Towards False Alarm Reduction using Fuzzy If-Then Rules for Medical Cyber Physical Systems

Li, Wenjuan; Meng, Weizhi; Su, Chunhua; Kwok, Lam For

Published in:
IEEE Access

Link to article, DOI:
10.1109/ACCESS.2018.2794685

Publication date:
2018

Document Version
Publisher's PDF, also known as Version of record

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON CYBER-PHYSICAL-SOCIAL COMPUTING AND NETWORKING

Received December 16, 2017, accepted January 12, 2018, date of publication January 17, 2018, date of current version March 9, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2794685

Towards False Alarm Reduction Using Fuzzy If-Then Rules for Medical Cyber Physical Systems

WENJUAN LI[1,2], (Student Member, IEEE), WEIZHI MENG[2], (Member, IEEE), CHUNHUA SU[3], AND LAM FOR KWOK[1]

[1]Department of Computer Science, City University of Hong Kong, Hong Kong
[2]Department of Applied Mathematics and Computer Science, DTU Compute, Technical University of Denmark, 2800 Kongens Lyngby, Denmark
[3]Division of Computer Science, University of Aizu, Aizuwakamatsu 965-8580, Japan

Corresponding author: Weizhi Meng (weme@dtu.dk)

This work was supported in part by JSPS Grants-in-Aid for Scientific Research under Grant KAKENHI WAKATE B-15K16005 and in part by the Competitive Research Funding from the University of Aizu under Grant P-21.

ABSTRACT Cyber-Physical Systems (CPS) are integrations of computation, networking, and physical processes. Its process control is often referred to as embedded systems. Generally, CPS and Internet of Things have the same basic architecture, whereas the former shows a higher combination and coordination between physical and computational elements, i.e., wireless sensor networks can be a vital part of CPS applications. With the rapid development, CPS has been applied to healthcare industry, where a wide range of medical sensors are used within a healthcare organization. However, these sensors may generate a large number of false alarms in practice, which could significantly reduce the system effectiveness. Targeting on this issue, in this work, we attempt to design a Medical Fuzzy Alarm Filter (named MFAFilter) for healthcare environments by means of fuzzy logic, especially fuzzy if-then rules, which could handle the vague and imprecise among data. In the evaluation, we conducted two major experiments to explore the performance of our approach in a simulated and a real network environment, respectively. Experimental results demonstrate that the use of fuzzy if-then rules could achieve a better accuracy as compared to the traditional supervised algorithms, and that our designed filter is effective in the practical environment.

INDEX TERMS False alarm reduction, fuzzy if-then rules, alarm filter, medical cyber-physical systems, wireless sensor networks, machine learning technique.

I. INTRODUCTION

Cyber-physical systems (CPS) connect cyberspace with the physical world through a set of large-scale, interconnected physical and engineered systems such as sensors, actuators and computational engines [35]. In other words, these systems integrate computation and communication with physical processes, in which physical and software components are deeply intertwined. Due to the economic and societal potential of such systems, CPS builds on the discipline of embedded systems and computer software, resulting in a wide application from embedded systems used in smart vehicles, to Supervisory Control And Data Acquisition (SCADA) systems in smart grids to control systems in water distribution systems, and so on.

With the rapid development, CPS technology has been applied to healthcare domain as well, including some applications like CPeSC3 [38] and eHealth [22]. It is worth emphasizing that medical industry is undergoing a significant and important transformation, embracing much more integration of embedded software and network connectivity. Instead of designing and implementing stand-alone medical devices to serve patients independently, current medical devices can work collaboratively under a distributed framework, enabling simultaneously to control multiple aspects of the patient's physiology [20]. These modern medical device systems, shortly *medical CPS*, present a distinct type of cyber-physical systems, which combines the embedded software controlling the devices, the networking capabilities, and the complicated physical dynamics that patient bodies may exhibit [11].

Wireless medical sensors (WMSs) are widely adopted for medical CPS, which are a kind of wireless sensor networks (WSNs) with energy and processing constraints. These medical sensors are small, resource constrained and capable of collecting different types of physiological parameters, such as Heart Rate (HR), Pulse, Oxygen Saturation (SpO2), Respiration and Blood Pressure (BP). These sensed data provide

valuable information for healthcare organizations to monitor and decide the medical condition of a patient. Because of the importance, it is critical to ensure the accuracy and reliability of the data to raise an alarm in case of emergency [12].

However, medical sensors may generate a large number of false alarms in practice, which have a negative impact on healthcare operations, degrading the quality of service and waste of valuable time and money. For example, the collected sensor data may be inaccurate due to sensor fault and resource constraint of the sensor node such as limitation of power and transmission capability. Moreover, as healthcare organizations are usually short of technical experts in IT, common personnel are hard to handle large false alarms in a quick manner [33]. As a result, it is very important to identify data inaccuracies and reduce false alarms.

CONTRIBUTIONS: Designing an appropriate alarm filter is promising to reduce false alarms. Similarly, in the domain of intrusion detection, a line of research studies (e.g., [28], [30], [31], [34]) have proven that alarm filters are easy for use and effective for alarm reduction in practical environments. In healthcare industry, an alarm filter is more easy to manage than some complicated security mechanisms [33]. In literature, there has been little work investigating false alarm reduction in medical industry. Motivated by these facts, in this work, we aim to develop an alarm filter for medical CPS and employ a fuzzing logic approach for alarm reduction. The contributions of our work can be summarized as below.

- Medical sensor networks are a special application of medical CPS, in which interconnected medical devices form a distributed medical device system in order to ensure effectiveness and patient safety. False alarms are one of the major challenges in medical CPS. In this work, we design an alarm filter using machine learning techniques to reduce false alarms in a healthcare environment.
- To handle data fusion, fuzzy classifiers are believed to be good at detecting anomalies. In this work, we employ fuzzy if-then rules, which can be easily understood by human users. As a comparison, we consider several traditional supervised classifiers including k-nearest neighbor (KNN), neural network (NN), support vector machine (SVM), decision tree (DT), Naive Bayes (NB) and a baseline classification algorithm: ZeroR.
- In the evaluation, we investigate the filter performance in both a simulated and a real medical network. Experimental results demonstrate that fuzzy if-then rules can outperform other classifiers in the aspect of filtration accuracy with reasonable workload, and that the designed filter is effective for alarm reduction.

The remaining parts of this paper are organized as follows. In Section II, we review relevant research studies regarding false alarm filtration in medical CPS and in intrusion detection area. Section III presents the architecture of our designed alarm filter and introduces fuzzy if-then rules in detail. Section IV describes an evaluation and comparison with a set of traditional supervised classifiers, and Section V provides a discussion regarding time consumption of training and the increased workload. We conclude our work in Section VI.

II. RELATED WORK

A. ALARM REDUCTION IN MEDICAL CPS

In the past decades, there is a technological revolution in healthcare domain, where new materials replace metals and devices based on information technology. Jiang *et al.* [18] introduced a closed-loop testing environment for medical CPS, allowing for interactive and physiologically relevant model-based test generation for basic pacemaker device operations such as maintaining the heart rate, atrial-ventricle synchrony, and complex conditions.

As medical devices become more complex and more interconnected, there are many challenges remain. False alarms are one of these challenges, which can greatly degrade the system performance and effectiveness [11]. In the field of medical CPS, this issue should be given more attention. Haque and Aziz [10] proposed an architecture for false alarm detection. In the proposed system, the status of a patient is classified as Normal, Intensive, Critical or Highly Critical, where all vital signs or a predetermined number of vital signs must cross the threshold in order to activate the alarm. They further developed an approach based on a prediction model, which used the spatio-temporal correlation that exists among physiological parameters.

Naive Bayes, Bayesian network and decision tree are common methods used in medical CPS; however, due to the confusion among medical data, the motivation of this work is to investigate the use of fuzzy logic to reducing false alarms for medical systems.

B. ALARM REDUCTION IN INTRUSION DETECTION

Alarm reduction is also a challenge in the field of intrusion detection. To mitigate this issue, a direct approach is to improve the detection algorithms like data summarization and alarm correlation (e.g., [8], [9], [13], [17], [37]). Another approach is to construct an alarm filter to decrease unwanted alarms in a post-preprocessing manner.

Machine learning classifiers are the most commonly used tools for constructing an alarm filter. Pietraszek [34] proposed an early adaptive alarm reduction system, which could utilize the feedback from analysts and intelligent classifiers to reduce false positives. Their method could drop alerts based on their classification confidence. Law and Kwok [19] then designed a false alarm filter by using KNN (k-nearest-neighbor) classifier and achieved good filtration performance. Alharbt and Imai [1] designed an alarm filter via continuous and discontinuous sequential patterns to detect unusual alarms. Chiu *et al.* [4] presented an alarm filter by means of semi-supervised learning classifier, which could reduce 85% false alarms while keeping a high detection rate. Bolzoni *et al.* [2] presented *ATLANTIDES*, an architecture for automatic alert verification, which detected anomalies based on output system traffic in a structural way. This architecture

could be used for reducing false positives in both signature-based and anomaly-based NIDSs.

For adaptive alarm reduction, Meng and Kwok [25] proposed an adaptive false alarm filter to reduce a large number of false alarms, by adaptively selecting the most appropriate classifiers, i.e., achieving and keeping a good filtration rate. Meng and Li [28] designed a non-critical alarm filter to improve the quality of output alarms by integrating contextual information like application and OS information. Meng *et al*. [32] developed a method of knowledge-based alert verification and design an intelligent alarm filter based on a multi-class k-nearest-neighbor classifier to filter out unwanted alarms. In particular, the alarm filter employs a rating mechanism by means of expert knowledge to classify incoming alarms to proper clusters for labeling. Several other related studies about the reduction of false alarms by constructing alarm filters can be referred to [24], [26], and [29]–[31].

C. FUZZY ALGORITHMS

Fuzzy algorithms have been studied in improving the performance of NIDSs, especially the anomaly-based NIDS. For example, Dickerson and Dickerson [5] developed a fuzzy intrusion recognition engine (FIRE) that used fuzzy logic to decide whether a malicious activity was happened. Their tests showed that the FIRE could detect a wide range of common attacks. Dickerson *et al*. [6] then explored the FIRE's performance of detecting other attacks and pointed out that this system could easily identify port scanning and denial-of-service (DoS) attacks.

Then, Bridges and Vaughn [3] developed a prototype of intelligent intrusion detection system (IIDS) to demonstrate the effectiveness of data mining techniques by using fuzzy logic and genetic algorithms. In particular, their system combined both anomaly-based intrusion detection and misuse-based detection. The former used fuzzy data mining techniques while the latter used traditional rule-based expert system techniques. The genetic algorithms are used to tune the fuzzy membership functions and to select an appropriate set of features. Luo *et al*. [23] defined and applied fuzzy frequent episodes in real-time intrusion detection. Their experiments showed their proposed technique could provide effective anomaly detection.

Later, Tian *et al*. [36] presented a method of combining multiple decision trees based on fuzzy logic. The idea was to divide a great large dataset into several sub-datasets, mine on sub-datasets separately to construct different sub-decision trees, detect TCP data by using different sub-decision trees, and then nonlinearly combine the results from multiple sub-decision trees by fuzzy integral. The experiment results showed that this technique outperformed individual decision trees. Several other relevant studies can be referred to [7], [8], and [27]. It is worth noting that although fuzzy classifiers were used in intrusion detection, its performance has not been researched in medical industry for false alarm reduction, which motivates this work.

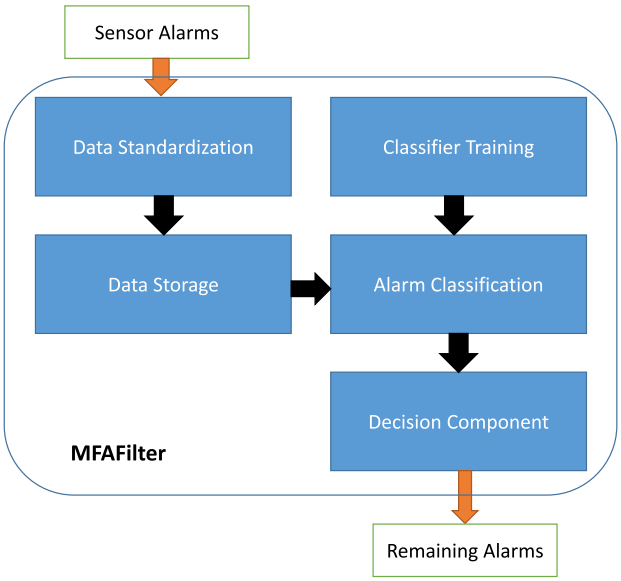


FIGURE 1. The high-level architecture of our designed medical fuzzy alarm filter, MFAFilter.

III. MEDICAL FUZZY ALARM FILTER

This section introduces the architecture of our designed MFAFilter (Medical Fuzzy Alarm Filter) for reducing sensor false alarms, and describes fuzzy if-then rules for alarm classification.

A. FILTER ARCHITECTURE

Figure 1 depicts the high-level architecture of MFAFilter, which consists of five main components: *data standardization*, *data storage*, *classifier training*, *alarm classification*, *decision component*.

- The component of data standardization is responsible for extracting alarm features and converting alarm formats, if required. This is because different medical sensors may generate alarms with distinct formats.
- The component of data storage provides a passive database to store all standardized alarms and make preparation for alarm filtration.
- The component of classifier training aims to train a classifier with labeled items. In real-world applications, IT administrators can decide when to update the training process by adding new labeled alarms.
- The component of alarm classification is responsible for refining false alarms by means of a fuzzy logic classifier, namely fuzzy if-then rules.
- The decision component can output alarms after filtration, by considering the outputs from the component of alarm classification and some pre-defined conditions (i.e., IT administrators can provide a list of whitelisted or blacklisted alarms).

In real-world applications, an IT expert or administrator in healthcare organizations can label a limited number of medical sensor alarms, and store them into the component of

alarm storage. Based on the training rules, the alarm filter can train the fuzzy classifier to establish a model, which can be used to identify unwanted alarms in the component of alarm classification. Afterwards, the classification results would be forwarded to decision component for alarm reduction and only ''true'' alarms can be output.

B. FUZZY IF-THEN RULES

Fuzzy logic is a form of many-valued logic which can be used to deal with the vague and imprecise. It has two major advantages when being applied to solving the problems in intrusion detection (e.g., anomaly detection).

- The process of intrusion detection involves many numeric attributes and various derived statistical measures. By directly building models on the numeric data may cause many detection errors (i.e., resulting in the generation of false alarms) whereas fuzzy logic is a good alternative.
- The intrusion detection process is also a fuzziness problem between the normal and the abnormal events (i.e., according to a threshold). In this case, it is appropriate to model anomalies by means of fuzzy logic.

Fuzzy logic is widely used in the field of machine control. Although genetic algorithms and neural networks can perform just as well as fuzzy logic in many cases, fuzzy logic has its own advantage; that is, its operators can be easily understood by human users; thus, their experience can be used in the controller design. In other words, it is easy for human users to understand each selected rule from fuzzy if-then rules.

Fuzzy logic requires defining fuzzy operations whereas these operations may not be known in some cases. To solve this problem, fuzzy if-then rules can be used to define fuzzy operations on fuzzy sets. In this work, we adopt the fuzzy classification based on [14] and [16] and follow our previous work [27]. The if-then rules are usually expressed in the form as described below:

$$IF\ variable\ IS\ property\ THEN\ action \tag{1}$$

Suppose there are two fuzzy variables x and y, fuzzy operators of Boolean logic like NOT, AND and OR can be defined as follows:

$$NOT\ x = (1 - truth(x)); \tag{2}$$

$$x\ AND\ y = minimum(truth(x),\ truth(y)); \tag{3}$$

$$x\ OR\ y = maximum(truth(x),\ truth(y)). \tag{4}$$

where $truth(x)$ means the truth value of x. A truth value (also called logical value) is a value indicating the relation of a proposition to truth.

In particular, we assume that a pattern space is the unit square $[0, 1] * [0, 1]$, and suppose there are m patterns $X_p = (X_{p1}, X_{p2})$, $p = 1, 2, \ldots, m$, which are given from M ($M << m$) classes (e.g., Class1 (C1), Class2 (C2)). The classification of each X_p is known as one of the above M classes. Therefore, the problem in generating fuzzy if-then rules is how to divide the pattern space into M disjoint decision areas.

Then, we assume that each axis of the pattern space can be partitioned into K fuzzy subsets as shown below:

$$K - fuzzy - subsets : K_1^K, K_2^K, K_3^K, \ldots, K_K^K \tag{5}$$

where K_i^K $(i = 1, 2, \ldots, K)$ means the *ith* fuzzy subsets and K means the number of fuzzy subsets on each axis. Therefore, for the two axes of the pattern space, we have K^2 fuzzy subspaces $A_i^k \times A_j^K$ $(i = 1, 2, \ldots, K; j = 1, 2, \ldots, K)$.

Since each fuzzy subspace has one fuzzy if-then rule, the number of fuzzy if-then rules in a single fuzzy rule table is also K^2. Regarding the M-class classification problems in the pattern space $[0, 1] * [0, 1]$, the corresponding fuzzy if-then rules can be represented as follows:

$$\begin{aligned} Rule\ R_{ij}^K :\ & IF\ X_{p1}\ is\ A_i^k\ AND\ X_{P2}\ is\ A_j^K \\ & THEN\ X_p\ belongs\ to\ Class C_{ij}^K\ with\ CF = CF_{ij}^K \end{aligned} \tag{6}$$

where $i = 1, 2, \ldots, K, j = 1, 2, \ldots, K$. R_{ij}^K means the fuzzy if-then rules, A_i^k and A_j^K means fuzzy subsets, $Class C_{ij}^K$ represents the classification results and CF_{ij}^K is the grade of certainty for this if-then rule. More specific details about the fuzzy if-then rule and its theory background can be referred to [14]–[16].

1) EXAMPLES

In order to implement the fuzzy classifier, there are two major phases for generating fuzzy if-then rules from numerical data:

- To partition a pattern space into fuzzy subspaces;
- To determine a fuzzy if-then rule for each fuzzy subspace.

To better explain the application of fuzzy if-then rules, we present a simple example with the following four fuzzy if-then rules [15]:

- **IF** $x1$ is small **AND** $x2$ is small **THEN** Class 1 with $CF1$,
- **IF** $x1$ is small **AND** $x2$ is large **THEN** Class 2 with $CF2$,
- **IF** $x1$ is large **AND** $x2$ is small **THEN** Class 3 with $CF3$,
- **IF** $x1$ is large **AND** $x2$ is large **THEN** Class 4 with $CF4$.

Based on the above four if-then rules, the classification boundary can be generated according to the assigned value of each CFi $(i = 1, 2, 3, 4)$. We give three examples with different grades of certainty to each fuzzy if-then rule in Figure 2.

Figure 2 (a) shows the same grade of certainty to each fuzzy if-then rule with (1,1,1,1), Figure 2 (b) shows different grades of certainty with (0.6,0.1,0.1,0.6) and Figure 2 (c) shows the grades of certainty with (0,0.6,0.6,0.1). It is visible that with different grades of certainty, the boundaries of each class could vary accordingly. Generally, a higher grade means that a class can have a bigger boundary.

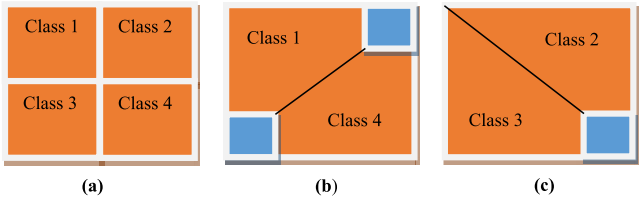


FIGURE 2. Three specific examples of classification boundaries generated by the mentioned four fuzzy if-then rules with different grades of certainty as follows: (a) (CF1,CF2,CF3,CF4) = (1,1,1,1); (b) (CF1,CF2,CF3,CF4) = (0.6,0.1,0.1,0.6); (c) (CF1,CF2,CF3,CF4) = (0,0.6,0.6,0.1).

2) IMPLEMENTATION

To realize the fuzzy if-then rules, we adopt and modify the fuzzy grid partition algorithm in fuzzy-weka project.[1] This project is written in Java and is an open-source project that can be implemented in WEKA [39]. WEKA is an open-source software that provides a set of machine learning algorithms. For the fuzzy-weka project, its class can be Binary class, Relational class, String class, Numeric class, Date class and Nominal class. Moreover, we can set the number of cross validation folds, adjust the number of fuzz subsets and choose the seed for randomizing the data during the implementation.

IV. EVALUATION

In this section, we conduct two major experiments to evaluate the performance of MFAFilter in a simulated and a real medical network environment, respectively. Several metrics are utilized to investigate the performance of a classifier. We denote true positive (TP) as the number of true positive instances predicted as positive, true negative (TN) as true negative instances predicted as negative, false positive (FP) as true negative instances predicted as positive and false negative (FN) as true positive instances predicted as negative. We specifically use four metrics to evaluate the performance: *classification accuracy (CA)*, *precision*, *recall* and *F-measure*, which can be computed as follows:

$$CA = \frac{TP + TN}{TP + TN + FN + FP} \tag{7}$$

$$Precision = \frac{TP}{TP + FP} \tag{8}$$

$$Recall = \frac{TP}{TP + FN} \tag{9}$$

$$F\text{-}measure = \frac{2Precision \times Recall}{Precision + Recall} \tag{10}$$

The metric of *classification accuracy* is used to measure the capability of classifying both positive instances and negative instances, the higher the better. The metric of *precision* is used to measure the proportion of predicted positive instances which are actually positive. A higher *precision* means lower false positive rate. The metric of *recall* is to measure the proportion of actual positive instances that are correctly identified. The metric of *F-measure* is a harmonic mean between precision and recall. In general, a higher value of *F-measure* means achieving better performance.

[1] http://fuzzyweka.sourceforge.net/.

FIGURE 3. The format of each item in the datasets.

TABLE 1. Three samples of medical CPS alarms.

Alarm ID	BP	HR	Pulse	ResR	SpO2
#42	122	82	87	27	101
#45	125	86	88	23	104
#67	165	43	78	26	102

A. EXPERIMENT IN A SIMULATED ENVIRONMENT

In this section, we use three datasets to investigate the settings of fuzzy if-then rules and the initial performance of MFAFilter. The datasets were collected by a simulated network in a practical healthcare center. The medical alarm format is depicted in Figure 3, which contains six major items: physiological parameters including Blood Pressure (BP), Heart Rate (HR), Pulse, Respiration Rate (ResR), and Oxygen Saturation (SpO2). All alarms were labeled by three healthcare experts and three samples are given in Table 1. By comparing these three alarms, it is not hard to find that the third alarm with #67 has two abnormal items: BP and HR, where BP is much higher but HR is much smaller than the other two alarms. Healthcare experts verified the deployed environment and labeled it as a false alarm. In the training phase, all features could be converted to [0, 1] using Min-Max scaling. The datasets are constructed as follows.

- DATASET1: This dataset contains 533 false alarms and 584 true alarms by random selection from the alarm pool. The occupancy ratio of false alarms and true alarms is nearly 1:1.
- DATASET2: This dataset consists of 683 false alarms and 1301 true alarms by random selection from the alarm pool. The occupancy ratio of false alarms and true alarms is nearly 1:2, which is not common in real scenarios.
- DATASET3: This dataset consists of 1179 false alarms and 523 true alarms by random selection from the alarm pool. The occupancy ratio of false alarms and true alarms is nearly 2:1 which is very common in real settings (i.e., in the field of intrusion detection [21]).

To compare the performance, we selected six traditional algorithms due to their wide adoption and popularity, as follows: k-nearest neighbor (KNN), neural network (NN), support vector machine (SVM), decision tree (DT), Naive Bayes (NB) and a simplest classification algorithm: ZeroR. The algorithm of ZeroR is used as a performance baseline in the comparison. We used the default WEKA settings for each algorithm and selected 10-fold cross validation. We evaluate the performance of fuzzy if-then rules by selecting different numbers of fuzzy subsets (i.e., starting the number of fuzzy

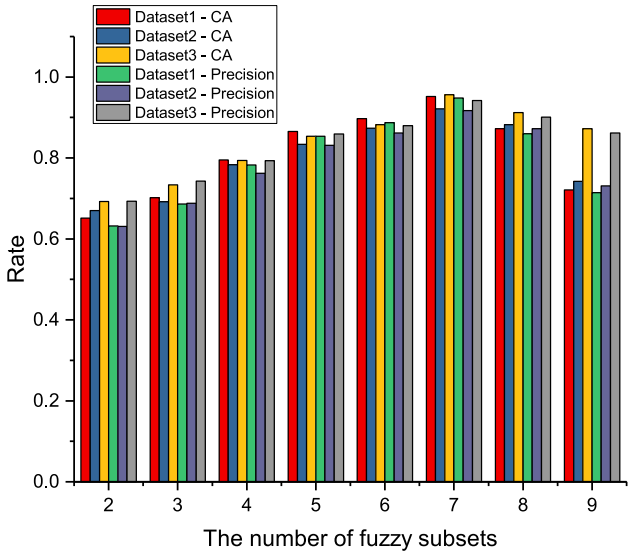


FIGURE 4. The performance of fuzzy if-then rules varied with different fuzzy subsets.

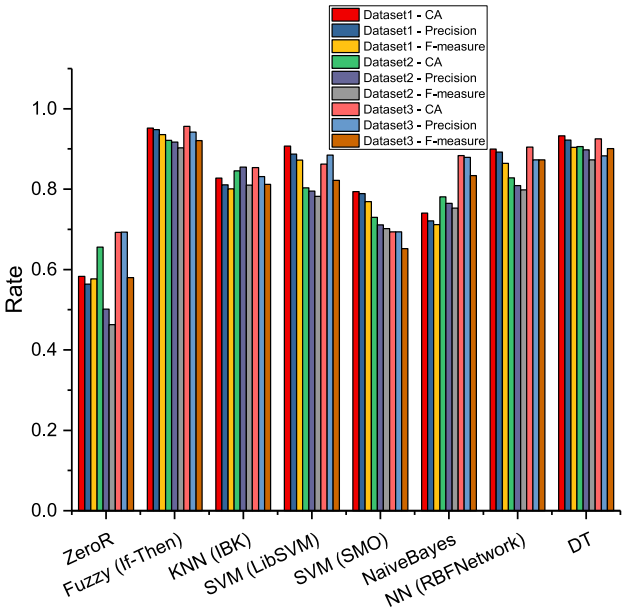


FIGURE 5. The performance comparison among different classifiers according to different datasets.

subsets from two). The performance of fuzzy if-then rules is shown in Figure 4.

It is found that the classification accuracy and precision would be varied according to the selected fuzzy subsets. In the beginning, both metrics can be gradually increased till the number of fuzzy subsets reach seven; afterwards, both metrics would be decreased. The number of fuzzy subsets decide how to draw a borderline and partition data items; thus, it is proven that the performance of classifier was better tuned when there were seven subsets. For fuzzy subsets with seven, the classifier could reach a classification accuracy of nearly 0.95, 0.92 and 0.96, and a precision of 0.95, 0.92 and 0.94 for Dataset1, Dataset2 and Dataset3, respectively. The peak is the same for *recall* and *F-measure*.

Then, we set fuzzy subsets to seven and compare the classification performance with other supervised learning algorithms. The results are shown in Figure 5. Based on the datasets, it is noticeable that fuzzy-if then rules could outperform other classifiers, such as k-nearest neighbor (KNN), neural network (NN), support vector machine (SVM), decision tree (DT), Naive Bayes (NB) and ZeroR. In addition to classification accuracy and precision, fuzzy-if then rules could reach a F-measure of 0.94, 0.9 and 0.92, respectively.

It is seen that SVM (LibSVM), KNN, NN (RBFNetwork) and DT could achieve a better accuracy than the remaining three algorithms, i.e., SVM (LibSVM), KNN, NN (RBFNetwork) and DT could achieve a classification accuracy in a range from 0.8 to 0.92, while accuracy of the remaining three classifiers is usually below 0.8. These results demonstrate that fuzzy-if then rules could be suitable for medical false alarm reduction.

B. EXPERIMENT IN A REAL NETWORK ENVIRONMENT

To investigate the practical performance of our designed filter, we further collaborated with a healthcare organization in China by implementing the filter in a real medical network environment. The network deployment is shown in Figure 6. The central server in the healthcare building is responsible for collecting the data from various sensors and producing alarms if detecting any anomalies. Our filter was deployed with the central server to help reduce false alarms.

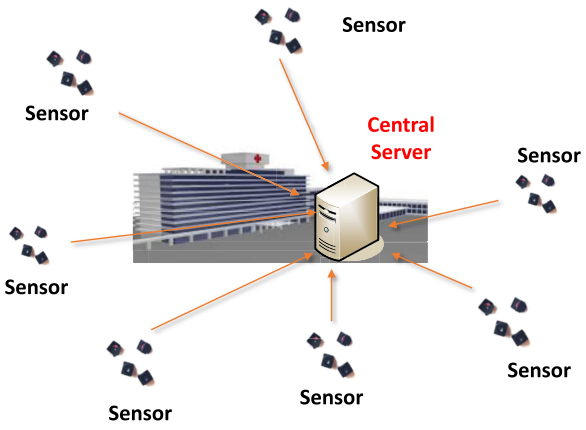


FIGURE 6. The high-level architecture of the real medical network environment through deploying our filter in the central server.

For privacy reason, the filtration process was handled by IT administrators from the healthcare organization. We focus on the same data format as shown in Figure 3, and required two IT experts in the same organization to help label the collected data items. These two experts have over five years' working experience and were familiar with the healthcare domain.

The experiment was conducted for 10 days and the number of alarms each day is depicted in Table 2. It shows that nearly a thousand of alarms could be generated each day. As there

TABLE 2. The number of produced alarms for each day in the deployed environment.

DAY	Day1	Day2	Day3	Day4	Day5
No.	872	763	799	1245	892
DAY	Day6	Day7	Day8	Day9	Day10
No.	1042	1224	973	863	1142

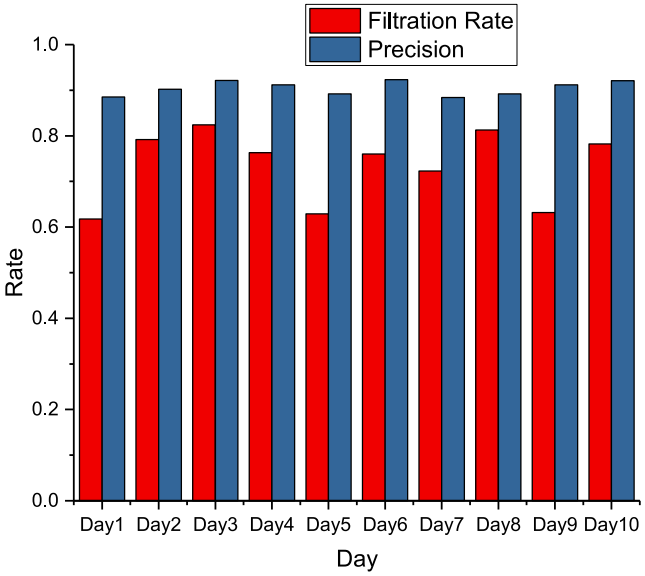


FIGURE 7. The results of alarm filtration and accuracy in the deployed environment.

is only limited IT experts in the healthcare organization, it is very hard for them to handle these alarms and give a response in a quick manner. Even worse, false alarms can consume many resources and make the whole medical systems ineffective. Thus, there is a great need to reduce false alarms and lighten the burden of analysts.

Figure 7 depicts the alarm filtration and accuracy in the deployed environment. It is noticeable that our filter can reduce the alarms in a range from 62% to 83%. For instance, the filter could have a filtration rate of 80%, 83% and 82% for Day2, Day3 and Day8, respectively. *Precision* here indicates the classifier's capability of identifying false alarms. The figure shows that our filter could reach an accuracy ranged from 0.88 to 0.93, i.e., achieved a rate of 0.9, 0.93 and 0.89 for Day2, Day3 and Day8, respectively. These results demonstrate that our filter - MFAFilter could perform well in a practical environment. Figure 8 further compared our filter with several traditional classifiers including SVM (LibSVM), KNN, NN (RBFNetwork) and DT, which had provided good performance in the simulated environment. It is found that our filter could reach a better accuracy than these supervised classifiers. The IT administrators from the participating organization also confirmed this observation, and they believed that MFAFilter can help lighten their workload in analyzing and reducing alarms each day.

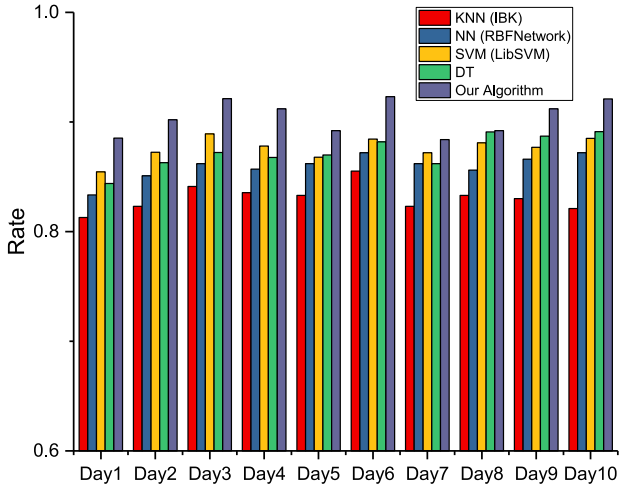


FIGURE 8. The performance comparison among different classifiers in the real environment.

TABLE 3. Training times (in seconds) required for building classifier models.

Algorithm	DATASET1	DATASET2	DATASET3
ZeroR	< 0.01	< 0.01	< 0.01
Fuzzy (IF-THEN)	0.63	1.46	1.13
KNN (IBK)	< 0.01	< 0.01	< 0.01
SVM (LibSVM)	0.28	0.52	0.43
SVM (SMO)	0.72	3.41	0.97
NaiveBayes	0.02	0.02	0.02
NN (RBFNetwork)	0.11	0.19	0.14
DT (J48)	0.06	0.24	0.07

V. DISCUSSION

The experimental results demonstrated that our filter could achieve good filtration performance and accuracy in practical scenarios. However, there are still some challenges in this area due to the features of healthcare environments.

A. TRAINING TIME

Intuitively, machine learning classifiers have to require sometime to build a model, which can be used in data classification. To explore this issue, we compare the training time for fuzzy if-then rules with other classifiers. The results based on the three datasets are shown in Table 3.

It is found that ZeroR and KNN classifier can finish training much faster than other classifiers, i.e., they finished the training with less than one second. NaiveBayes and DT could also reach a fast training phase. In comparison, fuzzy if-then rules need more time to build a model; however, the time consumption is acceptable in practice, as suggested by the healthcare IT administrator. This is because the training phase can be completed off-line. Through balancing the accuracy and the time consumption, it is believed that our filter is still promising in practical scenarios.

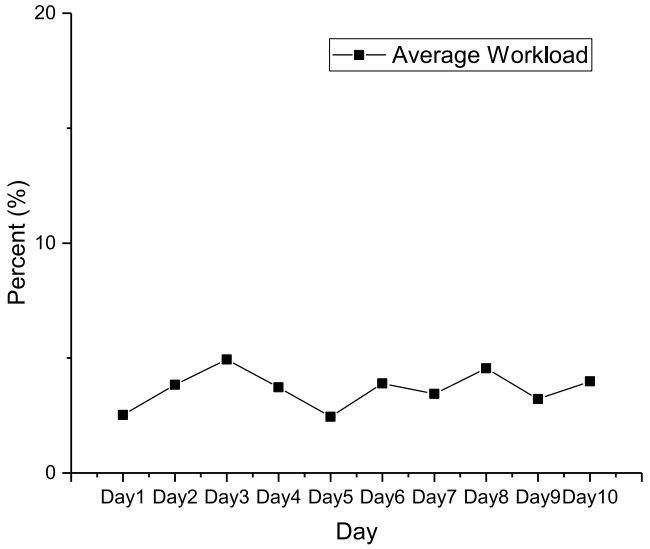


FIGURE 9. The average increased CPU workload by the deployment of alarm filter.

B. WORKLOAD

It is reasonable that deploying the alarm filter may increase some workload on the server side. To explore this issue, we implemented the filter on a Windows platform with Intel(R) Core(TM)2 Duo CPU, processor 2.8GHz and 4 GB of RAM. The average CPU workload caused by the filter is presented in Figure 9.

It is found that the increased CPU workload on average falls in a range from 2% to 5%, which is mainly caused by some filter operations, such as alarm classification, alarm filtration, and periodic classifier re-training. The IT administrator confirmed that such workload is acceptable in the practical environment. Thus, we consider that the deployment of MFAFilter would bring reasonable burden for real-world implementation.

C. PRECISION

For reducing alarms in the healthcare domain, decreasing false positives is more important than false negatives. This is because filtering true alarms may cause severe issues, i.e., delaying the diagnosis of patient. It is a common challenge in reducing false alarms for medical systems. In our work, all labeled false alarms would be stored for re-validation. As another solution, IT administrators can setup a list of sensors that should be given special attention. Then alarms from these sensors should be carefully examined by healthcare experts, and the filter can help advise a label to distinguish false and true alarms.

In addition, a classifier's precision can be further improved by updating training data in a regular way [32], or by integrating contextual information regarding the deployed environment [28]. To maintain the performance, there is an alternative to implement an intelligent false alarm filter by adaptively selecting the most appropriate classifier for alarm reduction [25].

D. SENSOR FEATURES

In this work, we mainly focus on the alarms with the features as shown in Figure 3. In practical scenarios, there would be many more features available depending on specific medical sensors. For example, biomedical sensors can be used to gather various physiological data. It is one of our future work to investigate the performance of our filter on other feature sets. As a result, we acknowledge that our current classifier and filter are effective in our settings.

VI. CONCLUSION

Medical sensor networks are an important part of CPS applications in the healthcare domain. However, these sensors may generate a large amount of false alarms, which could significantly reduce the effectiveness of medical systems and waste resources.

Focused on this issue, in this paper, we advocate the construction of alarm filters and attempt to design an alarm filter for healthcare environments by means of fuzzy if-then rules, which could handle the vague and imprecise among data. In the evaluation, we conducted two major experiments to test the filter in a simulated and a real network environment, respectively. As compared to other supervised classifiers, the experimental results demonstrate that fuzzy if-then rules can achieve a better classification accuracy and precision, and that our filter can work well with acceptable workload in a practical medical environment.

Our future work could include investigating the performance of fuzzy if-then rules in other medical network environments and validating the results obtained from this work. Future work could also include studying the influence of setting different parameters on the performance of fuzzy if-then rules, and implementing suitable privacy-preserving techniques (e.g., [40], [41]) to protect data privacy for healthcare applications.

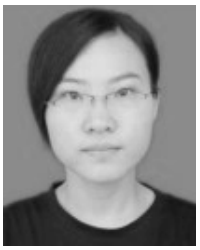
ACKNOWLEDGMENTS

The authors would like to thank the anonymous reviewers for their helpful comments. This work was extended from our previous version in Proc. of the 9th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD), pp. 505–509, 2012. [27].

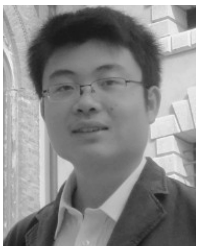
REFERENCES

[1] A. Alharby and H. Imai, "IDS false alarm reduction using continuous and discontinuous patterns," in *Proc. 3rd Int. Conf. Appl. Cryptogr. Netw. Secur. (ACNS)*, 2005, pp. 192–205.
[2] D. Bolzoni, B. Crispo, and S. Etalle, "ATLANTIDES: An architecture for alert verification in network intrusion detection systems," in *Proc. 21st Large Installation Syst. Admin. Conf. (LISA)*, 2007, pp. 141–152.
[3] S. M. Bridges and R. B. Vaughn, "Fuzzy data mining and genetic algorithms applied to intrusion detection," in *Proc. Nat. Inf. Syst. Secur. Conf.*, 2000, pp. 13–31.
[4] C.-Y. Chiu, Y.-J. Lee, C.-C. Chang, W.-Y. Luo, and H.-C. Huang, "Semi-supervised learning for false alarm reduction," in *Proc. 10th Ind. Conf. Adv. Data Mining (ICDM)*, 2010, pp. 595–605.
[5] J. E. Dickerson and J. A. Dickerson, "Fuzzy network profiling for intrusion detection," in *Proc. 19th Int. Conf. North Amer. Fuzzy Inf. Soc. (NAFIPS)*, 2000, pp. 301–306.
[6] J. E. Dickerson, J. Juslin, O. Koukousoula, and J. A. Dickerson, "Fuzzy intrusion detection," in *Proc. 20th Int. Conf. North Amer. Fuzzy Inf. Soc. (NAFIPS)*, 2001, pp. 1506–1510.

[7] A. El-Semary, J. Edmonds, J. Gonzalez, and M. Papa, "A framework for hybrid fuzzy logic intrusion detection systems," in *Proc. 14th Int. Conf. Fuzzy Syst.*, Reno, NV, USA, May 2005, pp. 325–330.
[8] F. Geramiraz, A. S. Memaripour, and M. Abbaspour, "Adaptive anomaly-based intrusion detection system using fuzzy controller," *Int. J. Netw. Secur.*, vol. 14, no. 6, pp. 352–361, 2012.
[9] R. Goel, A. Sardana, and R. C. Joshi, "Parallel misuse and anomaly detection model," *Int. J. Netw. Secur.*, vol. 14, no. 4, pp. 211–222, 2012.
[10] S. A. Haque and S. M. Aziz, "False alarm detection in cyber-physical systems for healthcare applications," in *Proc. AASRI Conf. Parallel Distrib. Comput. Syst.*, vol. 5, pp. 54–61, Nov. 2013.
[11] S. A. Haque, M. Rahman, and S. M. Aziz, "Sensor anomaly detection in wireless sensor networks for healthcare," *Sensors*, vol. 15, no. 4, pp. 8764–8786, 2015.
[12] S. A. Haque, S. M. Aziz, and M. Rahman, "Review of cyber-physical system in healthcare," *Int. J. Distrib. Sensor Netw.*, vol. 10, no. 4, 2014, Art. no. 217415.
[13] N. Hubballi, S. Biswas, and S. Nandi, "Towards reducing false alarms in network intrusion detection systems with data summarization technique," *Secur. Commun. Netw.*, vol. 6, no. 3, pp. 275–285, 2013.
[14] H. Ishibuchi, K. Nozaki, and H. Tanaka, "Distributed representation of fuzzy rules and its application to pattern classification," *Fuzzy Sets Syst.*, vol. 52, no. 1, pp. 21–32, 1992.
[15] H. Ishibuchi, T. Nakashima, and T. Morisawa, "Simple fuzzy rule-based classification systems perform well on commonly used real-world data sets," in *Proc. Annu. Meeting North Amer. Fuzzy Inf. Process. Soc. (NAFIPS)*, Syracuse, NY, USA, Sep. 1997, pp. 251–256.
[16] H. Ishibuchi, T. Murata, and M. Gen, "Performance evaluation of fuzzy rule-based classification systems obtained by multi-objective genetic algorithms," *Comput. Ind. Eng.*, vol. 35, nos. 3–4, pp. 575–578, 1998.
[17] A. Jamdagni, Z. Tan, X. He, P. Nanda, and R. P. Liu, "RePIDS: A multi tier real-time payload-based intrusion detection system," *Comput. Netw.*, vol. 57, no. 3, pp. 811–824, 2013.
[18] Z. Jiang, M. Pajic, and R. Mangharam, "Cyber–physical modeling of implantable cardiac medical devices," *Proc. IEEE*, vol. 100, no. 1, pp. 122–137, Jan. 2012.
[19] K. H. Law and L.-F. Kwok, "IDS false alarm filtering using KNN classifier," in *Proc. 5th Int. Workshop Inf. Secur. Appl. (WISA)*, 2005, pp. 114–121.
[20] I. Lee and O. Sokolsky, "Medical cyber physical systems," in *Proc. 47th Design Autom. Conf. (DAC)*, Jun. 2010, pp. 743–748.
[21] R. P. Lippmann *et al.*, "Evaluating intrusion detection systems: The 1998 DARPA off-line intrusion detection evaluation," in *Proc. DARPA Inf. Survivability Conf. Expo.*, Jan. 2000, pp. 12–26.
[22] A. Lounis, A. Hadjidj, A. Bouabdallah, and Y. Challal, "Secure and scalable cloud-based architecture for e-health Wireless sensor networks," in *Proc. Int. Conf. Comput. Commun. Netw. (ICCCN)*, Munich, Germany, Jul. 2012, pp. 1–7.
[23] J. Luo, S. M. Bridges, and R. B. Vaughn, "Fuzzy frequent episodes for real-time intrusion detection," in *Proc. 10th Int. Conf. Fuzzy Syst.*, Melbourne, VIC, Australia, Dec. 2001, pp. 368–371.
[24] C.-H. Mao, H.-M. Lee, D. Parikh, T. Chen, and S.-Y. Huang, "Semi-supervised co-training and active learning based approach for multi-view intrusion detection," in *Proc. ACM Symp. Appl. Comput. (SAC)*, 2009, pp. 2042–2048.
[25] Y. Meng and L.-F. Kwok, "Adaptive false alarm filter using machine learning in intrusion detection," in *Proc. 6th Int. Conf. Intell. Syst. Knowl. Eng. (ISKE)*, 2011, pp. 573–584.
[26] Y. Meng, W. Li, and L.-F. Kwok, "Intelligent alarm filter using knowledge-based alert verification in network intrusion detection," in *Proc. 20th Int. Symp. Methodol. Intell. Syst. (ISMIS)*, 2012, pp. 115–124.
[27] Y. Meng and L.-F. Kwok, "A case study: Intelligent false alarm reduction using fuzzy if-then rules in network intrusion detection," in *Proc. 9th Int. Conf. Fuzzy Syst. Knowl. Discovery (FSKD)*, May 2012, pp. 505–509.
[28] Y. Meng and W. Li, "Constructing context-based non-critical alarm filter in intrusion detection," in *Proc. 7th Int. Conf. Internet Monitor. Protection (ICIMP)*, 2012, pp. 75–81.
[29] Y. Meng and L.-F. Kwok, "Enhancing false alarm reduction using pool-based active learning in network intrusion detection," in *Proc. 9th Inf. Secur. Pract. Exper. Conf. (ISPEC)*, 2013, pp. 1–16.
[30] Y. Meng and L.-F. Kwok, "Adaptive non-critical alarm reduction using hash-based contextual signatures in intrusion detection," *Comput. Commun.*, vol. 38, pp. 50–59, Feb. 2014.
[31] Y. Meng and L.-F. Kwok, "Adaptive blacklist-based packet filter with a statistic-based approach in network intrusion detection," *J. Netw. Comput. Appl.*, vol. 39, pp. 83–92, Mar. 2014.
[32] Y. Meng, W. Li, and L.-F. Kwok, "Design of intelligent KNN-based alarm filter using knowledge-based alert verification in intrusion detection," *Secur. Commun. Netw.*, vol. 8, no. 18, pp. 3883–3895, 2015.
[33] W. Meng, W. Li, Y. Xiang, K.-K. R. Choo, "A Bayesian inference-based detection mechanism to defend medical smartphone networks against insider attacks," *J. Netw. Comput. Appl.*, vol. 78, pp. 162–169, Jan. 2017.
[34] T. Pietraszek, "Using adaptive alert classification to reduce false positives in intrusion detection," in *Proc. 7th Int. Symp. Recent Adv. Intrusion Detection (RAID)*, 2004, pp. 102–124.
[35] L.-A. Tang *et al.*, "Trustworthiness analysis of sensor data in cyber-physical systems," *J. Comput. Syst. Sci.*, vol. 79, no. 3, pp. 383–401, 2013.
[36] J.-F. Tian, Y. Fu, Y. Xu, and J.-L. Wang, "Intrusion Detection Combining Multiple Decision Trees by Fuzzy logic," in *Proc. 6th Int. Conf. Parallel Distrib. Comput., Appl. Technol. (PDCAT)*, Dalian, China, Dec. 2005, pp. 256–258.
[37] K. Tabia and P. Leray, "Alert correlation: Severe attack prediction and controlling false alarm rate tradeoffs," *Intell. Data Anal.*, vol. 15, no. 6, pp. 955–978, 2011.
[38] J. Wang, H. Abid, S. Lee, L. Shu, and F. Xia, "A secured health care application architecture for cyber-physical systems," *Control Eng. Appl. Inform.*, vol. 13, no. 3, pp. 101–108, 2011.
[39] *WEKA: Data Mining Software in Java*. Accessed: Oct. 15, 2017. [Online]. Available: http://www.cs.waikato.ac.nz/ml/weka/
[40] Q. Zhang, L. T. Yang, Z. Chen, and P. Li, "PPHOPCM: Privacy-preserving high-order possibilistic c-means algorithm for big data clustering with cloud computing," *IEEE Trans. Big Data*, to be published.
[41] Q. Zhang, L. T. Yang, Z. Chen, P. Li, and M. J. Deen, "Privacy-preserving double-projection deep computation model with crowdsourcing on cloud for big data feature learning," *IEEE Internet Things J.*, to be published.



WENJUAN LI (S'15) is currently pursuing the Ph.D. degree with the Department of Computer Science, City University of Hong Kong (CityU). She holds a visiting position with the Department of Applied Mathematics and Computer Science, Technical University of Denmark, Denmark. Prior to this, she was a Research Assistant with CityU, Hong Kong, and previously a Lecturer with the Department of Computer Science, Zhaoqing Foreign Language College, China. Her research interests include network management and security, collaborative intrusion detection, spam detection, trust computing, Web technology, and E-commerce technology. She was a winner of Cyber Quiz and Computer Security Competition in the Final Round of Kaspersky Laboratory Cyber Security for the Next Generation Conference in 2014.



WEIZHI MENG (M'10) received the B.Eng. degree in computer science from the Nanjing University of Posts and Telecommunications, China, and the Ph.D. degree in computer science from the City University of Hong Kong (CityU), Hong Kong. He is currently an Assistant Professor with the Department of Applied Mathematics and Computer Science, Technical University of Denmark (DTU), Denmark. He was known as Yuxin Meng and prior to joining DTU, he was a Research Scientist with the Infocomm Security Department, Institute for Infocomm Research, Singapore, and as a Senior Research Associate with CityU. His primary research interests are cyber security and intelligent technology in security including intrusion detection, mobile security and authentication, HCI security, cloud security, trust computation, web security, malware, and vulnerability analysis. He also shows a strong interest in applied cryptography. He was a recipient of the Outstanding Academic Performance Award during the Ph.D. study and also a recipient of the HKIE Outstanding Paper Award for Young Engineers/Researchers in 2014 and 2017. He is also a co-recipient of the Best Student Paper Award from the 10th International Conference on Network and System Security in 2016.

CHUNHUA SU received the B.S. degree for the Beijing Electronic and Science Institute in 2003, and the M.S. and Ph.D. degrees in computer science from the Faculty of Engineering, Kyushu University, in 2006 and 2009, respectively. He is currently an Associate Professor with the Division of Computer Science, University of Aizu. He was a Research Scientist with the Cryptography and Security Department, Institute for Infocomm Research, Singapore, from 2011 to 2013. From 2013 to 2016, he was an Assistant Professor with the School of Information Science, Japan Advanced Institute of Science and Technology. From 2016 to 2017, he was an Assistant Professor with the Graduate School of Engineering, Osaka University. His research interests include cryptanalysis, cryptographic protocols, privacy-preserving technologies in data mining, and IoT security and privacy.

LAM FOR KWOK received the M.Phil. degree in U.K. and the Ph.D. degree in information security from the Queensland University of Technology, Australia. He is currently an Associate Professor with the Department of Computer Science and the Executive Director of CityU Business and Industrial Club with the City University of Hong Kong. His research interests include information security and management, intrusion detection systems, and application of IT in education and web-based information systems. He was the Chairman with the IT Division, from 2010 to 2012. He is currently the Chairman with the Information Discipline Advisory Panel, Hong Kong Institution of Engineers. He is a Fellow of Hong Kong Institution of Engineers and British Computer Society.