

# Deep Q Learning for Self Adaptive Microservices Architecture

**BASEL MAGABLEH<sup>1</sup>, MUDER ALMIANI<sup>2</sup>, AND LUCA LONGO<sup>3</sup>**

<sup>1</sup>Technological University, Dublin, Ireland (e-mail: basel.magableh@dit.ie)

<sup>2</sup>Al-Hussein Bin Tala University, Ma'am, Jordan (e-mail: malmiani@my.bridgeport.edu)

<sup>3</sup>Technological University, Dublin, Ireland (e-mail: luca.longo@dit.ie)

Corresponding author: Magableh B. (e-mail: basel.magableh@dit.ie).

**ABSTRACT** Services running in Microservices cluster could be scaled in/out based on the demand issued by end-users, orchestration algorithm, or load balancer running on the cluster leader. The behaviour of Microservices architecture is continuously changing overtime, which makes it a challenging task to use a statistical model to identify normal and abnormal behaviour of the running services. The performance of the cluster nodes could fluctuate around the demand to accommodate scalability, orchestration and load balancing demands. This requires a model that is able to detect anomalies in real-time and generate a high rate of accuracy in detecting any anomalies and a low rate of false alarms. At the same time, it requires dynamic policy configuration that can be used to adapt the recent changes in the operational environment. This paper focuses on proposing a self-healing Microservices architecture, that is able to continuously monitor the operational environment, detects and observes anomalous behaviour, and provides a reasonable adaptation policy using multidimensional utility-based model. We argue in this paper that such model could offer self-scaling of Microservices architecture and adapt the sudden changes in the operational environment. The self-healing property is achieved by means of parameter tuning and dynamic adjustment of the cluster configuration. We believe integrating utility theory in the dynamic decision-making process improves the effectiveness of the adaptation and reduces the adaptation risk including resources over-provisioning and thrashing. Also, it preserving the cluster state by preventing multiple adaptation to take place at the same time

**INDEX TERMS** Anomaly detection, Microservices Architecture, Q Learning, Runtime configuration, Self Healing, Reinforcement learning, Policy Approximation

## I. INTRODUCTION

**A** MICROSERVICES architecture could be defined in the context of a service-oriented architecture as a composition of tiny fine-grained distributed loosely coupled building blocks of software components [1]. Microservices improve software modularity and make the application easy to develop and maintain. With the rapid development of cloud infrastructures and virtualisation techniques, a high demand for building Microservices architectures in a complete virtualised environment has emerged. This need was met by introducing containers engine like Docker<sup>1</sup> as well as cluster management framework such as Docker swarm<sup>2</sup>. The performance of Microservices running in cluster mode could fluctuate around the demand to accommodate scalability,

orchestration and load balancing offered by the cluster leader [1]. In their daily base tasks, many Dev-Ops face an issue of defining and identifying a threshold which can be used to identify a network, system or user activity as normal behaviour. Another challenge that exist in Microservices clusters is the ability to dynamically scale horizontally, (i.e. adjusting the number of nodes participating in the cluster), or vertically (i.e. adjusting the computational resources available for the services). In addition to this, it is not possible to configure auto scaling policy that could be used by the cluster leader to perform resilient and autonomous reasoning to achieve the desired QoS of the architecture.

Nowadays, cluster management technology does not embed a component that can guarantees continuous monitoring and adaptation of the operational environment. Also cluster management can not offer the architecture with dynamic capability to reason about context changes at run-time. To

<sup>1</sup><https://www.docker.com>

<sup>2</sup><https://docs.docker.com/engine/swarm/>

achieve such a high level of scalability, a swarm cluster, for instance, should have a component for continuously monitoring the cluster and a component for adaptation that can implement a reasonable reaction/scaling policy to accommodate the changes in the operating environment. This presents a challenge to build a self-healing microservices architecture that can dynamically adjust its own behaviour and heal itself against anomalous behaviour detected at real-time. Self-healing refers to a property of a self-adaptive software to have the capability of discovering, diagnosing and reacting to disruptions. It can also anticipate potential problems and, accordingly, take proper actions to prevent a failure [2]. To achieve a high level of self-healing it is necessary to have four major functionalities at run-time: 1) Monitoring and detecting events (contextual changes), 2) Context reasoning (dynamic decision making), 3) Adaptation strategies, 4) validation and verification of the adaptation action [3].

The proposed model in this paper offers Microservices architecture a self-healing property by providing a mechanism for continuous monitoring, context detecting of anomalous behaviour using real-time unsupervised anomaly detection algorithm, dynamic decision making using a multidimensional utility based model, enabling dynamic adaptation horizontally or vertically based on the demand and the changes of the operational environment, and runtime verification and validation of the fitness of proposed adaptation strategy. We argue that the self-healing attribute of Microservices architecture is achieved by leveraging parameter tuning and dynamic decision-making supported by an accurate anomaly detection of Microservices architecture.

This paper is structured as follows: Section II provides an overview of self-healing architectures and surveys the approaches for anomaly detection, and run-time configurations. Section III presents a model that can continuously observe Microservice architectures with Self-healing capabilities. Section IV-A proposes a strategy for analysing and evaluating the capability of the model to detect anomalous behaviours and to trigger suitable adaptation actions. Section IV-B is focused on results found followed by a critical discussion of the effectiveness of this model. Section V summarises this research, highlighting its contribution and setting future work.

## II. RELATED WORK

### A. SELF-ADAPTIVE SOFTWARE

Self-adaptive software is characterised by a number of properties best referred to as autonomic [4]. These the 'self-\*' properties' include Self-organisation, Self-healing, Self-optimisation and Self-protection [5]. Self-healing architecture refers to the capability of discovering, diagnosing and reacting to disruptions. It can also anticipate potential problems and, accordingly, take suitable actions to prevent a failure [5]. Self-healing aspects of Microservices architectures requires a decision-making strategy that can work in real-time. This is essential for Microservice to reason about its own state and

its surrounding environment in a closed control loop model and act accordingly [6]. Typically, a self-adapting system follows MAPE-K model (Monitor-Analyse-Plan-Execute over a shared Knowledge). a self-healing system should implements MAPE-K model including: Gathering of data related to the surrounding context (Context Sensing); Context observation and detection; Dynamic decision making; Adaptation execution to achieve the adaptation objectives defined as QoS; Verification and validation of the applied adaptation actions in terms of its ability to meet the adaptation objectives and meet the desired QoS.

### B. CONTEXT SENSING

However, there is many approaches are used for achieving high level of self-adaptability though Context sensing involving context collection, observation and detection of contextual changes in the operational environment [7]. Also, the ability of the system to dynamically adjust its behaviour can be achieved using parameter-tuning [8], component-based composition [9], or Middleware-based approaches [10]. Another important aspect of self-adaptive system is related to its ability to validate and verify the adaptation action at runtime based on Game theory [11], Utility theory as in [12], [13], or Model driven approach as in [14].

Context information (1) refers to any information that is computationally accessible and upon which behavioural variations depend [15]. Context observation and detection approaches (2) are used to detect abnormal behaviour within the microservices architecture at run-time. Related work in context modelling, context detection and engineering self-adaptive software system are discussed in [2], [6], [7], [16]. In dynamic decision making and context reasoning (3), the architecture should be able to monitor and detect normal/abnormal behaviour by continuously monitoring the contextual information found in the Microservices cluster.

### C. ADAPTATION PLANING AND EXECUTION

In Microservices cluster, the performance of the cluster nodes could fluctuate around the demand to accommodate scalability, orchestration and load balancing issued by cluster leader. This requires a model that is able to detect anomalies in real-time and generate a high rate of accuracy in detecting any anomalies and a low rate of false alarms. In addition, there will be a set of variations that can be used by the system to adapt the changes in its operational environment. This requires a dynamic decision making that can calculate the utility of all possible adaptation actions based on the architecture constraints (i.e. number of replicas, number of nodes, desired objectives, metrics thresholds), anomaly score of the detected conditions (CPU, Memory, DISK I/O, Network I/O), and the confidence and accuracy of the anomaly score of the detected abnormal behaviour, and the desired/predicted cluster state. Then, the adaptation manager will execute the adaptation action and verifies its successfulness over the cluster architecture. Also, the adaptation manager will be able to self-tune and self-adjust the architecture parameters to

meet high/low demand for services. Finally, the architecture will preserve the cluster state through the adaptation cycle (monitoring, observing, detecting, reacting, and verifying). This research focuses on finding a method to continuously observe and monitor the swarm cluster and be able to detect anomalous behaviour with a high accuracy and generate a low rate of false alarms. Then provide the architecture with adaptation strategies with high utility to reason about the detected anomalies and be able to self-adjust the architecture parameters and verifies the adaptation actions at runtime without human intervention.

#### D. ANOMALY DETECTION

There are two phases for detecting anomalies in a software system: a training phase which involves profiling the normal behaviour of the system; a second phase aimed at testing the learned profile of the system with new data and employing it to detect normal/abnormal behaviours [17].

Three major techniques for anomaly detection have emerged from the literature: statistical anomaly detection, data-mining and machine-learning based techniques.

Within the statistical methods, a system observes the activity of the system and generates profiles of system metrics to represent its behaviour. The system profile includes performance measures of the system resources such as CPU and Memory. For each measure, a separate profile is stored. Then, the current readings of the system are profiled and compared against the memorised past profile to calculate an anomaly score. This score is calculated by comparing all measures within the profile against a threshold specified by the developer. Once the system detects that the current readings of the system are higher than this threshold, then these will be automatically categorised as intrusions thus triggering an alert [18].

Various statistical anomaly detection systems have been proposed and they have some advantages [19], [20]. One of this is that they can detect an anomaly without prior knowledge of the system. This can mitigate the common problem of a cold start found in machine learning techniques. Additionally, statistical anomaly detection provides accurate notifications of malicious attacks that occurred over long periods of times and it performs better in detecting denial-of-service attacks [17]. However, a disadvantage is that a skilled attacker might train a statistical anomaly detection system to accept the abnormal behaviour as normal. It is difficult to determine the thresholds that make a balance between the likelihood of a false negative (the system fails to identify an activity as an abnormal behaviour) and the likelihood of a false positive (false alarms). Statistical methods need an accurate model with a precise distribution of all measures. In practice, the behaviour of virtual machines/computers cannot be entirely be modelled using solely statistical methods.

With regard to data-mining approaches, data-mining is about finding insights which are statistically reliable, unknown previously, and actionable from data [21]. The dataset must be available, relevant, adequate, and clean. The data

mining process involves discovering a novel, distinguished and useful data pattern in large datasets to extract hidden relationships and information about the data. In general, there are two issues involved in the use of data mining in an anomaly detection system. First, there is a lack of a large dataset to be used by the algorithm containing lots of information about the architecture. Second, few approaches were targeting the anomaly detection system in Microservices architecture [21]. Data mining based anomaly detection systems have three major difficulties which prevent them from being widely adopted in Microservices architecture [17]. Firstly, the low accuracy of detecting anomalous behaviour [17], [22], as the data mining process would require large dataset with longer time interval to be able to improve the accuracy of detection. Most data mining techniques are heavily on computational resources, this negatively influences their adoption in a Microservices architecture [17]. Additionally, usually a data mining method used to classify an attack within a specific system cannot be successfully employed within another system for the same purpose. This because the process of training, testing the model and performing classification of anomalies needs to be repeated with different data or architecture [23].

Machine learning, in the context of anomaly detection, can allow the creation of software system able to learn and improve its detection accuracy over time [24]. Machine learning-based anomaly detection models aims to detect anomalies similar to statistical and data mining approaches. However, unlike them latter which tend to focus on understanding the process that generated the data, the former are data-driven and are mainly focus on training a model based exclusively on past data [17]. This means that, when additional and new data is provided they can intrinsically change their detection strategy and classify significant deviations from the normal behaviour of an underlying software program. An application of Machine Learning which enables the Microservices cluster to distinguish between normal and abnormal behaviour in the data can be found in [23]. In general, anomaly detection systems uses a combination of clustering and classification algorithms to detect anomalies. The clustering algorithm is used to cluster the dataset and label them. Then, a decision tree algorithm can be used to distinguish between normal and abnormal behaviour. Golmah [25] suggested the use of an effective classification model to identify normal and abnormal behaviour in network-based anomaly detection. The usage of Machine Learning algorithm in this context can be found in [23], [25], [26]. Due to the opening deployment and limited resources found in a Microservices cluster, it is very important to use a lightweight approach of data clustering and classification. Due to this issue, this research focuses on proposing an anomaly detection mechanism that is more suitable for the Microservices architecture and can be easily deployed with less footprints on the limited resources found in the tiny containers running in Microservices cluster.

Numenta Platform for Intelligent Computing (NUPIC) is

based on the Hierarchical Temporal Memory (HTM) model proposed in [27]. HTM has been experimentally applied in real-time anomaly detection of streaming data in [28], [29]. The proposed system based on the HTM model claimed to be efficient and tolerant to noisy data. Most importantly it offers continuous monitoring of real-time data and adapts the changes of the data statistics. It also detects very subtle anomalies with a very minimum rate of false positives. In a recent study, Ahmad et al. [30] proposed an updated version of the anomaly detection algorithm with the introduction of the anomaly likelihood concept. The anomaly score calculated by the NUPIC anomaly detection algorithm represents an immediate calculation of the predictability of the current input stream. This approach works very well with predictable scenarios in many practical applications. As there is no noisy and unpredictable data found, the raw anomaly score gives an accurate prediction of false negatives. However, the changes in predictions would lead to revealing anomalies in the system's behaviour. Instead of using the raw anomaly score, Ahmad et al. [30] proposed a method for calculating the anomaly likelihood by modelling the distribution of anomaly scores and using the distribution to check the likelihood of the current state of the system to identify anomalous behaviour. The anomaly likelihood refers to a metric which defines how anomalous the current state is based on the prediction history calculated by the HTM model. So, the anomaly likelihood is calculated by maintaining a window of the last raw anomaly scores and then calculating the normal distribution over the last obtained/trained values, then the most recent average of anomalies is calculated using the Gaussian tail probability function (Q-function) [31].

### E. REINFORCEMENT LEARNING

*The goal of reinforcement learning (RL) is to learn a policy that decides sequential actions by maximizing the cumulative future rewards [30]. Recent trends [23, 32, 28, 27] in RL field is to combine the deep neural networks with RL algorithms by representing RL models such as value function or policy. By resorting of the deep features, many difficult problems such as playing Atari games [23] or Go [27] can be successfully solved in semi-supervised setting. Also, several methods were proposed to solve the computer vision problems, such as object localization [3] or action recognition [16], by employing the deep RL algorithms. There are two popular approaches in deep RL algorithms: Deep Q Networks (DQN) and policy gradient. DQN is a form of Q-learning with function approximation using deep neural networks. The goal of DQN is to learn a state-action value function (Q), which is given by the deep networks, by minimizing temporal-difference errors [23]. Based on the DQN algorithm, various network architectures such as Double DQN [32] and DDQN [37] were proposed to improve performance and keep stability. Policy gradient methods directly learn the policy by optimizing the deep policy networks with respect to the expected future reward using gradient descent. Williams et al. [38] proposed REINFORCE algorithm simply using the*

*immediate reward to estimate the value of the policy. Silver et al. [28] proposed a deterministic algorithm to improve the performance and effectiveness of the policy gradient in high-dimensional action space. In the work of Silver et al. [27], it is shown that pre-training the policy networks with supervised learning before employing policy gradient can improve the performance. In tracking problem, we train the proposed network with supervised learning to learn the appearance characteristics of the target objects, and train action dynamics of the tracking target with reinforcement learning using policy gradient method.*

## III. DESIGN AND METHODOLOGY

### A. SELF-HEALING MICROSERVICES ARCHITECTURE

One important aspect of a self-healing Microservices architecture is the ability to continuously monitor the operational environment, detect and observe anomalous behaviour, and provide a reasonable policy for self-scaling, self-healing, and self-tuning the computational resources to adapt a sudden changes in its operational environment dynamically at runtime.

The Microservices Architecture is shown in Figure III. The architecture was designed according to the MAPE-K model [32]. This model offering the Microservices architecture with the following functionalities:

**Metric collection:** Continuous collection of fine-grained metrics about cluster nodes, services, and containers including (CPU usage, Memory, Disk Reads Bytes/sec, Network Read/s, network write/s and Disk Writes Bytes/sec). The data are streamed into anomaly detection service at real-time.

**Model Training:** The NUPIC anomaly detection service [30] is continuously running over the streamed matrices collected in the matrices database, which enables the generation of the training model for the collected metric.

**Anomaly Detection:** The collected real-time data is feed on the fly to NUPIC anomaly detection service [30], which provides two features: First, continuous detection of anomalous behaviour with high accuracy. Second, it also provides predictions about the architecture performance based on the collected historic data. This can alert the architecture about incoming spike on resources demand which can be used by the adaptation manager to schedule a proactive adaptation strategy ahead of time. In addition, the anomaly detection service is able to detect anomalies as early as possible before the anomalous behaviour is interrupting the functionality of the running services in the cluster as demonstrated by Ahmad et al. [30].

**Adaptation Election:** Once there is an anomalous behaviour detected with high anomaly score and likelihood, both values are calculated by the Anomaly Detection Service as shown in Figure 1. The Alert manager notifies the adaptation manager about the anomalous detected. The adaptation manager selects the adaptation action(s) after calculating the utility value for all actions as explained in the following Section III-B. Then, the adaptation manager uses the input of the anomaly likelihood, architecture constraints (specified by



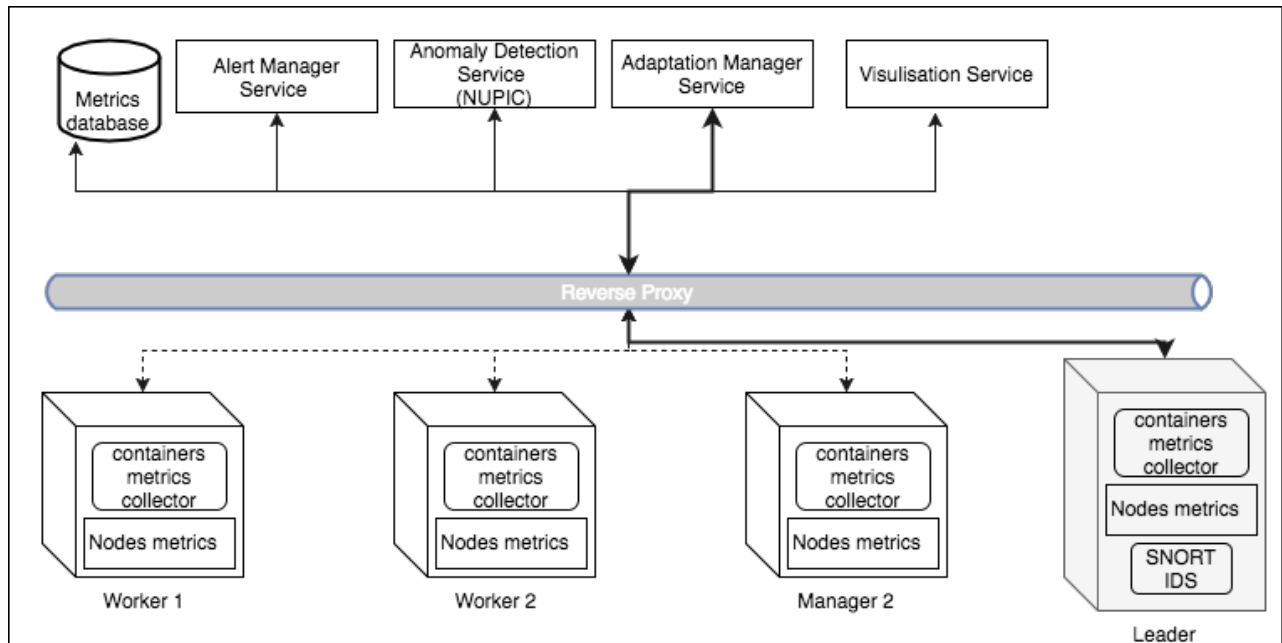


FIGURE 1. Microservices Architecture implemented in Docker Swarm

the DevOp during deployment), and desired/predicted QoS to calculate the best variation of the adaptation that has the highest utility.

**Adaptation Execution:** The adaptation manager executes the strategies based on the aggregated value of the utility returned by the algorithm. Once the adaptation action is completed by the adaptation manager, a set of adaptation actions are deployed in the architecture. To avoid, conflicts between multiple adaptation policies, the adapter allow the adaptation actions to be fully completed and verified by the cluster leader according to the consensus performed by RAFT, then it will put a cool off timer before initiating new adaptation actions. This technique is used to avoid resources thrashing and preserving the cluster state for auto-recovery. The adaptation manager sends the cluster leader a set of instructions that might involve tuning of cluster parameters, (horizontal scaling), adding/removing nodes, or vertical scaling of Microservice's containers like scaling a service in/out.

**Adaptation Verification:** The cluster leader and all managers in the cluster will vote on the adaptation action based on the consensus algorithm [33]. The vote results is used to validate and verifies the adaptation action. If the adaptation action won the votes, the adaptation action will be executed by the cluster leader, the adaptation manager records the adaptation attempt as successful. If the adaptation action lost the voting process, then the adaptation manager keeps the current state of the cluster and records the adaptation attempt as failed. In both cases, the adaptation manger records the number of attempts used to complete the adaptation actions.

## B. ADAPTATION STRATEGY

This research focuses on proposing a model that can continuously observe and monitor the Microservices architecture and be able to detect anomalous behaviour with high accuracy and generate low rate of false alarms. At the same time, the architecture should be able to respond to True positive alarms by suggesting a set of adaptation policies (adaptation strategy), that can be deployed in the cluster to achieve high level of self-adaptation in response to changes in its operating environment. The problem of self-healing architecture requires an algorithm to learn how to choose an adaptation action from an infinitely large action space and to optimise the adaptation action to guarantees that the architecture will reach the adaptation objectives [34]. This objective can be achieved using reinforcement learning algorithm, which can guarantee high accuracy of selecting the best adaptation action that fits in the current execution context.

Our adaptation strategy follows Markov Decision Process (MDP). MDP defined as set of states  $s \in S$  and actions  $a \in A$ . The transition model from state  $s$  to state  $s'$  is defined as a function  $T(s, a, s')$  and the reward of this action in the new state  $s'$  is defined by  $R(s, a, s')$ , which return a real value every time the system moves from one state to another. In Mircoservices architecture the set of possible adaptation actions are identified based on the observation of the current state of the cluster. This require identifying a set of sequential actions to adapt the contextual changes by executing an adaptation action to reach the adaptation objectives or quality of services. This means, that the adaptation manager will be rewarded with positive value once it reach the adaptation objectives (i.e. service convergence). Also the adaptation

manager will be rewarded negative value for every failed adaptation action.

However, the adaptation manager with discrete adaptation actions has no idea what the transition probabilities are (it does not know  $T(s, a, s')$ ), and it does not know what the rewards are going to be either (it does not know  $R(s, a, s')$ ) once it moves from one state to another. It must experience each state and each transition at least once to know the rewards, and it must experience them multiple times if it is to have a reasonable estimate of the transition probabilities. Knowing the optimal state value is very useful in identify the best adaptation action. Bellman [35] found an algorithm to estimate the optimal state-action values called Q-values. The Q-value of a state-action pair is noted by  $Q(s, a)$ . The  $Q(s, a)$  refers to the sum of discounted future rewards that the adaptation action expect to reach in a state  $s$  after selecting the adaptation action  $a$ . Q-value estimation is not applicable in environment with large set of states and actions. Alternatively, neural network could be used to estimate the Q-value by defining approximation function and train the model in deep Q-network, this approach is called Deep Approximate learning (Deep Q-learning). Deep Q-learning is a multi-layered neural network that for a given state  $s$  outputs a vector of action values using Markov Decision Process [35] and it uses approximation function to estimate the Q-value  $Q(s, a)$ .

So, our adaptation manager will be using a deep Q-learning approach for identifying the best adaptation action that can return the highest reward once it reaches the desired adaptation objective. For this aim, we need to defined the reward function i.e. Q-value  $Q(s, a)$  using function approximation technique. To achieve this, we need to look back at the state  $s$  of the Microservice architecture (see Figure 1. At each state  $s$  of the Microservice architecture there is a set of context values  $c \in C$  measuring the matrices of operating environment such as: CPU, Memory, Disk I/O and Network. The Anomaly detection services provides us with useful information about how anomalous the current cluster start comparing to the distribution of the previous learned state of the Microservice architecture. Our target is to provide the Deep Q-Learning algorithm with a scalable value that can be used to assign a weight  $w(s, c)$  for all context values  $c$  found in state  $s$ .

At each state  $s$ , the Anomaly detection service calculates the Anomaly Score ( $as$ ) and Anomaly Likelihood ( $al$ ) of all current context values  $c$ . The anomaly likelihood is accurately defining how anomalous the current context value comparing to the distribution of previously learned values about that specific context  $c$ . This enables the adaptation manager to scale the weight of each metric value over the distribution value calculated and aggregated in the anomaly likelihood value. The anomaly likelihood is a scaler value between 0 to 1, meaning if the context  $c_1$  is referring to the value of CPU usage of 70% and the Anomaly Likelihood  $al(cpu)$  value is 1 then this might give the Q-learning algorithm higher probability in selecting an adaptation action that would add new node to the cluster to reduce the CPU load

and keeping the cluster in the desired state. By desired state we mean the state that would return the highest reward to the adaptation manager.

In this paper, we assuming that both the anomaly detection and Deep Q-learning algorithms are fully trained at the initial state  $s_0$ , which normally the state following the deployment of the Microservices cluster, So at each new state, the adaptation manager perform the following functions:

- 1) Get the current observation from the metric database service *GetObservation(s, c)*, which return all metric values from the metrics database.
- 2) Get the current anomaly score, anomaly likelihood from the anomaly detection service *GetAnomalyScore(s, c)*. This function call the Anomaly detection service to return the values of Anomaly Score and Anomaly Likelihood for each context value  $c \in C$ , this will return a vector of the calculated values.
- 3) Get the possible adaptation action  $a \in A$  defined by the Dev-Ops. Those actions could be adding/removing node, scale a services in/out, trigger auto recovery and roll-back to previous state or stay at the current state .
- 4) Finally, the DQN will run the adaptation policy for several times and at each step it will calculate the reward from executing the chosen action but it will not apply the action yet. After running several episodes, it will compute each action score, which is the action that return less anomaly likelihood. This will allows the DQN to balance the adaptation action by calculating the highest probability  $y = 1 - al(c)$  that achieve the lowest value of the Anomaly likelihood.

### C. ADAPTATION POLICY GRADIENT

To provide this model with dynamic policy election that guarantees high accuracy of selecting the best adaptation action that fits in the current execution context. The adaptation manager implements a policy election process by employ a utility function to calculate the probability of transition from one state to another. This where the anomaly detection service plays a significant role. At each state  $s$  of the Microservice architecture there is a set of context values  $c_1, \dots, c_m$  measuring the matrices of operating environment such as: CPU, Memory, Disk I/O and Network.

The Anomaly detection service reads the current values of all matrices and calculates the Anomaly Score  $as_1, \dots, as_m$  and Anomaly Likelihood  $al_1, \dots, al_m$  of the current metric value in the current state. The anomaly likelihood is accurately defining how anomalous the current metric value comparing to the distribution of learned values by the anomaly detection service. This enables the adaptation manager to scale the weight of each metric value over the distribution value calculated and aggregated in the anomaly likelihood value. The anomaly likelihood is a scaler value between 0 to 1, meaning if the  $al_{cpu}$  is 1 and  $c_2$  refers to the CPU usage value is 70% then this might give this metric high utility dimension so it might to be considered in the next adaptation action, so the adaptation manager will select an adaptation

policy that can reason about the anomalous behaviour of the CPU value. In another scenario, if the anomaly likelihood is 0, this would give the metric low utility dimension so it will not be considered in the next adaptation action by the adaptation manager as it will return a low reward to the algorithm.

$$W(al_m, C_m) = \sum_{i=1}^m al_i \cdot c_i \quad (1)$$

$$U(C_m) = \max(W(al_m, C_m) \cdot as_m) \quad (2)$$

From utility theory, a von Neumann-Morgenstern utility function  $U_i : X_i \rightarrow \mathbb{R}$  assigns a real number to each quality dimension  $i$ , which we can normalize to the range  $[0, 1]$  [?]. Across multiple dimensions of contextual changes  $C_m$ , we can attribute a percentage weight to each dimension to account for its relative importance compared to other dimensions. These weights form the utility preferences. The overall utility is then given by the utility preference  $w(c_m)$  function calculated using equ. 1. For example, if three objectives,  $u(cpu)$ ,  $u(memory)$ ,  $u(disk)$ , are given anomaly likelihood as follows: the first is twice as important as the second, and the second is three times as important as the third. Then the weight would be quantified as  $[w1 : 0.6, w2 : 0.3, w3 : 0.1]$ , where the weight is the Anomaly Likelihood of each metric. This gives the CPU metric higher priority to be consider in the adaptation action.

In this paper. We argue that the use of anomaly likelihood to weight the collected metrics provides an accurate calculation of the utility function and provides the model with better estimation of the adaptation action. So the maximum metric is selected using the equation described in 2, which select the maximum  $W$  of specific metric value that has the highest Anomaly Score returned by the Anomaly detection service.

$$Cost(u_m) = \frac{(Current(c_m) - Predicted(c_m)) \cdot (as(c_m) \cdot W(al_m, C_m))}{UsageTime(u_m) * Cost(instanceType)} \quad (3)$$

In addition to that, an accurate calculation is needed, that calculates the required number of nodes needed to meet the demand of the adaptation action and at the same time maintain the resource provisioning within the allocated budget by the Dev-Ops. The utility cost of provisioning a new node/container in the architecture is calculated based on the equ. 3, the  $Current(c_m)$  is the current value of the metric value. The  $Predicted(c_m)$  refers to the Predicted value of the utility dimension. The  $AnomScore(c_m)$  is the Anomaly Score of the utility dimension at time  $t_i$ , and  $W_i$  is the anomaly likelihood value of metric value. The  $Predicted(c_m)$ ,  $AnomScore(c_m)$ , and  $W(c_m)$  are provided by anomaly detection service implemented based on NUPIC. The  $UsageTime(u_m)$  refers to the total number of hours the node is expected to be used per/day, this value is calculated based on the rate of changes calculated based on equ. 4. The  $Cost(instanceType)$  is the cost in \$ for provisioning an

instance per/day, normally this is a constant value specified by the cloud infrastructure provider based on the instance type. Finally, the value of  $Cost(u_m)$  is calculated against the constraint of  $budget$  as  $Cost(u_m) \leq budget$ . The  $budget$  is assigned by the Dev-Op to reflect the value of the available budget, so the adaptation manager will not exceed this value at any case. A negative value returned by  $Cost(u_i)$  function means the number of nodes/replicas in the cluster should be reduced by the adaptation action.

$$\Delta U_m = \sum_i^m (W_m - W_{m-1}) \quad (4)$$

To summarizes our proposed model. So to achieve highly level of self adaptability, this research implements a MAPK model that employ Markov Decision Process in identifying the transition model from one cluster state to another. Also, it employees a Deep Q-learning algorithm that able to select the optimal adaptation action that returns the highest reward from adaptation execution. At the same time, the use of reinforcement learning guarantees that the learned knowledge from each pair of action-state is learned by the Deep Q-learning, which will prevent the adaptation manager from executing adaptation action that would fail and return negative reward. In the following section, we will describe the experiment setup and the tools used to construct the Microservices architecture. Also, we will describe the structure of the neural network used in this experiment.

## IV. RESULTS

### A. EXPERIMENT SETUP

To validate the ideas presented in this paper, we design and develop a working prototype of Microservice architecture in Docker swarm<sup>3</sup> as shown in Figure 1. The cluster consisted of manager and worker nodes. Each cluster has one leader, which maintains the cluster state and preserves the cluster logs. Also, the leader node initializes the vote of Raft Consensus Algorithm [33] to agree/disagree on specific value based on the consensus by all nodes in the cluster. Only the leader node is allowed to commit and maintain all variable values and logs. To meet scalability and availability, the leader node distributed the work load between the workers based on Raft Consensus Algorithm [33]. This means that each service could be executed by assigning multiple containers across the cluster's nodes.

The main services implemented in this architecture are: Time series metrics database for context collection, Nodes metrics used to collect metrics from all nodes in the cluster, Alert and notification manager used to notify the adaptation manager about contextual changes offered by Prometheus framework<sup>4</sup>. Docker containers metrics collector for collecting fine-grained metrics about all running containers in all nodes<sup>5</sup>. Reverse proxy for routing traffic between all services

<sup>3</sup><https://docs.docker.com/engine/swarm/>

<sup>4</sup><https://prometheus.io>

<sup>5</sup><https://github.com/google/cadvisor>

in the cluster<sup>6</sup>. Unsupervised Real-time Anomaly Detection based on NUPIC<sup>7</sup>, Adaptation manager for executing, validating the adaptation actions developed as a prototype of this research. Time series analytic and visualisation dashboard for observing the behaviour of the Microservices cluster<sup>8</sup>. The adaptation manager implements a deep Q-learning Network using Tensorflow framework<sup>9</sup>.

A deep Q-learning Network using Tensorflow framework<sup>10</sup>. The neural network architecture consisted from three layers. The input layer is the size of the observation space. In this experiment, we collect CPU usage, Memory usage, Disk space, Network I/O. The second layer is dense hidden layer of 8 units. The third layer is the output layer which will be the probability  $y = 1 - \text{al}(c)$ . The output layer uses logistic (softmax) activation function. Finally, we use a cost function of softmax cross entropy with logits to select the best action. The DQN was implemented using Adam Optimizer, which is used to calculate the policy gradient at each state action pair and return the highest reward. A full code of the adaptation manager and services stack used in this experiment can be found in<sup>11</sup>. This live snapshot<sup>12</sup> provides a full virtualisation of all services running in the cluster.

The evaluation of the effectiveness of this model will be based on calculating a approximation function for all metrics monitored, then it will calculate the number of adaptation attempts, successful convergence of services/nodes, or errors which leads to unstable state of the cluster.

The evaluation of this model will come in three folds: First, evaluating the consistent behaviour of the cluster by evaluating the state of the swarm after executing a set of adaptation actions. Second, evaluating the accuracy of the model in electing the correct adaptation action by identifying the highest metric value that need to be consider in the adaptation. Third, Evaluating the accuracy of the anomaly detection service using confusion matrix [36], as described in the following section.

## B. DISCUSSION

First we run a stress test in the cluster manager until its CPU usage reaches 70%, which triggers an alert to the adaptation manager. The adaptation manager collects the current reading of the metrics, anomaly score, and anomaly likelihood (see figure 1). Then, the adaptation manager calculates the rate of changes in each metric to elect the metric that has the highest utility dimension. As example, Figure 2 is showing the utility of CPU usage, Memory usage, Disk reads (bytes/s), Disk writes (bytes/s), Docker Network (sent/received bytes/s). The CPU usage has the highest utility as confirmed by the Utility indifference indicator shown in Figure 2. Also, the

memory usage of the service shows slow rate of changes over time, which make it optional to be considered in the adaptation action. With regard to the utility of Disk Read/Write, the Figure 2 shows no divergent above the moving average (i.e. utility indifference curve) so it will not be considered in the next adaptation action. The docker network shows no changes over the time of the experiment as the load balancer and the reverse proxy manage to divert the traffic to many containers distributed in the cluster.

As the  $Utility_{(CPU)}$  has the highest value of changes as shown in Figure 2. This will trigger an adaptation action to reason about the high demand of CPU usage, so the adaptation manager will create additional nodes and add them to the swarm cluster automatically. The number of nodes is equals to the utility cost calculated as in equ. 4. This results in adding new nodes to the swarm as shown in the snapshot<sup>13</sup> (A full visualised and analytics dashboard of the swarm after the adaptation). Once the CPU demand is reduced, the adaptation manager will calculate the variations of the utility and remove number of nodes equals to value returned by the utility cost function in equ. 4. A snapshot<sup>14</sup> of the system after executing the adaptation action to reason about the low level of the cpu usage.

In another scenario, we simulated Distributed Denial of Service attack to a web service running in the swarm, to verify that the adaptation manager will be able to accommodate the DDOS attack by adding more replicas to the service. In this case, we wish to verify the ability of the proposed model to dynamical adjust the number of service's replicas against the variations of the CPU usage and to maintain an acceptable response time of the web service. At the same time, it is very important that the adaptation action would not scale the service endlessly. So the utility cost is calculated to count the number of replicas needed. The outcome of this experiments is shown in Figure 4. The figure show how the number of scaled replicas are tuned linearly against the CPU usage. Also, it shows the number of steps taken by the adaptation manager to execute the scaling policy in/out. The adaptation manager counts the utility of the CPU metric and the utility cost to define the number of added/removed replicas. The adaptation manager waits for receiving a high utility value by sending heartbeat signal to get the latest value of utility dimension and cost every 20s for a window of 300s. Once the utility of the CPU get the highest utility dimension, the adaptation manager calculates the number of replicas to be added/removed to the service. Also, the number of steps needed to achieve the desired state are counted as shown in Figure 4. The number of steps needed to perform the adaptation varies based on the severity and variation of the utility cost over time. Once the adaptation is applied and verified by winning the consensus algorithm votes, the service will be scaled and the adaptation manager puts a cool off timer of 300s before initiating new adaptation action.

<sup>6</sup><https://caddyserver.com/docs/proxy>

<sup>7</sup><http://nupic.docs.numenta.org/stable/index.html>

<sup>8</sup><https://grafana.com>

<sup>9</sup><https://www.tensorflow.org>

<sup>10</sup><https://www.tensorflow.org>

<sup>11</sup><https://github.com/baselm/mgr-selfhealing.git>

<sup>12</sup><https://snapshot.raintank.io/dashboard/snapshot/UJlrTzwubrRQjDwM1YFJle5zvdlKQA7Znplde2>

<sup>13</sup><https://snapshot.raintank.io/dashboard/snapshot/sstuT2tuYkob8zJbh1YXzBYxSJl>

<sup>14</sup><https://snapshot.raintank.io/dashboard/snapshot/UJlrTzwubrRQjDwM1YFJle5zvdlKQA7Znplde2>



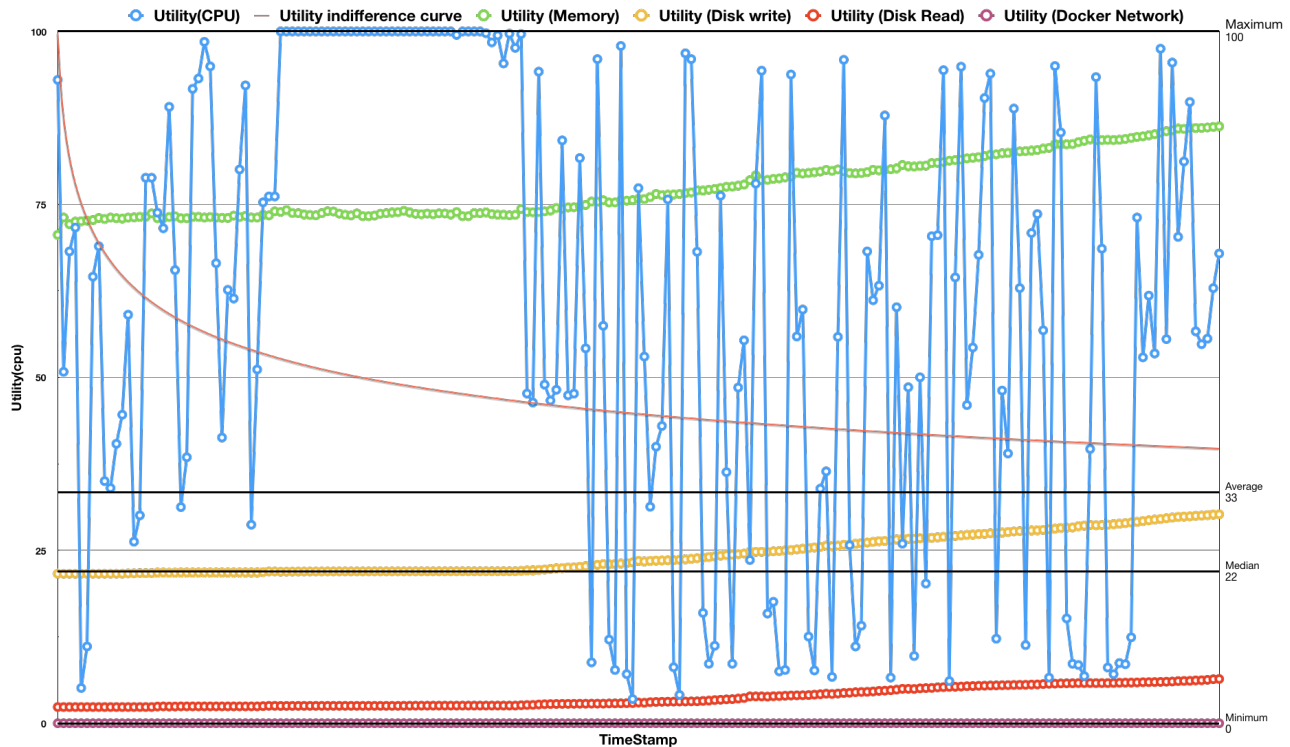


FIGURE 2. Dimensional analysis of variations of utility functions

Also, it reset the steps timer.

The accuracy of the utility cost, rate of changes, and the maximum utility dimension are vital for the success of the adaptation process. So, Figure 3 depicts the calculation of the rate of changes and the utility cost to reach the desired number of nodes/replicas needed. We find the calculation accurately satisfies the adaptation objectives and provides the architecture with accurate calculation of the needed number of nodes/replicas. As shown in Figure 3, the number of nodes increases at the right time when the CPU demand spikes, then the number of nodes/replicas reduced just before the CPU demand is declined significantly as shown in Figure 3. The rate of changes in CPU usage declined so the Utility cost return negative value for the required number of nodes/replicas as long they are above the minimum number of nodes/replicas specified by the Dev-Ops. Also, as shown in Figure 3 The utility cost normalizes and tunes the CPU demand. This provides a great evidence that the employment of the utility dimension provides the adaptation cycle a dynamic variability over the needed/allocated resources. Instead of scaling the architecture in/out according to a static threshold.

The accuracy of the anomaly score and likelihood plays an important role for the successes the proposed model. So, in the following we will evaluate the accuracy of the anomaly detection algorithm implemented in this model. A famous technique for evaluating anomaly detection algorithm is the use of a confusion matrix [36]. The confusion matrix represents the total number of records inspected by algorithm

as shown in Table 1. The matrix represents the relationship between the actual levels of normal behaviour and the detected level of normal behaviour by the algorithm. Also, it represents the relationship between the actual anomaly recorded in the system and the predicted/identified anomaly that the algorithm identified as anomalous behaviour.

In case of our proposed model, If NUPIC anomaly detection considered a specific record as anomalous and it was an actual anomaly then this attempt is classified as a **True Positive**. If NUPIC classifies the data as normal behaviour and it was normal data then this attempt is classified as **True Negative**. If NUPIC classifies an anomalous behaviour as normal behaviour this means that NUPIC failed to detect anomaly. In the case, this attempt is classified as **False Negative**. If NUPIC classifies the data as anomalous behaviour but the data was normal behaviour then this attempt is considered a **False Alarm/False Positive**. Both True Positive and False Positive are important benchmark to measure the accuracy of intrusion detection systems. Table 1 summarizes the values used for evaluating the anomaly detection algorithm we used in this paper. The confusion matrix will be used to calculate the model detection rate, false positive, and accuracy. Those results will be compared against SNORT<sup>15</sup> [20]. SNORT is implemented as a container in the leader node of the cluster (see Figure 1). Based on the calculations of NUPIC anomaly detection shown in Table 1 and Snort in Table 2, it was found that our proposed model of using NUPIC performs

<sup>15</sup><https://snort.org>

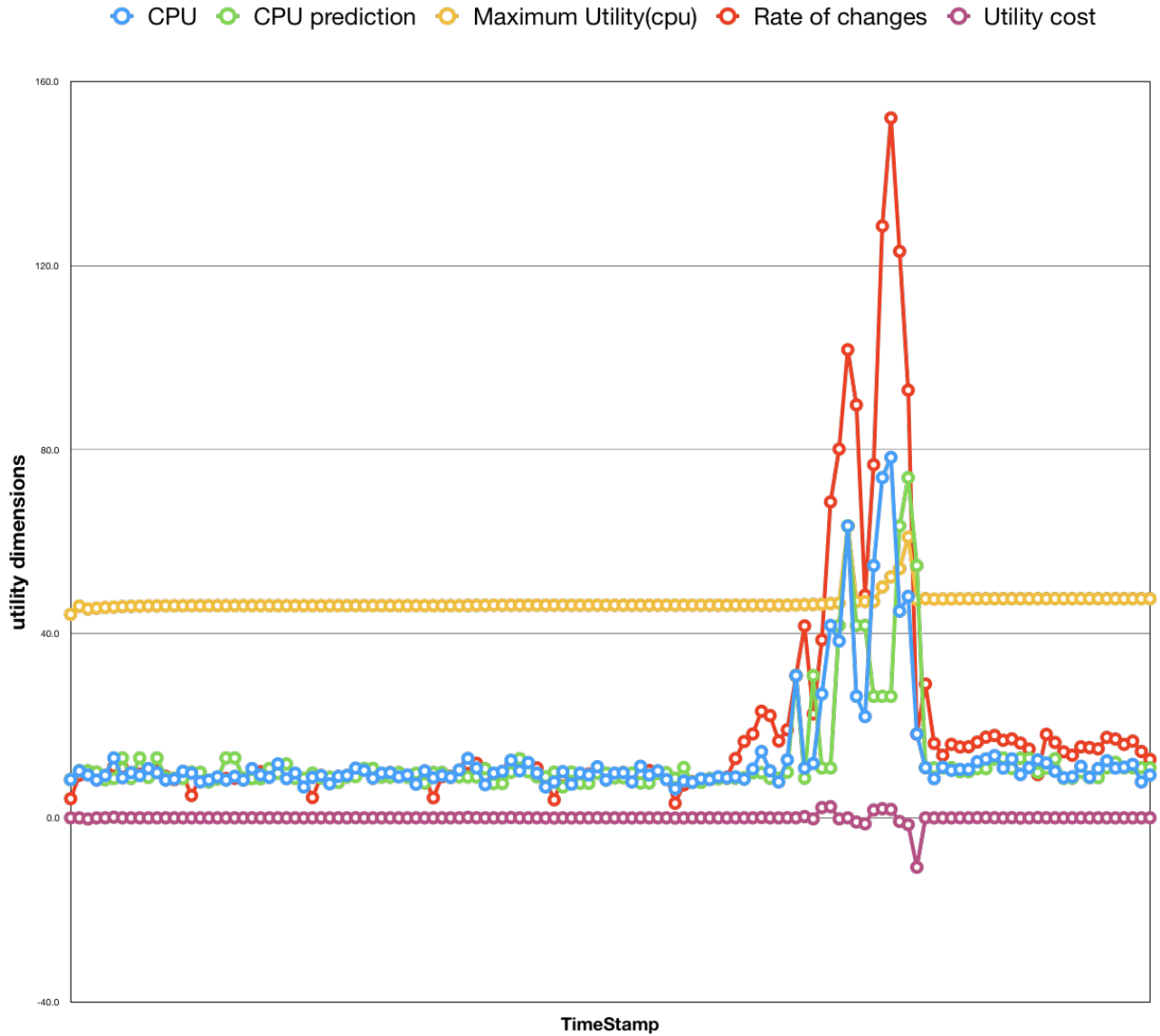


FIGURE 3. Utility(cpu) rate of changes and Cost calculated based in equ. 3 and 4

significantly better in terms of the detection rate, false alarms, and accuracy. The false alarm rate in the model (0.0264) is lower than SNORT (1,12). In addition, the model provides a high rate of true alarms and anomaly detection as summarised in Table 3. The equations used in this evaluation are listed in 3.

TABLE 1. Results of the proposed anomalies detection model on confusion matrix

X= 1528	Predicted anomalies	Predicted normality
Actual anomalies (TP + FN) (55)	TP = 49	FN = 6
Actual normalities (FP + TN) (1473)	FP/ False Alarm = 38	TN = 1435

The values in Table 3 clearly show that the proposed model performs better in terms of false alarms, detection rate, and accuracy. A further calculation, as shown below, could provide a better idea of the performance of the proposed model.

TABLE 2. Results of the SNORT anomaly detection on confusion matrix

X= 1528	Predicted anomalies	Predicted normality
Actual anomalies (TP + FN) (55)	TP = 32	FN = 23
Actual normalities (FP + TN) (1473)	FP/ False Alarm = 62	TN = 1411

The detection rate of SNORT is  $32 / ((32 + 62)) = 0.340$  and this indicates that the proposed model has a better detection rate, as the proposed model used a machine-learning algorithm to build a model about the data and provides a prediction for each value. Those factors improve the detection rate compared with SNORT, which used a rule-based engine to match the incoming traffic and pre-configured rules.

The False Alarm of the proposed model is 0.0257. This indicates that the proposed model has a very low rate of providing a false alarm or identifying normal behaviour as

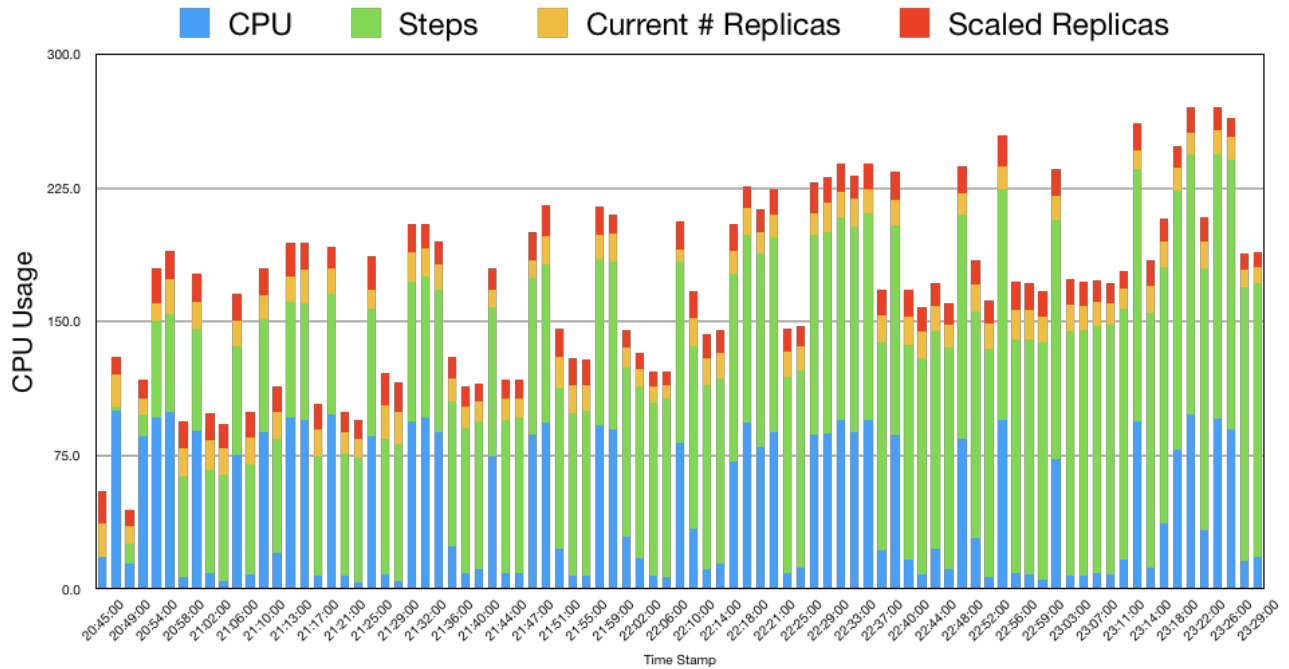


FIGURE 4. Dynamic Scaling of Web Service

TABLE 3. Comparison between SNORT Anomaly Detection and the Proposed Model

Rate	NUPIC	SNORT	Result
Accuracy	0.97	0.944	Implementation of NUPIC provides better accuracy $Accuracy = (TP + TN)/x$ , over the SNORT anomaly detection.
Misclassification	0.0287	0.0554	The rate of false alarms is lower in the proposed model compared with SNORT. The Misclassification is calculated using $Misclassification = (FP + FN)/x$
True Positive Rate (TP)	0.89	0.58	$TP\ rate = TP/(Actual\ anomalies\ in\ x)$ . The rate of true alarms in the model is significantly better than SNORT.
False Positive (FP)/ False Alarm	0.0264	1.12	The proposed model has a lower rate of incorrect classification of attacks calculated using $FP\ rate = FP/(Actual\ in\ x)$ , but SNORT has a higher rate of not detecting attacks and considering them as normal behaviour
True Negative (TN)	0.998	0.981	Both models- SNORT and the proposed model- have a good rate of detecting the normal behaviour of the system as calculated by $TN\ rate = TN/(Actual\ in\ x)$ . However, the proposed model provides better results.
Precision	0.89	0.58	The precision $Precision = TP/(Predicted\ anomalies\ in\ x)$ , of the proposed model is far better than SNORT. The gap between the two models is clear.
Prevalence	0.03599	0.03599	Both models have the same prevalence rate calculated by $Prevalence = (Actual\ anomalies)/x$ as the DDOS was simulated as part of the experiment.

anomalous. In the contrast, the false alarm for SNORT is  $62/((62 + 1411)) = 0.042$ . This value is a clear indication that SNORT would provide more false alarms about normal traffic in the system. This is due to the fact that SNORT considers one factor of identifying an anomaly which is the network traffic. In contrast, the proposed model continuously observed and learned the behaviour of so many performance criteria about the cluster in addition to the network traffic.

The overall accuracy of the proposed model is 0.97. The accuracy of SNORT is 0.944, due to the fact that SNORT is continuously monitoring the system network, but it has

no means of understanding the behaviour of the system. The proposed model builds an accurate model of the system behaviour so it has better insight into any fluctuations or spikes in the data. This feature is considered to be very important for the success of the adaptation strategy and the self-healing property of the Microservices architecture.

However, we believe that this model manages to offer the Microservices architecture with continuous monitoring, continuous detection of anomalous behaviour, and provides the architecture with dynamic decision making based on the employment of multidimensional utility-based model.

The results in above, shows high accuracy in detecting the anomaly and an accurate calculation of variant adaptation actions. It Also shows high success rate in performing horizontal and vertical autoscaling in response to contextual changes.

## V. CONCLUSIONS AND FUTURE WORK

This model manages to offer the Microservices architecture with continuous monitoring, continuous detection of anomalous behaviour, and provides the architecture with dynamic decision making based on the employment of multidimensional utility-based model. The results in above, shows high accuracy in detecting the anomaly and an accurate calculation of variant adaptation actions. It Also shows high success rate in performing horizontal and vertical scaling in response to contextual changes. The uses of utility-based model enables the architecture to dynamically elect a reasoning approach based on the highest utility dimension of context changes in the operational environment. The self-healing property is achieved by parameter tuning of the running services and dynamic adjustment of the swarm cluster. We believe integrating utility theory in the decision making process improves the effectiveness of the adaptation and reduces the adaptation risk including resources over-provisioning and thrashing. Also, it preserving the cluster state by preventing multiple adaptation to take place at the same time. Enabling a prediction over the metrics of the operational resources enables the architecture to schedule a proactive adaptation actions.

This model supports vertical and horizontal scaling of the Microservices architecture, but it requires further improvement with regard to services compositions, and decentralised decision making. Currently, Docker swarm enables the cluster to have one leader, which prevents us from testing this model in multi leaders environment. This enforces us to implement the adaptation manager as a central component in the leader node but it has the ability to execute the adaptation action via the leader node orchestration algorithm. Also, this model requires an enhanced mechanism of run-time configurations, as it supports currently parameter tuning of the architecture configurations. Also, the current implementation of NUPIC requires multiple implementations for each contextual changes. NUPIC has no support for swarming (model training) over multiple variables data model. Finally, we believe the ability of the Microservices to self-heal itself is achievable, but a major question stands related to how we could evaluate the self-healing property of Microservice architecture. This question requires further investigation to find an applicable runtime evaluation mechanisms.

## REFERENCES

- [1] J. Stubbs, W. Moreira, and R. Dooley, "Distributed systems of microservices using docker and serfnod," in Science Gateways (IWSG), 2015 7th International Workshop on. IEEE, 2015, pp. 34–39.
- [2] M. Salehie and L. Tahvildari, "Self-adaptive software: Landscape and research challenges," *Transactions on Autonomous and Adaptive Systems (TAAS)*, vol. 4, no. 2, May 2009.
- [3] G. M. Kapitsaki, G. N. Prezerakos, N. D. Tselikas, and I. S. Venieris, "Context-aware service engineering: A survey," *Journal of Systems and Software*, vol. 82, no. 8, pp. 1285–1297, 2009.
- [4] O. B. M. Jelasity, A. M. C. Fetzer, S. L. A. van Moorsel, and M. van Steen, "Self-star properties in complex information systems," 2005.
- [5] P. Horn, "Autonomic computing: IBM's Perspective on the State of Information Technology," *Tech. Rep.*, 2001.
- [6] B. Cheng, R. de Lemos, H. Giese, P. Inverardi, J. Magee, R. M. Malek, H. Müller, S. Park, M. Shaw, and M. Tichy, "Software Engineering for Self-Adaptive Systems: A Research Road Map (Draft Version)," *Dagstuhl Seminar Proc.* 08031, 2008.
- [7] T. Strang and C. Linnhoff-Popien, "A context modeling survey," in *Workshop on advanced context modelling, reasoning and management, UbiComp*, vol. 4, 2004, pp. 34–41.
- [8] S.-W. Cheng, D. Garlan, and B. Schmerl, "Evaluating the effectiveness of the rainbow self-adaptive system," in *Software Engineering for Adaptive and Self-Managing Systems*, 2009. SEAMS'09. ICSE Workshop on. IEEE, 2009, pp. 132–141.
- [9] M. Mikalsen, N. Paspallis, J. Floch, E. Stav, G. A. Papadopoulos, and A. Chimeris, "Distributed context management in a mobility and adaptation enabling middleware (madam)," in *Proceedings of the 2006 ACM symposium on Applied computing*. ACM, 2006, pp. 733–734.
- [10] D. Cheung-Foo-Wo, J. Y. Tigli, S. Laviotte, and M. Riveill, "Self-adaptation of event-driven component-oriented middleware using aspects of assembly," *Proceedings of the 5th international workshop on Middleware for pervasive and ad-hoc computing: held at the ACM/IFIP/USENIX 8th International Middleware Conference*, pp. 31–36, 2007.
- [11] W. Wei, X. Fan, H. Song, X. Fan, and J. Yang, "Imperfect Information Dynamic Stackelberg Game Based Resource Allocation Using Hidden Markov for Cloud Computing," *IEEE Transactions on Services Computing*, vol. 11, no. 1, pp. 78–89, Feb. 2016.
- [12] D. A. Menascé and V. Dubey, "Utility-based qos brokering in service oriented architectures," in *Web Services, 2007. ICWS 2007. IEEE International Conference on*. IEEE, 2007, pp. 422–430.
- [13] K. Kakousis, N. Paspallis, and G. A. Papadopoulos, "Optimizing the utility function-based self-adaptive behavior of context-aware systems using user feedback," in *OTM Confederated International Conferences "On the Move to Meaningful Internet Systems"*. Springer, 2008, pp. 657–674.
- [14] M. Sama, D. S. Rosenblum, Z. Wang, and S. Elbaum, "Model-based fault detection in context-aware adaptive applications," in *Proceedings of the 16th ACM SIGSOFT International Symposium on Foundations of software engineering*. ACM, 2008, pp. 261–271.
- [15] R. Hirschfeld, P. Costanza, and O. M. Nierstrasz, "Context-oriented programming," *Journal of Object technology*, vol. 7, no. 3, pp. 125–151, 2008.
- [16] R. De Lemos, H. Giese, H. A. Müller, M. Shaw, J. Andersson, M. Litoiu, B. Schmerl, G. Tamura, N. M. Villegas, T. Vogel et al., "Software engineering for self-adaptive systems: A second research roadmap," in *Software Engineering for Self-Adaptive Systems II*. Springer, 2013, pp. 1–32.
- [17] A. Patcha and J.-M. Park, "An overview of anomaly detection techniques: Existing solutions and latest technological trends," *COMPUTER NETWORKS*, vol. 51, no. 12, pp. 3448–3470, Aug. 2007.
- [18] C. Kruegel and G. Vigna, "Anomaly detection of web-based attacks," in *Proceedings of the 10th ACM conference on Computer and communications security*. ACM, 2003, pp. 251–261.
- [19] D. Anderson, T. Frivold, and A. Valdes, "Next-generation intrusion detection expert system (NIDES): A summary," 1995.
- [20] M. Roesch, "Snort: Lightweight intrusion detection for networks," in *Lisa*, 1999, pp. 229–238.
- [21] C. Phua, V. Lee, K. Smith, and R. Gayler, "A comprehensive survey of data mining-based fraud detection research," *arXiv preprint arXiv:1009.6119*, 2010.
- [22] D. Gupta, S. Singhal, S. Malik, and A. Singh, "Network intrusion detection system using various data mining techniques," in *Research Advances in Integrated Navigation Systems (RAINS)*, *International Conference on*. IEEE, 2016, pp. 1–6.
- [23] A. L. Buczak and E. Guven, "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1153–1176, May 2016.
- [24] T. Bujlow, T. Riaz, and J. M. Pedersen, "A method for classification of network traffic based on C5. 0 Machine Learning Algorithm," in *Computing, Networking and Communications (ICNC)*, 2012 *International Conference on*. IEEE, 2012, pp. 237–241.



- [25] V. Golmah, "An efficient hybrid intrusion detection system based on C5.0 and SVM," *International Journal of Database Theory and Application*, vol. 7, no. 2, pp. 59–70, 2014.
- [26] N. F. Haq, A. R. Onik, M. A. K. Hridoy, M. Rafni, F. M. Shah, and D. M. Farid, "Application of machine learning approaches in intrusion detection system: a survey," *IJARAI-International Journal of Advanced Research in Artificial Intelligence*, vol. 4, no. 3, pp. 9–18, 2015.
- [27] J. Hawkins and S. Blakeslee, *On Intelligence*. Macmillan, Apr. 2007.
- [28] S. Ahmad and S. Purdy, "Real-Time Anomaly Detection for Streaming Analytics," *arXiv preprint arXiv:1607.02480*, vol. abs/1607.02480, 2016.
- [29] A. Lavin and S. Ahmad, "Evaluating Real-time Anomaly Detection Algorithms - the Numenta Anomaly Benchmark," *CoRR*, vol. abs/1510.03336, pp. 38–44, 2015.
- [30] S. Ahmad, A. Lavin, S. Purdy, and Z. Agha, "Unsupervised real-time anomaly detection for streaming data," *Neurocomputing*, vol. 262, no. Supplement C, pp. 134–147, 2017.
- [31] J. W. Craig, "A new, simple and exact result for calculating the probability of error for two-dimensional signal constellations," in *Military Communications Conference, 1991. MILCOM'91, Conference Record, Military Communications in a Changing World., IEEE*. IEEE, 1991, pp. 571–575.
- [32] A. Computing et al., "An architectural blueprint for autonomic computing," *IBM White Paper*, vol. 31, pp. 1–6, 2006.
- [33] D. Ongaro and J. K. Ousterhout, "In search of an understandable consensus algorithm," in *USENIX Annual Technical Conference, 2014*, pp. 305–319.
- [34] H. Van Hasselt, "Reinforcement learning in continuous state and action spaces," in *Reinforcement learning*. Springer, 2012, pp. 207–251.
- [35] R. Bellman, "A Markovian decision process," *Journal of Mathematics and Mechanics*, pp. 679–684, 1957.
- [36] R. Kohavi and F. Provost, "Confusion matrix," *Machine learning*, vol. 30, no. 2-3, pp. 271–274, 1998.

• • •