A Monitoring System for Anomaly Detection in Fog Manufacturing

Lening Wang
Grado Department of Industrial and Systems Enginnering
Virginia Tech
Blacksburg, USA
yutongz@vt.edu

Yutong Zhang
Grado Department of Industrial and Systems Enginnering
Virginia Tech
Blacksburg, USA
wangln@vt.edu

Ran Jin
Grado Department of Industrial and Systems Enginnering
Virginia Tech
Blacksburg, USA
jran5@vt.edu

***Abstract*—Fog manufacturing is an advanced manufacturing system that integrates Fog computing with interconnected manufacturing processes. It can provide responsive and robust computation services compared with Cloud manufacturing. However, the performance of Fog manufacturing is still not satisfactory due to various anomalies such as inappropriate architecture designs, cyber-attacks, etc. These problems can lead to anomalies in Fog manufacturing and can impede the wide adoption of Fog manufacturing. To quickly detect the anomalies in Fog manufacturing during operations, a monitoring system is desirable. Therefore, in this paper, we proposed a monitoring system based on statistical process control (SPC) methods to comprehensively monitor different types of anomalies in Fog manufacturing. The exponentially weighted moving average (EWMA) and risk-adjusted (RA) charts are adopted to detect different anomalies based on corresponding monitoring statistics. A simulation study and a real case study based on a Fog manufacturing testbed are implemented to evaluate the performance of the proposed monitoring system. The result shows the proposed monitoring system can quickly and efficiently detect different types of anomalies in Fog manufacturing. This monitoring system can also potentially help to improve architecture designs and offloading strategies by further analyzing the root causes of a specific anomaly in future work.**

Keywords—Anomaly Detection, Fog Manufacturing, Modeling, Monitoring, Real-time Information System

I. Introduction

Fog manufacturing is an interconnected manufacturing network embedded with a Fog computing system to provide a responsive and high data privacy computation service in the industrial cyber-physical system [1, 2]. Instead of a Cloud computing system that requires high bandwidth utilization and reliable network connection to integrate all information on Cloud, a Fog computing system can distribute computation tasks and data storages onto Fog nodes to simultaneously execute computation tasks and keep the sensitive data locally [2]. Therefore, in a Fog manufacturing system, the data collected from the physical manufacturing system can be efficiently secured and analyzed via Fog computing. The corresponding data analysis results can further support effective decision-making to improve the flexibility and efficiency for manufacturing [2].

On the other hand, there are still some limitations that affect the reliability and accessibility of Fog manufacturing in practice [3]. More specifically, the anomalies can significantly affect the computation performance (e.g., time latency, analysis accuracy, etc.) in a Fog manufacturing system. For example, anomalies such as communication fluctuations (i.e., variations on bandwidth consumption over time) and computation fluctuations (i.e., variations of CPU utilization over time) can lead to inefficient and ineffective computation tasks in the Fog manufacturing system. Moreover, other anomalies such as inappropriate architecture designs [4] (e.g., imbalanced workload among Fog nodes), and cyber-attacks [5] can also significantly affect the performance of computation services and data privacy. Therefore, it is necessary to develop a monitoring system based on efficient methods, such as statistical process control (SPC), in Fog manufacturing to quickly detect these anomalies during operations. Based on the monitoring system, the operator/operation system can identify and react to anomalies in time.

In the context, the objective of this work is to propose a monitoring system to detect anomalies in Fog manufacturing based on SPC methods. However, due to the complexity of a Fog manufacturing system, there are many types of the anomaly which have not been comprehensively defined. Moreover, it is difficult to identify the proper monitoring statistics for each anomaly scenario. In the literature, there are many variables, such as computation complexity, sample number, etc., which can indirectly reflect the variations of the Fog manufacturing system, which have been defined . But how to utilize these variables to improve the accuracy and efficiency of the monitoring system is still unclear.

In the literature, anomalies in Cloud manufacturing have been intensively studied. For example, Tan et al. presented a predictive performance anomaly prevention (PREPARE) system to detect anomalies on the performance of computation services, such as CPU *hog* (i.e., the competition on CPU utilization), bottleneck (i.e., high workloads until hitting the capacity limit), etc., via the combination of attribute value prediction and supervised anomaly classification methods [6]. Lo et al. proposed a cooperative intrusion detection system (IDS) for the anomaly detection on denial-of-service (DoS)

This research is partially supported by ICTAS junior faculty award "Fog Computing based Smart Additive Manufacturing" at Virginia Tech, 2018.

978-1-7281-6389-5/20/$31.00 ©2020 IEEE

attack, which makes the judgment on the warning message via the majority vote method within the cooperative system [7]. Guan and Fu introduced an adaptive anomaly detection method for hardware failures via exploring the most relevant performance data generated from Cloud (e.g., CPU utilization) of different failure types [8]. In summary, there are many anomaly scenarios defined for Cloud manufacturing. However, because the Fog manufacturing has different structure compared with Cloud manufacturing, even though a portion of knowledge from the Cloud manufacturing can be adopted, it is still unclear how the abnormal scenarios should be defined and what are the corresponding monitoring statistics.

On the other hand, different types of SPC methods have been widely used to quickly and efficiently detect anomalies in systems. For example, the X-bar chart, which monitors the mean of samples within a time period, is efficient to detect the mean shift of the system [9]. Exponentially weighted moving average (EWMA) chart, which varies weights among monitoring statistics along time, is widely adopted to efficiently detect the small shift in the process, which is less sensitive to normality assumption [10]. Besides, the risk-adjusted (RA) chart is proposed by integrating corresponding covariates in the system to monitor the residual between the real monitoring statistics and prediction value estimated by covariates [11]. In summary, there are many existing SPC methods that can be potentially used to detect anomalies in Fog manufacturing.

In this paper, a Fog manufacturing is monitored by SPC methods to detect different types of anomalies. First, four categories of anomalies are defined in Fog manufacturing: 1) extreme system utilization, 2) imbalanced workload among Fog nodes, 3) cyber-attacks, and 4) Fog node failures. Moreover, the corresponding monitoring statistics are introduced for each anomaly. The EWMA and RA are adopted for anomalies. The EWMA is designed to detect mean and variance change of CPU and bandwidth utilization, which can be directly measured through the system informatics efforts. The RA chart is designed to detect the DDoS type of cyber-attacks, because the relationship between the CPU or bandwidth utilization and the complexity of the dataset or algorithms reflects the attack; the monitoring of multivariate performance measures in EWMA chart will not be effective to detect the cyber-attacks. To validate the proposed monitoring system, a simulation study was conducted to calculate the Average Run Length (ARL), which evaluate the Type-II error of the monitoring given the same Type-I error [9]. A Fog manufacturing testbed was adopted by executing different types of computation tasks to evaluate the monitoring performance.

The rest of this paper is organized as follows. In section II, the definition of abnormal scenarios and the SPC methods are introduced in detail. Section III validates the detection efficiency of the proposed monitoring system via a simulation study. Section IV discusses the adopted Fog manufacturing testbed and the result of a real case study. Section V summarizes the contributions of this work and discusses future work.

II. Methodology

A. A Monitoring System for Fog Manufacturing

In order to detect anomalies in a Fog manufacturing system, the corresponding abnormal scenarios should be clearly defined based on the engineering domain knowledge. As shown in Table I, the abnormal scenarios are summarized into four categories: 1) extreme system utilization, 2) imbalanced workload among Fog nodes, 3) cyber-attacks, and 4) Fog node failures. The corresponding detection rules, monitoring statistics, and SPC methods are also summarized.

The extreme system utilization represents the scenarios in which the utilization of communication or computation resources (i.e., bandwidth utilization or CPU utilization) are

TABLE I. A List for Abnormal Scenarios

Categories	***Abnormal Scenario Definitions***			
	Scenario Names	***Detection Rules***	***Monitor Statistics***	***Control Chart Types***
Extreme system utilization	High computation loads	High computation utilization	Mean of CPU utilization among Fog nodes	EWMA
	Inefficient computation utilization	Low computation utilization	Mean of CPU utilization among Fog nodes	EWMA
	High communication loads	High communication utilization	Mean of bandwidth utilization among Fog nodes	EWMA
	Inefficient communication utilization	Low communication utilization	Mean of bandwidth utilization among Fog nodes	EWMA
Imbalanced workload among Fog nodes	Imbalanced workload	Imbalanced computation utilization among nodes	Standard deviation of CPU utilization among Fog nodes	EWMA
Cyber-attacks	Distributed denial of service (DDoS)	High bandwidth utilization but low computation utilization	Bandwidth utilization conditional on computation intensity for each Fog node	RA
	Man-in-the-middle	Abnormal prediction accuracy	Accuracy of each computation task	N/A[*]
Fog node failures	Fog node computation failure	Abnormal computation utilization	Computation time latency and CPU utilization for each computation task	N/A[*]
	Fog node communication failure	Abnormal communication utilization	Communication time latency and Bandwidth utilization for each computation task	N/A[*]

[*] (Due to the limited space, we did not focus on these scenarios in this paper)

abnormally high or low compared with normal conditions. The extreme high utilization can significantly affect the performance of a Fog manufacturing system since it can lead to congestion for computation tasks. On the other hand, extremely low utilization can result in communication or computation resource wasting. In order to detect these anomalies, the average bandwidth utilization and CPU utilization of Fog nodes are used as monitoring statistics in a Fog manufacturing system.

The imbalanced workload represents the assignment of computation tasks (i.e., offloading strategy) is not reasonable and leads to imbalanced computation workloads among Fog nodes. This anomaly can downgrade the performance of computation services, such as high time latency and shortened lifetime of some fog nodes, which can further increase the probability of unexpected failures. Therefore, the standard deviation of computation utilization among Fog nodes is employed to detect this anomaly in a Fog manufacturing system.

The cyber-attack is one of the most significant risks in Fog manufacturing. From the literature, there are two major types of cyber-attacks in Cloud/Fog computing platforms: distributed denial of service (DDoS) and man-in-the-middle [7]. DDoS is a malicious attack by flooding the bandwidth and/or CPU utilization of a target system. Since the attack can occupy the majority of communication and/or computation resources, the reliability and responsiveness of Fog manufacturing can be significantly affected. Without loss generality, we focus on computation utilization, and will apply similar strategies to monitor the communication utilization. In order to detect the DDoS attack, we consider computation utilization and the corresponding computation covariate in Fog manufacturing, since high-intensity computation tasks can also result in high utilization. For example, if the computation intensity of a task is indeed very low but a high computation utilization is observed at the same time, it has a higher probability to be considered as an abnormal scenario.

There are also other anomalies shown in Table 1 including Man-in-the-middle type of cyber-attacks [12] which can replace the raw data/intermediate results with fake data, and the Fog node failure. For the Man-in-the-middle, the model prediction accuracy is considered as the monitoring statistics since the prediction accuracy for a fake dataset, which usually is significantly different with the historical data, can be relatively low. The Fog node failure is a straightforward anomaly category that indicates the hardware/software failure for one/multiple Fog node(s) in a Fog manufacturing system. Therefore, the mean of CPU or bandwidth utilization is employed as monitor statistics since they will suddenly decrease to zero once the anomalies happened. Specifically, the abnormal scenarios including the extreme system utilization, imbalanced workload, and DDoS cyber-attack are mainly focused on this study since these scenarios are more commonly observed compared with other scenarios. Besides, scenarios such as node failures can be easily observed based on the real-time computation performance variables without a SPC method. Moreover, due to the limited budget and the implementation complexity, the man-in-the-middle will be studied in future work.

B. SPC Methods for the Fog Manufacturing Monitoring System

To accurately detect the abnormal scenarios based on defined monitoring statistics in a Fog manufacturing system, appropriate SPC methods are necessary. In this study, the EWMA chart [10] is adopted for 1) extreme system utilization, and 2) imbalanced workload. The EWMA chart gives weights to historical observations in geometrically decreasing order, thereby increases the influence of recent samples and decreases the influence of distant samples to improve the robustness to the long-term noise [10]. Instead of the original monitoring statistics, the EWMA control chart computes new statistics as monitoring statistics z_i for i-th observation:

$$z_i = \lambda \bar{x}_i + (1-\lambda) z_{i-1}, \tag{1}$$

where $\bar{x}_i = \frac{\sum_{j=1}^{n_i} x_{ij}}{n_i}$ is the average for i-th subgroup of size n_i; λ is a pre-defined weight for $\bar{x}_i$ which is determined by MCMC to control the Type-I error; In the simulation, the Type-I is tuned to be the same by adjusting λ [9]; and z_{i-1} is the most recent proposed statistic. Moreover, the control limits for the control chart are calculated as:

$$\bar{\bar{x}} \pm \left(\frac{LS}{\sqrt{n}}\right) \times \left(\sqrt{\frac{\lambda}{2-\lambda}} \times \sqrt{1-(1-2\lambda)^{2i}}\right), \tag{2}$$

where $\bar{\bar{x}} = \frac{\sum_{i=1}^{k} \sum_{j=1}^{n_i} x_{ij}}{\sum_{i=1}^{k} n_i}$ is the grand mean; k is the number of subgroups; $L = 3$ is the multiplier for the standard deviation; S is the standard deviation of the monitoring statistics.

Besides, the RA chart is adopted to monitor DDoS type of cyber-attacks because the RA chart can incorporate the corresponding covariates which relate to the monitoring statistics to improve the accuracy and efficiency of the monitoring system [11]. Specifically, in this study, the RA chart adjusts the potential risk factor (i.e., the corresponding computation covariate) via a linear regression model between the monitoring statistics y_i (i.e., log of the CPU utilization) and the potential risk factor $\boldsymbol{x}_i$ for i-th observation as :

$$y_i = \beta_0 + \boldsymbol{\beta}_1^{\mathrm{T}} \boldsymbol{x}_i + \epsilon_i, \tag{3}$$

where β_0 is the intercept; $\boldsymbol{\beta}_1$ is the coefficients for the risk factor $\boldsymbol{x}_i = [x_{i1}, x_{i2}, x_{i3}]^{\mathrm{T}}$; x_{i1} is the sample size for i-th computation task; x_{i2} is the complexity of i-th computation task; x_{i3} is the mean value of the temperature for CPU when executing i-th computation task; and ϵ_i is the residual term follows a normal distribution $N(0, \sigma^2)$ with a constant variance σ^2. The residual is calculated as $\epsilon_i = \hat{y}_i - y_i$, where $\hat{y}_i$ is the predicted monitoring statistics based on the linear regression model for i-th observation. ϵ_i is adopted as the new monitoring statistics in the RA chart because the residual can properly reflect the difference between the expected and the real computation utilization. If there is a large differences between these two values, it indicates that the system is under attack by DDoS and results in additional computation workloads. Moreover, the control limit for the RA chart can be calculated as:

$$\bar{\epsilon} \pm 3\overline{MR}/d \qquad (4)$$

where $\bar{\epsilon} = \frac{\sum_{i=1}^{n} \epsilon_i}{n}$ is the mean of the residual; n is the number of observations; $\overline{MR} = \frac{\sum_{i=1}^{k} MR_i}{k-1}$; $MR_i = |\epsilon_{i+1} - \epsilon_i|$; $1/d$ is the multiplier which is determined by MCMC to control the Type-I error [9].

III. SIMULATION STUDY

A simulation study is implemented to evaluate the ARL [11] of the proposed monitoring system. In total, six scenarios are simulated as stated in Table II. The computation utilization and communication utilization are simulated based on data analytical models in Fog manufacturing [2]. To simulate abnormal scenarios 1-4, the residual of corresponding monitoring statistics in the models is fluctuated up and down for 50% of mean magnitude compared with normal observations. For abnormal scenario 5 (i.e., imbalanced workload), the monitoring statistics for abnormal Fog node is fluctuated up to 50% of mean magnitude compared with other nodes. For the DDoS cyber-attack, the residual of the monitoring statistics fluctuated 200% of mean residual compared with normal observations. For each scenario, 5000 replications have been conducted in the simulation. In each replication, 20 abnormal observations followed with 30 normal observations are simulated. To compare the performance of two control charts, the expectations of ARL_0 (i.e., the average number of observations until the first false alarm) for both charts are all adjusted to 75 [9] . Recall the monitoring statistics for different abnormally scenarios as described in Section II, EWMA charts were used for scenarios 1-5 because the monitoring statistics are mean and standard deviations of directly measurable variables; RA charts were not appropriate in these scenarios. In scenario 6, RA charts were used because the monitoring statistics are the modeling residual for computation utilization; EWMA charts were not appropriate in this scenario.

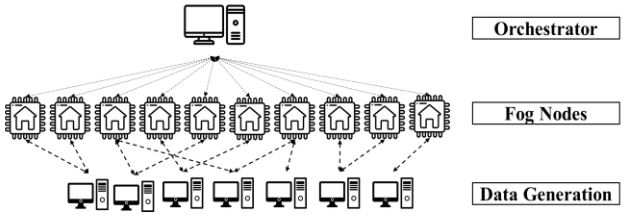

Fig. 1. The architecture design of the testbed (redrawn from [1] with authors' permission).

TABLE II. AVERAGE RUN LENGTH OF THE MONITORING SYSTEM

	Scenarios	ARL_1	***Control Chart Types***
1	High computation loads	2.009	EWMA
2	Inefficient computation utilization	4.362	EWMA
3	High communication loads	1.000	EWMA
4	Inefficient communication utilization	1.000	EWMA
5	Imbalanced computation utilization	4.467	EWMA
6	DDoS cyber-attack	1.011	RA

The simulation results are shown in Table II. It can be observed that the ARL_1 (i.e., the average number of observations between the anomaly signaled and the anomaly detected) for all scenarios is smaller than 5. Especially for high communication loads, inefficient communication utilization, and DDoS cyber-attack, the monitoring system can successfully detect the anomaly within 2 observations on average. The ARL_1 for scenarios 1 and 2 are larger than those for scenarios 3 and 4, because the variation of computation utilization is much larger than that of the communication

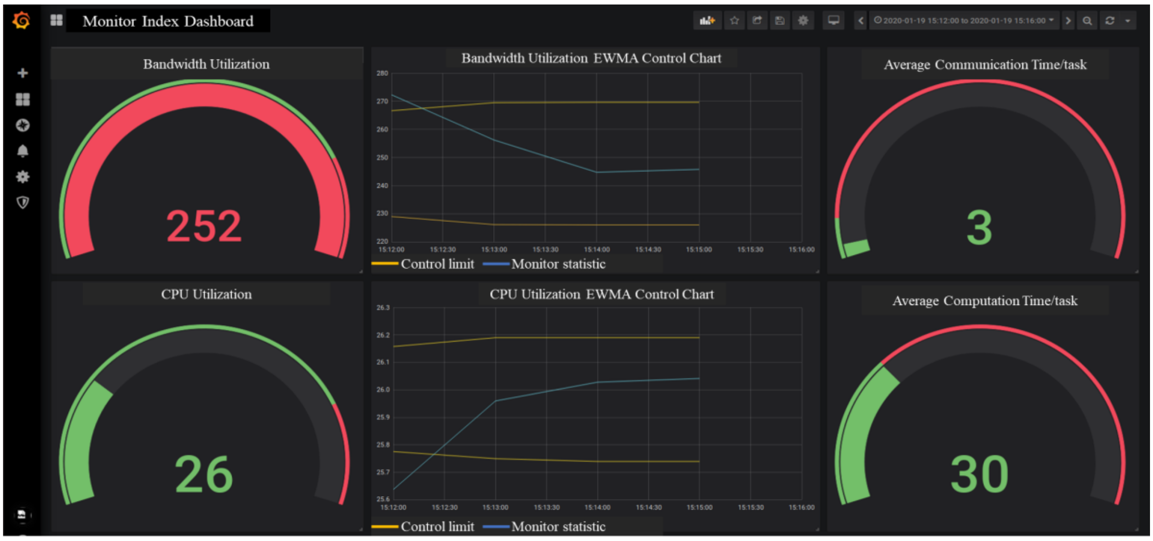

Fig. 2. A visualization dashboard for the monitoring system of Fog manufacturing.

utilization, which makes it more difficult to detect the changes in scenarios 1 and 2.

IV. A Real Case Study

A. *Fog Manufacturing Testbed*

To validate the proposed monitoring system in a real case study, a Fog manufacturing testbed is adopted as shown in Fig. 1. This testbed contains three layers. From the top to the bottom, the first layer is the orchestrator layer that controls data flow, assignment for computation tasks, data processing for the SPC control charts, and the visualization dashboard. The second layer is the Fog nodes layer which contains 10 Raspberry Pi that can implement the pre-defined computation tasks for the Fog manufacturing system. The third layer is the data generation layer which contains 7 databases to simulate real plasma chemical vapor deposition manufacturing processes based on the historical data. This layer can transfer raw data to Fog nodes simultaneously as the input of pre-defined computation tasks. In order to better demonstrate the result of the proposed monitoring system, an open-source visualization dashboard is created by utilizing GRAFANA as shown in Fig. 2 [13].

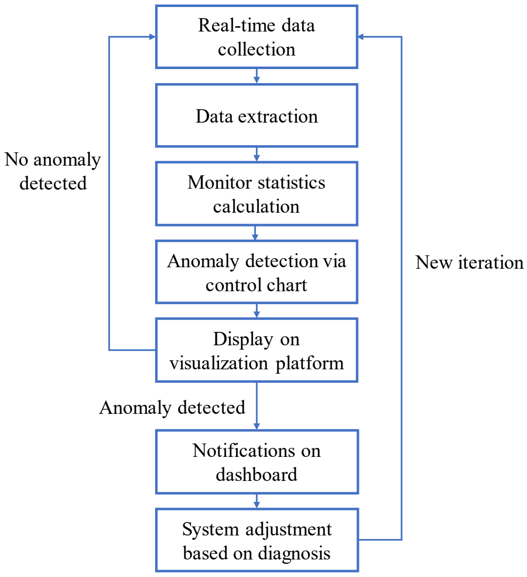
Real-time data collection
Data extraction
Monitor statistics calculation
Anomaly detection via control chart
Display on visualization platform
Notifications on dashboard
System adjustment based on diagnosis
No anomaly detected
Anomaly detected
New iteration

Fig. 3. The workflow of the monitoring system.

A monitoring workflow can be summarized as in Fig. 3. During the operation of the Fog manufacturing system, *in situ* process variables (e.g., CPU utilization, bandwidth consumption, etc.) on Fog nodes will be collected and stored in a local database to reduce the influence for bandwidth utilization. After finishing a computation task on each Fog node, the monitoring system will remotely extract the collected data and calculate the corresponding monitoring statistics defined in Table 1. These monitoring statistics will be further substituted into the pre-defined SPC control charts to judge the current status of the Fog manufacturing system. The control charts will also be visualized on the GRAFANA dashboard to provide a straightforward understanding of the system status for operators. If the anomaly is detected, the Fog manufacturing system will send a notification to the operator through a visualization dashboard system [13].

B. *Experiment Plan*

TABLE III. DATA SIZE AND COMPLEXITY OF COMPUTATION TASKS FOR EXPERIMENTS

	Scenarios	***Sample Size***	***Computation Task Complexity***
1	High computation loads	Normal (400 samples)	High (Gaussian Regression)
2	Inefficient computation utilization	Normal (400 samples)	Low (Linear Regression)
3	High communication loads	Large (600 samples)	Normal (Lasso Regression)
4	Inefficient communication utilization	Small (200 samples)	Normal (Lasso Regression)
5	Imbalanced computation utilization	Normal (400 samples)	Normal (Lasso Regression)
6	DDoS cyber-attack	Normal (400 samples)	Normal (Lasso Regression)

To further validate the ARL of the proposed system, experiments are implemented on the testbed to generate normal and abnormal scenarios. As shown in Table III, the data size and the complexity of computation tasks (i.e., Gaussian regression [14], Lasso regression [15] and ordinary linear regression [9]) are varied to generate abnormal communication and computation utilizations for the extreme system utilization. Moreover, the imbalanced workload scenario is generated by following an improper offloading strategy: one node is assigned 90% of computation tasks. The DDoS cyber-attack is generated by conducting multiple simultaneous computation tasks at the same time on the testbed. At the beginning of each experiment, the Fog manufacturing system will execute 30 computation tasks under normal conditions (e.g., normal computation complexity tasks computed on normal size samples for extreme system utilization). Then, the abnormal conditions will be introduced (e.g., extremely high computation intensity task with large data transformation requests). Each abnormal condition will be repeated five times to comprehensively quantify the performance of the proposed monitoring system.

C. *Results and Discussion*

In summary, the mean of ARL for all six scenarios are smaller than 4. Figs. 4-5 show two examples of EWMA charts for inefficient computation utilization and imbalanced workload scenarios in respectively. Fig. 6 shows the RA chart for DDoS cyber-attack in the adopted testbed. Other figures are omitted due to the limited space and are available upon requests. It can be observed that the proposed monitoring system can quickly and efficiently detect anomalies after the anomalies are signaled at time 30. It indicates that in practice, the proposed monitoring system is effective to detect anomalies in Fog manufacturing.

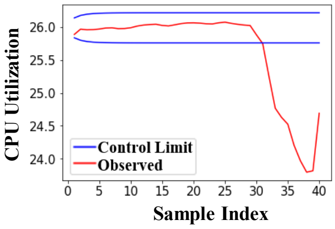

Fig. 4. EWMA charts for inefficient computation utilization.

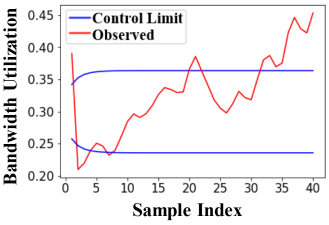

Fig. 5. EWMA chart for imbalanced workloads.

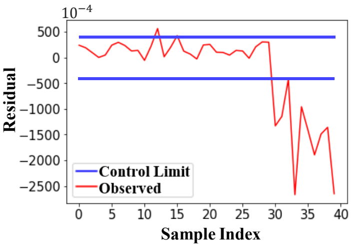

Fig. 6. RA chart for DDoS cyber-attack.

In the meantime, according to the monitoring statistics and system is overloaded or deficient from computation and communication aspects. Moreover, we can also detect whether the workload is evenly offloaded to each Fog nodes. Based on these messages, further adjustments can be made to the architecture design and offloading strategies to improve the performance of a Fog manufacturing system.

V. Conclusions

In the industrial cyber-physical system, Fog manufacturing can provide responsive and robust computation services compared with the Cloud computing system. However, due to anomaly issues, Fog manufacturing is still not widely adopted in practice. In this study, we proposed a monitoring system to detect anomalies in Fog manufacturing. To start with, anomalies are defined in four categories: extreme system utilization, imbalanced workload, cyber-attack, and Fog node failure. Moreover, the corresponding monitoring statistics and SPC methods are adopted based on the properties of anomalies. The system is validated via both simulation study and a real case study. The results show the proposed monitoring system can quickly and accurately identify the anomalies in Fog manufacturing.

This paper leads to a few future research topics. First, since there are many text logs generated in a Fog manufacturing system, a data fusion method for texts and numerical data to jointly detect the anomalies will be studied. Next, a robust monitoring system will be studied to reduce the influence of outliers. Finally, other anomalies such as man-in-the-middle types cyber-attacks will be investigated.

References

[1] Y. Zhang, X. Chen, L. Wang, and R. Jin, "System Informatics and Hypothesis Tests of Significant Factors to Performance in a Fog Manufacturing System," in *Proceedings of IISE Annual*, 2020, p. Just Accepted.

[2] Y. Zhang, L. Wang, X. Chen, and R. Jin, "Fog Computing for Distributed Family Learning in Cyber-Manufacturing Modeling," in *Proceedings of 2019 IEEE International Conference on Industrial Cyber Physical Systems (ICPS)*, 2019: IEEE, pp. 88-93.

[3] S. Yi, C. Li, and Q. Li, "A Survey of Fog Computing: Concepts, Applications and Issues," in *Proceedings of the workshop on mobile big data*, 2015: ACM, pp. 37-42.

[4] M. S. De Brito, S. Hoque, R. Steinke, and A. Willner, "Towards Programmable Fog Nodes in Smart Factories," in *Proceedings of IEEE International Workshops on Foundations and Applications of Self* Systems (FAS* W)*, 2016: IEEE, pp. 236-241.

[5] S. Khan, S. Parkinson, and Y. Qin, "Fog Computing Security: A Review of Current Applications and Security Solutions," *Journal of Cloud Computing,* vol. 6, no. 1, p. 19, 2017.

[6] Y. Tan, H. Nguyen, Z. Shen, X. Gu, C. Venkatramani, and D. Rajan, "Prepare: Predictive Performance Anomaly Prevention for Virtualized Cloud Systems," in *Proceedings of IEEE International Conference on Distributed Computing Systems*, 2012: IEEE, pp. 285-294.

[7] C. Lo, C. Huang, and J. Ku, "A Cooperative Intrusion Detection System Framework for Cloud Computing Networks," in *Proceedings of International Conference on Parallel Processing Workshops*, 2010: IEEE, pp. 280-284.

[8] Q. Guan and S. Fu, "Adaptive Anomaly Identification by Exploring Metric Subspace in Cloud Computing Infrastructures," in *Proceedings of IEEE International Symposium on Reliable Distributed Systems*, 2013: IEEE, pp. 205-214.

[9] D. C. Montgomery, *Introduction to statistical quality control*. John Wiley & Sons, NJ, 2007.

[10] J. S. Hunter, "The Exponentially Weighted Moving Average," *Journal of quality technology,* vol. 18, no. 4, pp. 203-210, 1986.

[11] A. Sachlas, S. Bersimis, and S. Psarakis, "Risk-Adjusted Control Charts: Theory, Methods, and Applications in Health," *Statistics in Biosciences,* vol. 11, no. 3, pp. 630-658, 2019.

[12] M. Wu, Z. Song, and Y. B. Moon, "Detecting Cyber-Physical Attacks in Cyber-Manufacturing Systems with Machine Learning Methods," *Journal of intelligent manufacturing,* vol. 30, no. 3, pp. 1111-1123, 2019.

[13] Grafana. "The Open Observability Platform." https://grafana.com/ (accessed Jan. 19, 2020).

[14] J. Quiñonero-Candela and C. E. Rasmussen, "A unifying view of sparse approximate Gaussian process regression," *Journal of Machine Learning Research,* vol. 6, no. Dec, pp. 1939-1959, 2005.

[15] R. Tibshirani, "Regression shrinkage and selection via the lasso," *Journal of the Royal Statistical Society: Series B (Methodological),* vol. 58, no. 1, pp. 267-288, 1996.