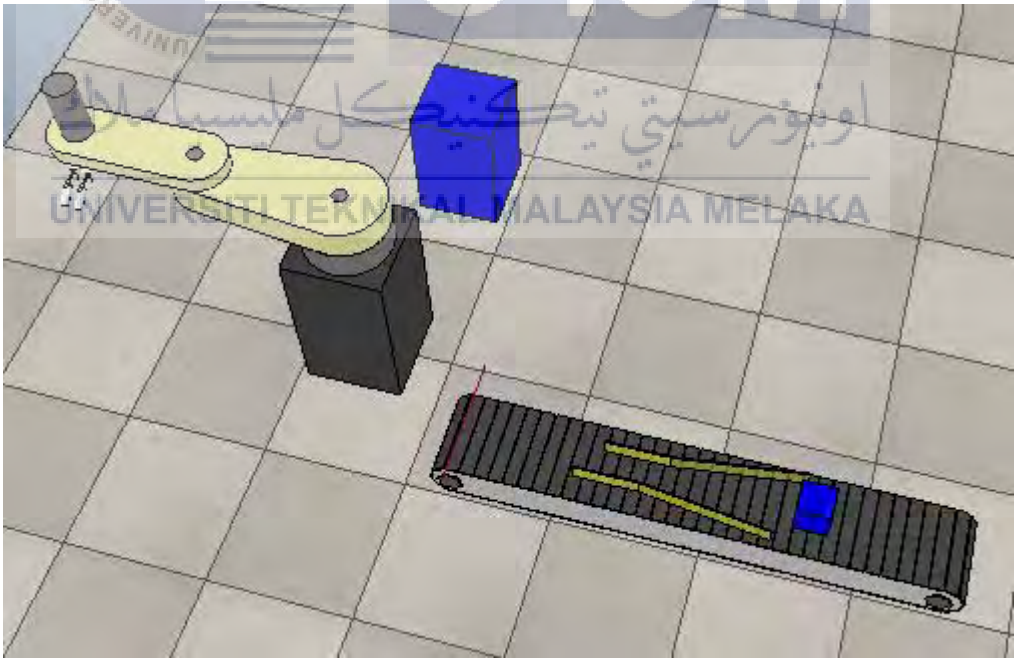

Figure 3.5: The pick-and-place application in V-Rep Robot Simulator

3.6 EXPERIMENT FOR ANALYSIS

3.6.1 Threshold optimization

The objective of the test is to determine the optimum value of Euclidean distance threshold, $d_{ij}^{\emptyset}$. The data used for the threshold optimization is the data that collected from V-rep simulator (1000 samples with 40 anomalies inserted), while the data collected from the test is the TP, TN, FP, FN at different threshold after the algorithm execution. The experiment is executed and analysed via Matlab as the algorithm is designed in the Matlab interface.

Table 3.2: The parameter setup for threshold optimization

Parameter	Setting
Learning rate, $\eta(t)$	0.01
Neighbourhood strength decay rate, $\vartheta(t)$	1.00
Habituation threshold, Υ_j	0.85

The data is inserted to the algorithm in Matlab for execution of program. The dataset is read row by row in order to fulfill the real-time situation. The algorithm is executed with starting threshold value of 0.0005 and follow by increment of 0.0005 until no anomalies are detected by the algorithm. The TP, TN, FP, FN after the execution of algorithm for the various Euclidean distance threshold are recorded. FPR and TPR is calculated based on the TP, TN, FP, FN by using Equation (3.8) and (3.10). The ROC curve is plotted based on TPR and FPR calculated. The curve is smoothed with the use of Matlab tool. The most suitable $d_{ij}^{\emptyset}$ is selected based on the ROC curve.

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

3.6.2 Accuracy analysis

The objective to run the analysis is to evaluate the performance of designed algorithm in term of accuracy. The data used for the test is the data collected from the V-rep robotic simulator that contains 1000 samples with different number of anomalies which is 10, 20, 30 and 40 anomalies are inserted randomly into the samples. The data that collected from the experiment is the number of TP, TN, FP, FN of the algorithm detected. The experiment is executed and analysed via Matlab as the algorithm is designed and programmed in the Matlab interface.

Table 3.3: The parameter setup for accuracy analysis

Parameter	Setting
Learning rate, $\eta(t)$	0.01
Neighbourhood strength decay rate, $\vartheta(t)$	1.00
Euclidean distance threshold, $d_{ij}^{\emptyset}$	0.056
Habituation threshold, Υ_j	0.85

The reasonable number of neuron and proper distribution of neuron weight is obtained via k-means clustering before the experiment started. The train and test using different data is used for the evaluation procedure. Before the execution of the algorithm with the test data that with anomalies inserted, the algorithm is first with the training data set that do not contain any anomalies. Then, the data that collected from V-rep simulator with 10 anomalies are inserted to the designed algorithm in Matlab. The dataset is read row by row in order to fulfil the real-time situation. After the execution of algorithm, the TP, TN, FP and FN in term of the anomalies detected by the algorithm. The experiment is then executed with the datasets with 20, 30 and 40 anomalies inserted. The accuracy of the designed algorithm on different number of anomalies in same number of dataset is calculated with the use of Equation (3.8), (3.11), (3.12), (3.13) and (3.14).

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

CHAPTER 4

RESULT

4.1 INTRODUCTION

This chapter discusses the result that obtained along FYP period. The test is run with the use of Matlab. The result obtained during the test are tabulated or plotted for the ease to analyse and discuss. The result obtained during the test is evaluated based on the confusion matrix and ROC curve.

4.2 RESULTS AND DISCUSSION

Based on the proposed method that had been discussed in Section 3.3, it is found that the performance of SOM greatly depends on the initialization of the weight vector for the algorithm execution. Hence, before the threshold optimization and the analysis on algorithm's accuracy, k-means clustering is first executed in order to obtained reasonable number of cluster and proper distribution of weight vector. 500 samples of the data that extracted from the V-rep robot simulator is used to run k-means clustering.

After the execution of k-means clustering, it is found that the reasonable number of neuron for the data set for simulation is 8 clusters with the neuron weight of 3.0001, 11.0005, 5.0028, 0.5019, 9.001, 4.001, 1.9978, 0.9984. The neuron weight is save as matrix file (w.mat) for the execution of the Habituating SOM algorithm to detect the anomaly.

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

4.2.1 Threshold optimization

After the execution of algorithm by varying the Euclidean threshold value, the TP, FP, TN and FN are evaluated based on the parameter discussed in Section 3.4 and recorded. The TPR and FPR are calculated based on the Equation (3.8) and (3.10). The ROC curve that plotted based on TPR against FPR is shown in Figure 4.1 that range of both axis from 0 to 1.

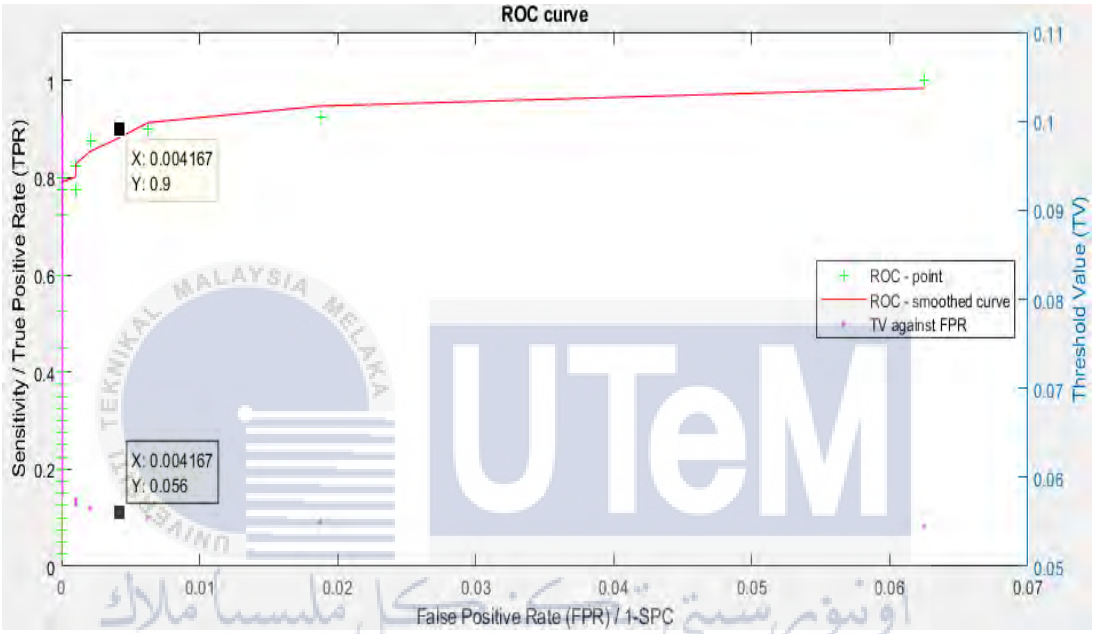

Figure 4.1: The ROC curve for threshold optimization

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

The nearer the Receiver Operating Characteristic (ROC) curve to the upper left corner and the larger the area under curve of ROC, the higher the overall accuracy for the algorithm [58]. Hence, it is found that the algorithm have relatively high accuracy as the area under curve of the ROC is relatively higher. Based on the result and ROC curve, maximum number of TP (TPR=0.004167) and minimum number of FP (FPR=0.9) is detected when the Euclidean threshold is 0.056. Hence, the optimum $d_{ij}^{\emptyset}$ is 0.056. When the $d_{ij}^{\emptyset}$is 0.056, the ROC curve is nearest to the upper left corner of ROC curve. Besides, the range of optimum $d_{ij}^{\emptyset}$ is among 0.056 to 0.0564. Although there is an allowable range, but the minimum value is selected in order to avoid possibility of anomalies that located near to the normal instances cannot be detected and ensure the accuracy and sensitivity of the algorithm.

4.2.2 Accuracy analysis

The anomalies detected by the algorithm in the Test Dataset 1 (1000 samples with 10 anomalies) is shown in the Figure 4.2.

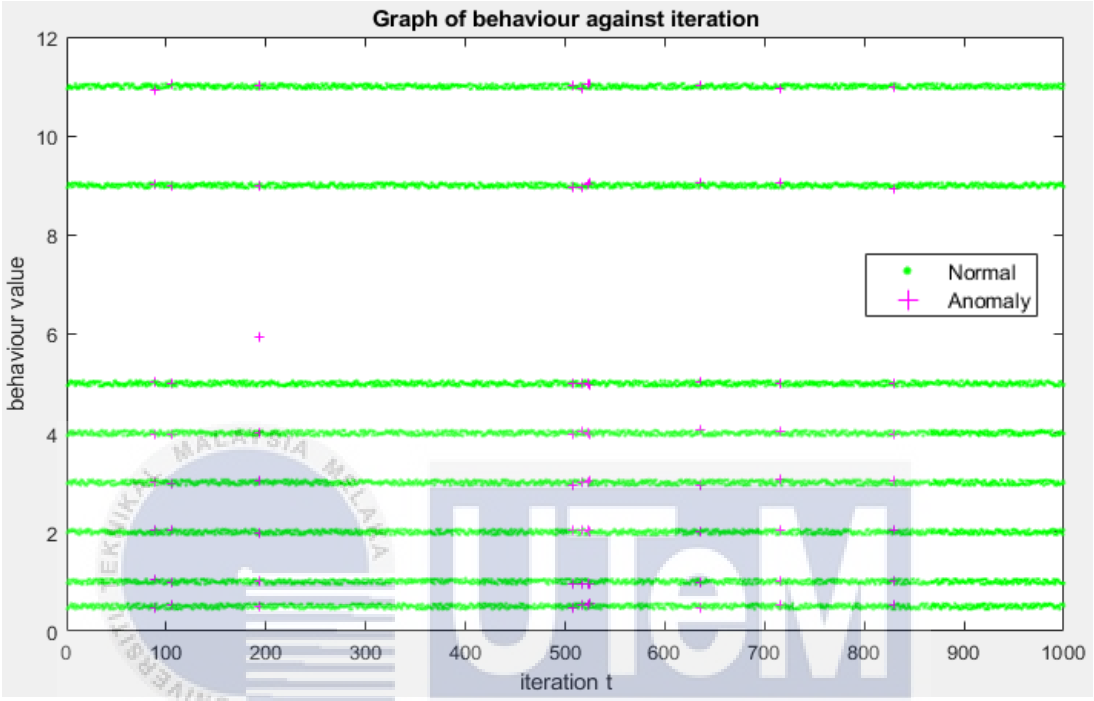

Figure 4.2: Graph of behaviour against iteration for 10 anomalies.

اونيۏرسيتي تيکنيکل مليسيا ملاک
UNIVERSITI TEKNIKAL MALAYSIA MELAKA

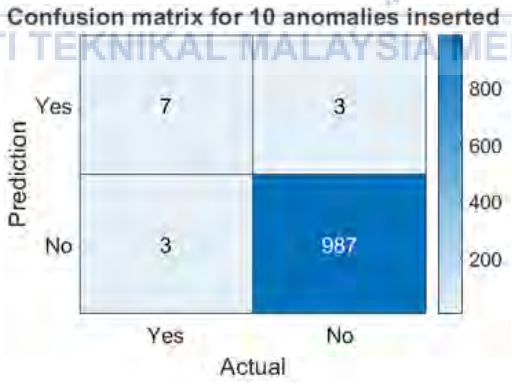

Figure 4.3: The confusion matrix for 1000 samples with 10 anomalies inserted

From Figure 4.2 and 4.3, it is found that 10 anomalies are detected by the algorithm, but among them only 7 of them are true anomalies. Rest of the anomalies detected by the algorithm is the normal behaviour that should not be identified as anomalies by the algorithm. This situation occurs due to the d_{ij} greater than $d_{ij}^{\emptyset}$.

The anomalies detected by the algorithm in the Test Dataset 2 (1000 samples with 20 anomalies) is shown in the Figure 4.4 with a marker '+'.

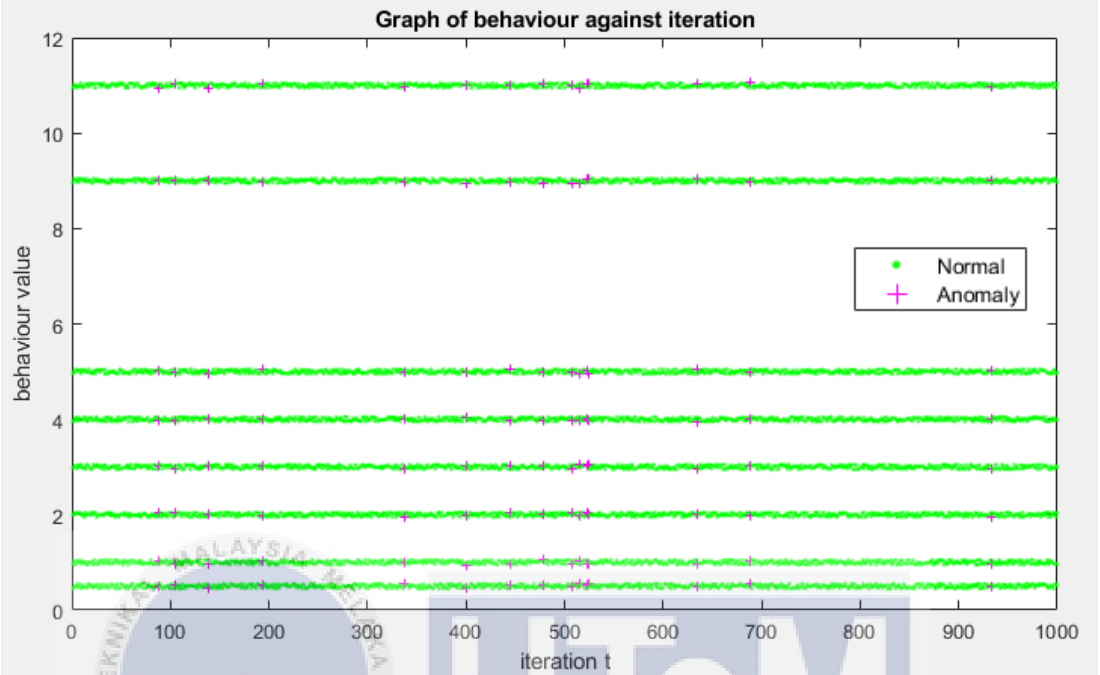

Figure 4.4: Graph of behaviour against iteration for 20 anomalies

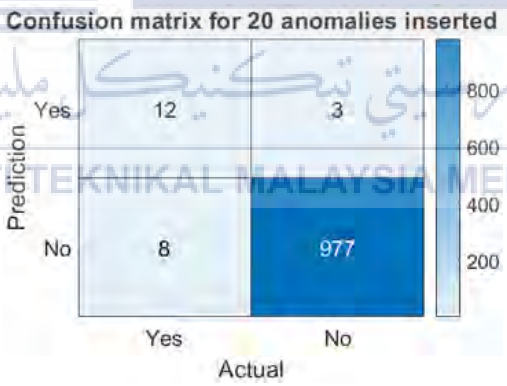

Figure 4.5: The confusion matrix for 1000 samples with 20 anomalies inserted

From Figure 4.4 and 4.5, it is found that only 15 anomalies are detected by the algorithm and only 12 of them are true anomalies. 8 true anomalies are identified as normal instances by the algorithm as the Euclidean distance of the current reading with neuron is lesser than the threshold value. The number of anomalies that identified by the algorithm as normal behaviour in Dataset 2 is greater compared to Dataset 1.

The anomalies detected by the algorithm in the Test Dataset 3 (1000 samples with 30 anomalies) is shown in the Figure 4.6. The anomalies is randomly put in the 1000 samples for the algorithm execution.

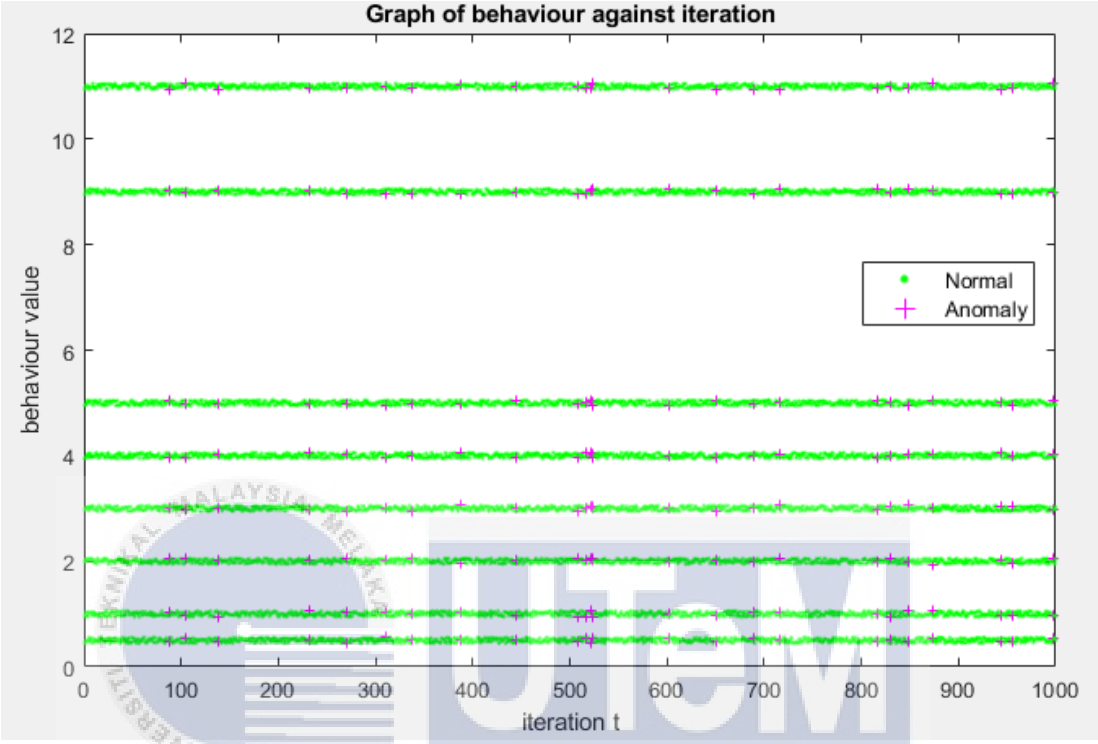

Figure 4.6: Graph of behaviour against iteration for 30 anomalies.

اونيۏرسيتي تيکنيکل مليسيا ملاک
UNIVERSITI TEKNIKAL MALAYSIA MELAKA

Figure 4.7: The confusion matrix for 1000 samples with 30 anomalies inserted

From Figure 4.6 and 4.7, 25 samples are detected as anomaly by the algorithm and only 20 of them are true anomalies. 10 true anomalies are identified as normal instances by the algorithm. This situation happened due to the Euclidean distance of the current reading with neuron is lesser than the threshold value.

The anomalies detected by the algorithm in the Test Dataset 4 (1000 samples with 40 anomalies) is shown in the Figure 4.8. 40 samples in the dataset are altered as anomalies for the algorithm execution.

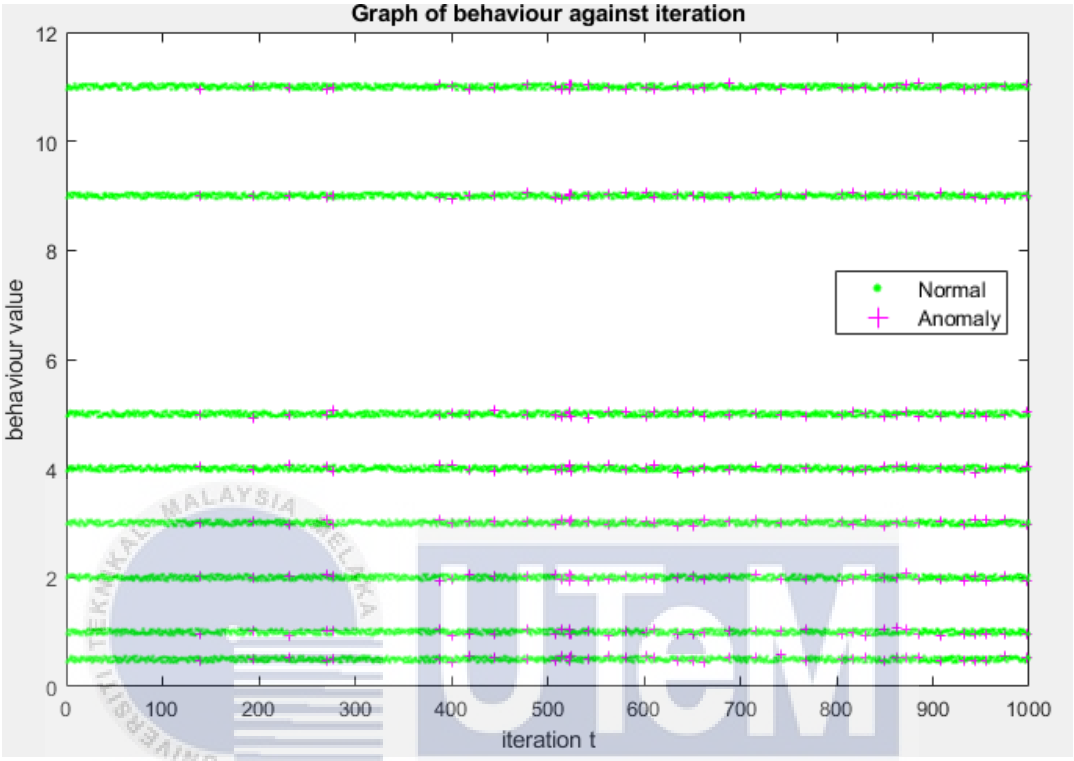

Figure 4.8: Graph of behaviour against iteration for 40 anomalies

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

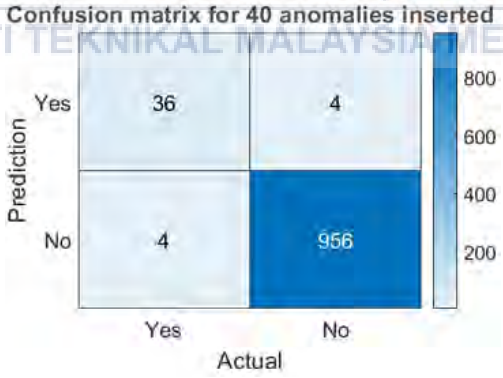

Figure 4.9: The confusion matrix for 1000 samples with 40 anomalies inserted

From Figure 4.7 and 4.8, 40 samples are detected as anomaly by the algorithm. Among the 40 anomalies detected by the algorithm, 36 of them are true anomalies and only 4 true anomalies are identified as normal instances by the algorithm. The detection rate on true anomalies in Dataset 4 is higher compared to other dataset.

The accuracy of the algorithm in detecting anomalies is calculated based on the confusion matrix in Figure 4.3, 4.5, 4.7 and 4.9 with the use of Equation (3.8), (3.11), (3.12), (3.13) and (3.14) that had been discussed in Section 3.4. The confusion matrixs is tabulated in order to give a clear view on the accuracy of the algorithm.

Table 4.1: Tabulated data for the accuracy analysis

Test Data	Anomaly Inserted	Anomaly Detected	TP	FP	TN	FN	ACC (%)	F1 Score	TPR	PPV	MCC
1	10	10	7	3	987	3	99.4	0.7	0.7	0.7	0.7
2	20	15	12	3	977	8	98.9	0.7	0.6	0.8	0.7
3	30	25	20	5	965	10	98.5	0.7	0.7	0.8	0.7
4	40	40	36	4	956	4	99.2	0.9	0.9	0.9	0.9

Dataset 3 have the lowest accuracy which is 98.5%. This situation may due to the implementation of anomalies that too close to the normal behaviour that lead to the identification of the anomalies to normal behaviour by the algorithm. But by implement the anomalies that close to the normal instances can prove that the algorithm can still detect the anomaly in the harsh situation such as anomalies that close to the normal behaviour. From Table 4.1, the algorithm reached highest accuracy when the anomalies inserted is minimum and start to decrease when the number of anomalies increases. But the accuracy of the algorithm increased back to 99.2% when the number of anomalies increased to 40.

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

Anomaly detection always deal with the imbalanced data as the anomaly is rare to be happen in CPS. Imbalanced data refer to the classes that are not characterized equally where the ratio of minority class to majority class is unequal and the event rate is less than 5% [60]. Hence, the accuracy only replicating the underlying class distribution as most of the data belong to the majority classes.

Jason [61] recommend that precision (PPV), recall or TPR and F1 score is more suitable to evaluate the performance of the algorithm and give more vision into the accuracy of the model. PPV and TPR refer to the ratio of a classifier exactness and completeness respectively, while F1 score define as harmonic average of PPV and TPR. The performance of algorithm is best when the F1 score is 1 and worst at 0. The measurements are used for imbalanced data performance evaluation as the measurement do not take into account the TN. From Table 4.1, it is found that test data set 1 have the lowest PPV and TPR which is 0.7, while test data have the highest PPV

and TPR which is 0.9. But when it comes to the F1 score, the test data set 1 to 3 share the same value which is 0.7, while test data 4 still have the highest F1 score which is 0.9. The result show that the designed algorithm can handle and detect the anomaly in the data set with higher number of anomalies.

Chicco [62] state that MCC is more suitable in evaluating the binary classification problem such as imbalanced data compared to other confusion matrix measures as it carries more information and take into account the balance ratio of TP, TN, FP and FN. The algorithm is in worst performance when MCC is -1 and perfect performance when MCC is 1. From Table 1, the MCC for the first three test data is 0.7 and highest for test data 4 which is 0.9. The 0.7 to 0.9 MCC indicate that the designed algorithm can detect the anomalies accurately and means that the algorithm is working well on both the positive and negative basics. Besides, it is found that both the F1 score and MCC share the same score for every data set.

Overfitting is commonly happened in the imbalanced data classifier. If the previous data of CPS is given with the presence of anomalies, resampling the data set for the training of algorithm is recommended to balance the classes in the training data in order to give the algorithm more insight to the upcoming data and ensure wider application of algorithm. Resampling divided into under-sampling that eliminating common examples and over-sampling that replicating minority [60]. Besides, if k-fold cross-validation is used for the training of algorithm, it is better to be done before the over-sampling of data to avoid the overfitting of algorithm to specific synthetic bootstrapping result [63].

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

4.3 SUMMARY

The designed algorithm is able to detect the anomaly in the data set accurately with the accuracy of minimum 98.5%. The designed algorithm have minimum 0.7 of F1 score and MCC that indicate that the algorithm have relatively high exactness and completeness. Threshold plays important in the designed algorithm, thus the threshold optimization is important in order to ensure the accuracy of the algorithm. In order to increase the accuracy of algorithm, the Euclidean threshold can be set to a value with more decimal place. Besides, the neuron weight initialization also play important role to ensure the shortest processing time for the execution of algorithm.

CHAPTER 5

CONCLUSION AND FUTURE WORK

5.1 CONCLUSION

In conclusion, the failure in the machinery is very dangerous and harmful to either the worker or the business itself. Therefore, this project is to design an anomaly detection algorithm to be implement to CPS with the use of SOM. Review from other previous work on anomaly detection is important in order to have a glance on the method that the previous work used and understand the theory and principle for the anomaly detection execution. The reviews had been summarised. The suitable method to implement to design the anomaly detection algorithm for CPS environment is selected, which is Habituating SOM with k-means clustering. The process is follow with the designation of algorithm based on Matlab software. K-means clustering used for cluster and neuron weight optimization while SOM for anomaly detection. It can be concluded that the anomaly detection algorithm that designed based on Habituating SOM can detect the anomalies accurately with the minimum accuracy of 98.5% and minimum F1 score and MCC of 0.7. Threshold optimization and neuron weight initialization is important in the algorithm in order to ensure the sensitivity and accuracy of the algorithm and minimize the processing time of algorithm.

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

5.2 FUTURE WORK

The algorithm need to be implement to the CPS with sensor integrated in order to test the practicality of the algorithm. Besides, the algorithm need to be connect to different CPS to test the robustness of algorithm in handling different sensory data. The sensory data should be send to the cloud or cyberspace for the execution of algorithm in order to fully embrace the challenges of I4.0.

REFERENCES

[1] Qin, J., Liu, Y. and Grosvenor, R., "A categorical framework of manufacturing for industry 4.0 and beyond.," Procedia CIRP, vol. 52, pp. 173-178, 2016.

[2] I. A. Ahmad, "Is It The Dawn of Industrial 4.0 in Malaysia," myForesight, vol. 04, pp. 04-07, 2016.

[3] T. Sung, "Industry 4.0: A Korea perspective. ," Technological Forecasting and Social Change, 2017.

[4] Hermann, M., Pentek, T. and Otto, B., "Design principles for industrie 4.0 scenarios," In System Sciences (HICSS), 2016 49th Hawaii International Conference on, pp. 3928-3937, 2016.

[5] Lee, J., Bagheri, B. and Kao, H.A., "A cyber-physical systems architecture for industry 4.0-based manufacturing systems," Manufacturing Letters, vol. 3, pp. 18-23, 2015.

[6] Lee, J., Ardakani, H.D., Yang, S. and Bagheri, B., "Industrial big data analytics and cyber-physical systems for future maintenance & service innovation," Procedia CIRP, vol. 38, pp. 3-7, 2015.

[7] Namratha, M., Prajwala, T.R., "A comprehensive overview of clustering algorithms in pattern recognition," IOSR J. Comput. Eng., vol. 4, no. 6, p. 23–30, 2012.

[8] "Machine Learning: What is it & Why its matters," SAS, [Online]. Available: https://www.sas.com/en_my/insights/analytics/machine-learning.html. [Accessed 01 10 2017].

[9] Gulenko, A., Wallschläger, M., Schmidt, F., Kao, O. and Liu, F., "Evaluating machine learning algorithms for anomaly detection in clouds.," In Big Data (Big Data), pp. 2716-2721, 2016.

[10] A. Ruban, "Malaysia Must Ready For Industry 4.0 Now," Malaymail Online, 2017.

[11] S. Amarthalingam, "Malaysia's Industry 4.0 Initiative Slow On Uptake," Edge Financial Daily,, June 28, 2017.

[12] H. Ishak, "Industrial Revolution 4.0 – Tackling It By Its Horn.," myForesight, vol. 04, p. 22 – 25, 2016.

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

[13] J. Jacobs, "The opportunity and threat of Industry 4.0.," The Edge Malaysia,, July 12, 2017.

[14] Stojanovic, L., Dinic, M., Stojanovic, N. and Stojadinovic, A., "Big-data-driven anomaly detection in industry (4.0): An approach and a case study.," In Big Data (Big Data), 2016 IEEE International Conference on, pp. 1647-1652, 2016.

[15] Y. Reddy, "Security and design challenges in cyber-physical systems.," In Information Technology-New Generations (ITNG), 2015 12th International Conference on, pp. 200-205, 2015.

[16] Y. Reddy, "Cloud-based cyber physical systems: Design challenges and security needs," n Mobile Ad-hoc and Sensor Networks (MSN), 2014 10th International Conference on, pp. 315-322, 2014.

[17] L. Ribeiro, "Cyber-physical production systems' design challenges," In Industrial Electronics (ISIE), 2017 IEEE 26th International Symposium on, pp. 1189-1194, 2017.

[18] "Industry 4.0: the fourth industrial revolution – guide to Industrie 4.0," i-scoop.edu, [Online]. Available: https://www.i-scoop.eu/industry-4-0/#. [Accessed 5 october 2017].

[19] Hodge, V.J. and Austin, J., "A survey of outlier detection methodologies.," Artificial Intelligence Review, vol. 22, no. 2, pp. 85-126, 2004.

[20] Markou, M. and Singh, S., "Novelty detection: a review—part 2:: neural network based approaches," Signal processing, vol. 83, no. 12, pp. 2499-2521, 2003.

[21] P. Choudhary, "Introduction to Anomaly Detection," DATASCIENCE.COM, 14 February 2017. [Online]. Available: https://www.datascience.com/blog/python-anomaly-detection. [Accessed 15 October 2017].

[22] Kalinichenko, L., Shanin, I. and Taraban, I., "Methods for Anomaly Detection: a Survey," In Proc. of the 16th All-Russian Conference “Digital Libraries: Advanced Methods and Technologies, Digital Collections-RCDL-2014, 2014.

[23] D. Nicoulaz, "LinkedIn," 24 11 2016. [Online]. Available: https://www.linkedin.com/pulse/anomaly-detection-manufacturing-didier-nicoulaz/. [Accessed 30 9 2017].

[24] Goldstein, M. and Uchida, S. , "A comparative evaluation of unsupervised anomaly detection algorithms for multivariate data," PloS one, vol. 11, no. 4, p. e0152173, 2016.

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

[25] Chandola, V., Banerjee, A. and Kumar, V., "Anomaly detection: A survey," ACM computing surveys (CSUR), vol. 41, no. 3, p. 15, 2009.

[26] Gulenko, A., Wallschläger, M., Schmidt, F., Kao, O. and Liu, F., "Evaluating machine learning algorithms for anomaly detection in clouds.," In Big Data (Big Data), 2016 IEEE International Conference on, pp. 2716-2721, 2016.

[27] Shahreza, M.L., Moazzami, D., Moshiri, B. and Delavar, M.R., "Anomaly detection using a self-organizing map and particle swarm optimization," Scientia Iranica, vol. 18, no. 6, pp. 1460-1468, 2011.

[28] Han, J., & Kamber, M., Data mining: concepts and techniques second edition, United States of America: Morgan Kaufmann Publishers, 2006.

[29] Rui, X. and Donald, W., "Survey of clustering algorithms," IEEE Transactions on Neural Networks, vol. 16, no. 3, pp. 645-678, 2005.

[30] Swagatam, D., Ajith, A. and Amit, K., "Automatic kernel clustering with a multi-elitist particle swarm optimization algorithm," Pattern: Recognition Letters, vol. 29, no. 5, pp. 688-699, 2008.

[31] Ahmed, M., Mahmood, A.N. and Hu, J., "A survey of network anomaly detection techniques," Journal of Network and Computer Applications, vol. 60, pp. 19-31, 2016.

[32] Haupt, R.L. and Haupt, S.E., Practical genetic algorithms, United States of America: John Wiley & Sons, 2004.

[33] Shamshirband, S., Anuar, N.B., Laiha, M., Kiah, M. and Misra, S., "Anomaly detection using fuzzy Q-learning algorithm," Acta Polytechnica Hungarica, vol. 11, no. 8, pp. 5-28, 2014.

[34] Eskin E, ArnoldA,PrerauM,PortnoyL,StolfoS., "A geometric framework for unsupervised anomaly detection," Applications of data mining in computer security, vol. 6, pp. 77-101, 2002.

[35] S. Samarasinghe, Neural networks for applied sciences and engineering: from fundamentals to complex pattern recognition, New york: Auerbach Publications, 2007.

[36] S. Haykin, Neural network: A comprehensive Foundation, New York: MacMillan College Publishing, 1994.

[37] Callegari, C., Giordano, S. and Pagano, M., "Neural network based anomaly detection," In Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), 2014 IEEE 19th International Workshop on, pp. 310-314, 2014.

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

[38] Li, W., Wu, G. and Du, Q., "Transferred Deep Learning for Anomaly Detection in Hyperspectral Imagery.," IEEE Geoscience and Remote Sensing Letters, vol. 14, no. 5, pp. 597-601, 2017.

[39] Lokman, G. and Yilmaz, G., "A new method for anomaly detection and target recognition," n Unmanned Aircraft Systems (ICUAS), 2014 International Conference on, pp. 577-583, 2014.

[40] Nanduri, A. and Sherry, L., "Anomaly detection in aircraft data using Recurrent Neural Networks (RNN)," In Integrated Communications Navigation and Surveillance (ICNS), pp. 5C2-1, 2016.

[41] Kwon, D., Kim, H., Kim, J., Suh, S.C., Kim, I. and Kim, K.J., "A survey of deep learning-based network anomaly detection," Cluster Computing, pp. 1-13, 2017.

[42] T. Kohonen, Self-organization and associative memory (Vol. 8), Springer Science & Business Media, 2012.

[43] C. Looney, Pattern recognition using neural networks: theory and algorithms for engineers and scientists, New York: Oxford University Press, Inc., 1997.

[44] Lee, S., Kim, G. and Kim, S., "Self-adaptive and dynamic clustering for online anomaly detection," Expert Systems with Applications, vol. 38, no. 12, pp. 14891-14898, 2011.

[45] W. Huai-bin, Y. Hong-liang, X. Zhi-jian, and Y. Zheng, "A Clustering Algorithm Use SOM and K-Means in Intrusion Detection," in 2010 International Conference on E-Business and E-Government,, pp. 1281-1284, 2010.

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

[46] Tian, J., Azarian, M.H. and Pecht, M., "Anomaly Detection Using Self-Organizing Maps-Based K-Nearest Neighbor Algorithm," in In Proceedings of the European Conference of the Prognostics and Health Management Society, 2014.

[47] Zhang, S., Fung, C., Huang, S., Luan, Z. and Qian, D., "PSOM: Periodic Self-Organizing Maps for unsupervised anomaly detection in periodic time series," In Quality of Service (IWQoS), 2017 IEEE/ACM 25th International Symposium on, pp. 1-6, 2017.

[48] Siripanadorn, S., Hattagam, W. and Teaumroong, N., "Anomaly detection using self-organizing map and wavelets in wireless sensor networks," In Proceedings of the 10th WSEAS international conference on Applied computer science (ACS'10), pp. 291-297, 2010.

[49] Shahreza, M.L., Moazzami, D., Moshiri, B. and Delavar, M.R., "Anomaly detection using a self-organizing map and particle swarm optimization," Scientia Iranica, vol. 18, no. 6, pp. 1460-1468, 2011.

[50] Liu, J., Chen, S., Zhou, Z. and Wu, T.,, "An Anomaly Detection Algorithm of Cloud Platform Based on Self-Organizing Maps," Mathematical Problems in Engineering, vol. 2016, 2016.

[51] M. Miskon, Novelty detection using a mobile robot: challenges and benefits, Monash University, 2009.

[52] Miskon, MF., Sobran, NMM., Ali, F., Shukor, AZH., "Spatial Habituating Self Organizing Map," Jurnal Teknologi, vol. 74, no. 9, pp. 183-189, 2015.

[53] De la Hoz, E., de la Hoz, E., Ortiz, A., Ortega, J. and Martínez-Álvarez, A., "Feature selection by multi-objective optimisation: Application to network anomaly detection by hierarchical self-organising maps," Knowledge-Based Systems, vol. 71, pp. 322-338, 2014.

[54] Chiu, C.H., Chen, J.J. and Yu, F., "An Effective Distributed GHSOM Algorithm for Unsupervised Clustering on Big Data," In Big Data (BigData Congress), 2017 IEEE International Congress on, pp. 297-304, 2017.

[55] S. Albayrak, C. Scheel, D. Milosevic, and A. Muller,, "Combining Self-Organizing Map Algorithms for Robust and Scalable Intrusion Detection," in International Conference on Computational Intelligence for Modelling, Control and Automation and International Conference on Intelligent Agents, Web Technologies and Internet Commerce (CIMCA-IAWTIC'06), pp. 123-130, 2005.

[56] S. Marsland, On-line novelty detection through self-organization, with application to inspection robotics, University of Manchester, 2001.

[57] J. A. Swets, Signal detection theory and ROC analysis in psychology and diagnostics : collected papers, Psychology Press., 2014.

[58] Zweig MH, and Campbell G., "Receiver-operating characteristic (ROC) plots: a fundamental evaluation tool in clinical medicine," Clinical Chemistry, vol. 39, pp. 561-577, 1993.

[59] "Sensor Terminology," National Instruments, 23 September 2013. [Online]. Available: http://www.ni.com/white-paper/14860/en/. [Accessed 23 January 2018].

[60] Upasana, "How to handle Imbalanced Classification Problems in machine learning?," Analytics Vidhya, 17 March 2017. [Online]. Available: https://www.analyticsvidhya.com/blog/2017/03/imbalanced-classification-problem/. [Accessed 24 May 2018].

[61] J. Brownlee, "8 Tactics to Combat Imbalanced Classes in Your Machine Learning Dataset," Machine Learning Mastery, 19 August 2015. [Online]. Available: https://machinelearningmastery.com/tactics-to-combat-imbalanced-classes-in-your-machine-learning-dataset/. [Accessed 24 May 2018].

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

[62] C. D, "Ten quick tips for machine learning in computational biology," BioData Mining, vol. 10, no. 35, pp. 1-17, 2017.

[63] Ye Wu & Rick Radewagen, "7 Techniques to Handle Imbalanced Data," KD Nuggets, 18 June 2017. [Online]. Available: https://www.kdnuggets.com/2017/06/7-techniques-handle-imbalanced-data.html. [Accessed 24 May 2018].

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

APPENDIX A: Matlab Coding (k-means Clustering)

```
rng default; % For reproducibility
load('km.mat')
X = S3

figure;
plot(X(:,1),X(:,2),'.');
title 'Weight Vector Initialization';
%%
% There appears to be 8 clusters in the data.
%
% Partition the data into 8 clusters, and choose the best
arrangement out
% of five initializations. Display the final output.
%%
opts = statset('Display','final');
[idx,C] = kmeans(X,8,'Display','iter','Distance','sqeuclidean',...
    'MaxIter',300,'Options',opts);
%%
% By default, the software initializes the replicates separately
using _k_-means++.
%
% Plot the clusters and the cluster centroids.
%%
figure;
plot(X(idx==1,1),X(idx==1,2),'r.','MarkerSize',4)
hold on
plot(X(idx==2,1),X(idx==2,2),'b.','MarkerSize',4)
hold on
plot(X(idx==3,1),X(idx==3,2),'g.','MarkerSize',4)
hold on
plot(X(idx==4,1),X(idx==4,2),'m.','MarkerSize',4)
hold on
plot(X(idx==5,1),X(idx==5,2),'k.','MarkerSize',4)
hold on
plot(X(idx==6,1),X(idx==6,2),'c.','MarkerSize',4)
hold on
plot(X(idx==7,1),X(idx==7,2),'y.','MarkerSize',4)
hold on
plot(X(idx==8,1),X(idx==8,2),'ro','MarkerSize',4)
hold on
plot(C(:,1),C(:,2),'kx',...
     'MarkerSize',10,'LineWidth',0.2)
legend('Cluster 1','Cluster 2','Cluster 3','Cluster 4','Cluster
5','Cluster 6','Cluster 7','Cluster 8','Centroids',...
       'Location','NW')
title 'Cluster Assignments and Centroids'
hold off
w=(C(:,1))';
save('var1.dat',"h","w");%%save as dat. file for anomaly detection
```

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

APPENDIX B: Matlab Coding (ROC Plot)

Matlab Coding (Threshold Variation)

```
clear all
clc
tic;
index=0;
load ('thres1.mat')
load ('var1.dat','-mat');
learning_rate=0.01;
data_size=size(thres);

for i=1:data_size(1)%%indicating size of matrix S1 row

    current_reading=thres(i,:);
    index=index+1;
    neuron_matrix_size=size(w);
    for k=1:neuron_matrix_size(2)%%indicating size of matrix w
column
        square_distance=((current_reading(k)-w(1,k)).^2);
        euc_distance_neuron(k)=sqrt(square_distance);
    end
    max_euc_dist=max(euc_distance_neuron);
    if max_euc_dist<0.055%%insert various threshold
(start:0.0005;increment:0.0005)
       for k=1:neuron_matrix_size(2)%%indicating size of matrix w
column
           w(1,k)=w(1,k)+learning_rate*(current_reading(k)-w(1,k));
        end
    else
       w=[w;current_reading];
    end
end
toc;
```

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

Matlab Coding (ROC Plot and Curve Smoothing)

```
x=thresS3(:,3);
y=thresS3(:,2);
r=thresS3(:,1);
c=smooth(y,0.1,'loess');
plot(x,y,'g+',x,c,'r-');
set(gca,'YLim',[0 1.1]);
yyaxis left
title('ROC curve');
xlabel('False Positive Rate (FPR) / 1-SPC');
ylabel('Sensitivity / True Positive Rate (TPR)');
yyaxis right
plot(x,r,'m.');
ylabel('Threshold Value (TV)')
legend('ROC - point','ROC - smoothed curve','TV against FPR')
```

APPENDIX C: Matlab Coding (Habituating SOM)

```
clear all
clc
tic;
index=0;
load('S4.mat');%%insert dataset matrix
load ('var1.dat','-mat');%%insert habituating matrix & neuron weight
learning_rate=0.01;%%initialize learning rate
data_size=size(dataCopyS5);%%indiate size of dataset

for i=1:data_size(1)%%indicating size of matrix S1 row
    %%ensure the insertion of dataset row by row to fulfill real-
time
    %%situation
    current_reading=dataCopyS5(i,:);
    index=index+1;
    neuron_matrix_size=size(w);%%indicate size of w
    for k=1:neuron_matrix_size(2)%%indicating size of matrix w
column
        square_distance=((current_reading(k)-w(1,k)).^2);
        euc_distance_neuron(k)=sqrt(square_distance);
    end
    %%find max euclidean distance among the BMU
    max_euc_dist=max(euc_distance_neuron);
    %%the current_reading only consider as normal when max_euc_dist
is
    %%lower than the threshold set
    if max_euc_dist<0.056
        for k=1:neuron_matrix_size(2)%%indicating size of matrix w
column
            %%update the neuron weight of neurons
            w(1,k)=w(1,k)+learning_rate*(current_reading(k)-w(1,k));
        end
    else
        w=[w;current_reading];
    end
    title('Graph of behaviour against iteration');
    xlabel('iteration t');
    ylabel('behaviour value');
    if max_euc_dist<0.056
        plot(i,dataCopyS5(i,:),'g.','MarkerSize',10);hold on
    else
        plot(i,dataCopyS5(i,:),'m+','MarkerSize',10);hold on
    end
    legend('Normal','Anomaly')
end
toc;
```

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

APPENDIX D: Project Gantt Chart

Activities/Planning	Week													
	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Define problem														
Research on CPS, I4.0 and Anomaly detection														
Clarify problem statement, objective and scope														
Literature review														
Propose method														
Design algorithm														
Algorithm testing														
Presentation														
Report writing														

Activities/Planning	Week													
	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Improvement on algorithm														
Validation on algorithm														
Experiment														
Tabulation of result														
Analysis performance														
Presentation														
Report writing														

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

APPENDIX E: Table of Threshold Variation for ROC Plot

Threshold Value	Anomaly Detected	TP	FP	TN	FN	TPR	FPR
0.0005	1000	40	960	0	0	1	1
0.001	1000	40	960	0	0	1	1
0.0015	1000	40	960	0	0	1	1
0.002	1000	40	960	0	0	1	1
0.0025	1000	40	960	0	0	1	1
0.003	1000	40	960	0	0	1	1
0.0035	1000	40	960	0	0	1	1
0.004	1000	40	960	0	0	1	1
0.0045	1000	40	960	0	0	1	1
0.005	1000	40	960	0	0	1	1
0.0055	1000	40	960	0	0	1	1
0.006	1000	40	960	0	0	1	1
0.0065	1000	40	960	0	0	1	1
0.007	1000	40	960	0	0	1	1
0.0075	1000	40	960	0	0	1	1
0.008	1000	40	960	0	0	1	1
0.0085	1000	40	960	0	0	1	1
0.009	1000	40	960	0	0	1	1
0.0095	1000	40	960	0	0	1	1
0.01	1000	40	960	0	0	1	1
0.0105	1000	40	960	0	0	1	1
0.011	1000	40	960	0	0	1	1
0.0115	1000	40	960	0	0	1	1
0.012	1000	40	960	0	0	1	1
0.0125	1000	40	960	0	0	1	1
0.013	1000	40	960	0	0	1	1
0.0135	1000	40	960	0	0	1	1
0.014	1000	40	960	0	0	1	1
0.0145	1000	40	960	0	0	1	1
0.015	1000	40	960	0	0	1	1
0.0155	1000	40	960	0	0	1	1
0.016	1000	40	960	0	0	1	1
0.0165	1000	40	960	0	0	1	1
0.017	1000	40	960	0	0	1	1
0.0175	1000	40	960	0	0	1	1
0.018	1000	40	960	0	0	1	1
0.0185	1000	40	960	0	0	1	1
0.019	1000	40	960	0	0	1	1
0.0195	1000	40	960	0	0	1	1
0.02	1000	40	960	0	0	1	1

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

0.0205	1000	40	960	0	0	1	1
0.021	1000	40	960	0	0	1	1
0.0215	1000	40	960	0	0	1	1
0.022	1000	40	960	0	0	1	1
0.0225	1000	40	960	0	0	1	1
0.023	1000	40	960	0	0	1	1
0.0235	1000	40	960	0	0	1	1
0.024	1000	40	960	0	0	1	1
0.0245	1000	40	960	0	0	1	1
0.025	1000	40	960	0	0	1	1
0.0255	1000	40	960	0	0	1	1
0.026	1000	40	960	0	0	1	1
0.0265	1000	40	960	0	0	1	1
0.027	1000	40	960	0	0	1	1
0.0275	1000	40	960	0	0	1	1
0.028	1000	40	960	0	0	1	1
0.0285	1000	40	960	0	0	1	1
0.0285	1000	40	960	0	0	1	1
0.029	1000	40	960	0	0	1	1
0.0295	1000	40	960	0	0	1	1
0.03	992	40	952	8	0	1	0.991667
0.0305	985	40	945	15	0	1	0.984375
0.031	979	40	939	21	0	1	0.978125
0.0315	971	40	931	29	0	1	0.969792
0.032	970	40	930	30	0	1	0.96875
0.0325	970	40	930	30	0	1	0.96875
0.033	970	40	930	30	0	1	0.96875
0.0335	970	40	930	30	0	1	0.96875
0.034	970	40	930	30	0	1	0.96875
0.0345	970	40	930	30	0	1	0.96875
0.035	970	40	930	30	0	1	0.96875
0.0355	970	40	930	30	0	1	0.96875
0.036	970	40	930	30	0	1	0.96875
0.0365	970	40	930	30	0	1	0.96875
0.037	970	40	930	30	0	1	0.96875
0.0375	970	40	930	30	0	1	0.96875
0.038	970	40	930	30	0	1	0.96875
0.0385	970	40	930	30	0	1	0.96875
0.039	965	40	925	35	0	1	0.963542
0.0395	951	40	911	49	0	1	0.948958
0.04	916	40	876	84	0	1	0.9125
0.0405	890	40	850	110	0	1	0.885417
0.041	886	40	846	114	0	1	0.88125
0.0415	878	40	838	122	0	1	0.872917
0.042	869	40	829	131	0	1	0.863542

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

0.0425	849	40	809	151	0	1	0.842708
0.043	835	40	795	165	0	1	0.828125
0.0435	804	40	764	196	0	1	0.795833
0.044	804	40	764	196	0	1	0.795833
0.0445	802	40	762	198	0	1	0.79375
0.045	802	40	762	198	0	1	0.79375
0.0455	802	40	762	198	0	1	0.79375
0.046	802	40	762	198	0	1	0.79375
0.0465	802	40	762	198	0	1	0.79375
0.047	774	40	734	226	0	1	0.764583
0.0475	757	40	717	243	0	1	0.746875
0.048	724	40	684	276	0	1	0.7125
0.0485	673	40	633	327	0	1	0.659375
0.049	570	40	530	430	0	1	0.552083
0.0495	576	40	536	424	0	1	0.558333
0.05	532	40	492	468	0	1	0.5125
0.0505	530	40	490	470	0	1	0.510417
0.051	513	40	473	487	0	1	0.492708
0.0515	486	40	446	514	0	1	0.464583
0.052	420	40	380	580	0	1	0.395833
0.0525	404	40	364	596	0	1	0.379167
0.053	313	40	273	687	0	1	0.284375
0.0535	271	40	231	729	0	1	0.240625
0.054	148	40	108	852	0	1	0.1125
0.0545	100	40	60	900	0	1	0.0625
0.055	55	37	18	942	3	0.925	0.01875
0.0555	42	36	6	954	4	0.9	0.00625
0.056	40	36	4	956	4	0.9	0.004167
0.0565	35	35	2	958	5	0.875	0.002083
0.057	33	33	1	959	7	0.825	0.001042
0.0575	32	31	1	959	9	0.775	0.001042
0.058	32	32	0	960	8	0.8	0
0.0585	31	31	0	960	9	0.775	0
0.059	31	31	0	960	9	0.775	0
0.0595	29	29	0	960	11	0.725	0
0.06	24	24	0	960	16	0.6	0
0.0605	21	21	0	960	19	0.525	0
0.061	21	21	0	960	19	0.525	0
0.0615	21	21	0	960	19	0.525	0
0.062	21	21	0	960	19	0.525	0
0.0625	18	18	0	960	22	0.45	0
0.063	16	16	0	960	24	0.4	0
0.0635	16	16	0	960	24	0.4	0
0.064	16	16	0	960	24	0.4	0
0.0645	15	15	0	960	25	0.375	0

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

0.065	15	15	0	960	25	0.375	0
0.0655	14	14	0	960	26	0.35	0
0.066	13	13	0	960	27	0.325	0
0.0665	13	13	0	960	27	0.325	0
0.067	13	13	0	960	27	0.325	0
0.0675	13	13	0	960	27	0.325	0
0.068	12	12	0	960	28	0.3	0
0.0685	12	12	0	960	28	0.3	0
0.069	12	12	0	960	28	0.3	0
0.0695	12	12	0	960	28	0.3	0
0.07	12	12	0	960	28	0.3	0
0.0705	12	12	0	960	28	0.3	0
0.071	12	12	0	960	28	0.3	0
0.0715	11	11	0	960	29	0.275	0
0.072	11	11	0	960	29	0.275	0
0.0725	11	11	0	960	29	0.275	0
0.073	11	11	0	960	29	0.275	0
0.0735	10	10	0	960	30	0.25	0
0.074	10	10	0	960	30	0.25	0
0.0745	9	9	0	960	31	0.225	0
0.075	9	9	0	960	31	0.225	0
0.0755	9	9	0	960	31	0.225	0
0.076	9	9	0	960	31	0.225	0
0.0765	9	9	0	960	31	0.225	0
0.077	9	9	0	960	31	0.225	0
0.0775	8	8	0	960	32	0.2	0
0.078	8	8	0	960	32	0.2	0
0.0785	8	8	0	960	32	0.2	0
0.079	8	8	0	960	32	0.2	0
0.0795	7	7	0	960	33	0.175	0
0.08	6	6	0	960	34	0.15	0
0.0805	5	5	0	960	35	0.125	0
0.081	5	5	0	960	35	0.125	0
0.0815	5	5	0	960	35	0.125	0
0.082	5	5	0	960	35	0.125	0
0.0825	5	5	0	960	35	0.125	0
0.083	5	5	0	960	35	0.125	0
0.0835	5	5	0	960	35	0.125	0
0.084	5	5	0	960	35	0.125	0
0.0845	5	5	0	960	35	0.125	0
0.085	5	5	0	960	35	0.125	0
0.0855	5	5	0	960	35	0.125	0
0.086	5	5	0	960	35	0.125	0
0.0865	5	5	0	960	35	0.125	0
0.087	5	5	0	960	35	0.125	0

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

0.0875	5	5	0	960	35	0.125	0
0.088	5	5	0	960	35	0.125	0
0.0885	5	5	0	960	35	0.125	0
0.089	5	5	0	960	35	0.125	0
0.0895	5	5	0	960	35	0.125	0
0.09	5	5	0	960	35	0.125	0
0.0905	5	5	0	960	35	0.125	0
0.091	5	5	0	960	35	0.125	0
0.0915	5	5	0	960	35	0.125	0
0.092	5	5	0	960	35	0.125	0
0.0925	5	5	0	960	35	0.125	0
0.093	5	5	0	960	35	0.125	0
0.0935	5	5	0	960	35	0.125	0
0.094	5	5	0	960	35	0.125	0
0.0945	5	5	0	960	35	0.125	0
0.095	5	5	0	960	35	0.125	0
0.0955	5	5	0	960	35	0.125	0
0.096	5	5	0	960	35	0.125	0
0.0965	5	5	0	960	35	0.125	0
0.097	5	5	0	960	35	0.125	0
0.0975	5	5	0	960	35	0.125	0
0.098	4	4	0	960	36	0.1	0
0.0985	4	4	0	960	36	0.1	0
0.099	3	3	0	960	37	0.075	0
0.0995	2	2	0	960	38	0.05	0
0.1	2	2	0	960	38	0.05	0
0.1005	1	1	0	960	39	0.025	0

UNIVERSITI TEKNIKAL MALAYSIA MELAKA