Hybrid Approach for Intrusion Detection Using Fuzzy Association Rules Plus Anomaly and Misuse Detection

Samira Douzi, Ibtissam Benchaji, and Bouabid El Ouahidi

Abstract—**In today's world, users and enterprises are facing a growing number of internet attacks that are causing damage to their networks. The design and implementation of efficient intrusion detection algorithms is mandatory to minimise such damage and to preserve the integrity and availability of computer networks. Our study, which differs from some of the approaches in the literature that handle anomaly detection and misuse detection separately and, then, aggregate the outcomes, is a novel method for intrusion detection in network traffic based on a hybrid system that hierarchically combines anomaly detection, misuse detection and fuzzy rules. Two techniques for feature selection are used in the training phase, consisting first of reducing the feature space with an Autoencoder and, then, using the Weighted Fuzzy C-Mean Clustering Algorithm (WFCM) to identify the relevant features that are highly predictive in detecting malicious behaviour. These techniques are applied to reduce the input data, which influences the number of fuzzy rules generated. The proposed approach aims to be an accurate and flexible detection system that minimises the number of false alarms and increases the intrusion detection rate.**

Index Terms—**Anomaly detection, deep learning, fuzzy logic, misuse detection.**

I. Introduction

In cybersecurity, the increasing dependence that companies have on their computer networks makes their protection from intrusion a critical issue. These attacks are used by intruders to perform malicious activities, leading to the loss or unauthorised use of large amounts of data on the network. To mitigate the effects of a network attack, an intrusion detection system (IDS) must accurately and quickly identify the attack to prevent further damage.

There are two main intrusion detection approaches: misuse and anomaly intrusion detection. Misuse intrusion detection is a rule-based approach that uses stored signatures of known intrusion instances to detect an attack. This approach is highly successful in detecting occurrences of previously known attacks. The main drawback of this approach is its inability to identify and characterise new attacks and to respond to them intelligently. On the other hand, anomaly detection algorithms analyse activities that vary from the established patterns for normal users and classify such behaviour as an attack. Anomaly detection algorithms can be useful for new attack patterns; however, they have lower detection rates for known attacks and higher false positive rates than misuse detection models.

Furthermore, detecting network intrusions efficiently requires the collection of large numbers of network transactions, including the full details of recent transactions.

To develop an effective ID and achieve a tradeoff between detecting new attacks, maintaining a low false alarm rate, and dimensionality reduction, we propose a new hybrid fuzzy system that hierarchically integrates anomaly detection, misuse detection, and fuzzy rules to create an accurate network profile in an environment with imprecision and uncertainty.

Our hybrid approach has two main phases. In the training phase, we filter the data using two feature selection techniques. First, we reduce the feature space with an Autoencoder and, then, we use the weighted fuzzy C-mean (WCFM) clustering algorithm to identify the relevant features that are highly predictive in identifying malicious behaviour. This allows us to reduce the input data and easily construct if-then rules for our fuzzy logic system. In the detection phase, we use machine learning classifiers and fuzzy rules. We exhibit how an intrusion detection model can be built and used to find system attacks.

The remainder of this paper is organised as follows. Section II summarises some related works from the recent literature. The training phase is presented in Section III. Section IV describes the testing phase of the implemented fuzzy network IDS. Finally, the conclusion and plans for future work are presented in Section V.

II. Related Works

German Florez *et al.* extracted a set of fuzzy association rules from a network audit of a normal class. To detect anomalous behaviour, they generated fuzzy association rules from new audit data and computed the similarity with sets mined from normal data [1]. The drawback of this method is it cannot classify a single transaction, since it requires a set of test transactions to derive a rule set. Bharanidharan Shanmugam and Idris proposed a hybrid model based on improved fuzzy and data mining techniques, which can detect both misuse and anomaly attacks [2]. Martin Botha *et al.* [3] combined neural networks and fuzzy logic. They determined patterns of misuse by mapping a template graph of user actions. The output of this mapping process is used by the central strategic engine to determine whether an intrusion has taken place. The major disadvantage of this method is it does

Manuscript received. July 22, 2018; revised September 6, 2018.

The authors are with University Mohammed V Faculty of Science IPSS. B.O. 1014, Rabat, Morocco (e-mail: samiradouzi8@ gmail.com, b.ibtissam@gmail.com, Bouabid.ouahidi@gmail.com).

doi: 10.18178/ijmlc.2018.8.5.738

not automate the rule generation process and for a new type of attack; the rules have to be given by an external security officer. Arman Tajbakhsh *et al*. [4] proposed a classification algorithm that uses fuzzy association rules to build classifiers. The rule sets are exploited as descriptive models of different classes based on a compatibility threshold. This system uses the WFCM clustering algorithm to define fuzzy membership functions and it uses hyperedges for item or feature reduction. Hamamoto *et al*. [5] proposed a scheme combining a genetic algorithm and fuzzy logic for network anomaly detection. The genetic algorithm is used to generate a digital signature of a network segment, and the fuzzy logic scheme decides whether an instance represents an anomaly. With real network traffic, the proposed approach achieves an accuracy of 96.53% and a false positive rate of 0.56%.

III. Background

The main problem in predicting network behaviour is it can change suddenly depending on the environment. Furthermore, the nature of an anomaly depends on its context and on how it occurred. Thus, fuzzy logic is used to verify whether some behaviour is an anomaly based on the membership function and rules.

A. Fuzzy Set Theory

Classic logic is based on two truth values: true or false. However, it is sometimes inadequate with unreliable and incomplete information, and therefore, it is unable to produce a decision. The theory of fuzzy sets, first introduced by Zadeh in 1965, provides an appropriate framework for representing and processing vague concepts by allowing partial membership [6].

A fuzzy set *F* is any set that allows its members to have different degrees of membership. $u_F(\ )$ is the membership function of *F* and $u_F(a)$ indicates the membership degree of an element *a* in F.

Let $A = \{a_1, a_2, \dots, a_n\}$ be the set where a_j represents the *j*th record in *A*. Then,

$$F = \{(a_j, u_F(a_j))/a_j \in A, u_F(a_j) \in]0,1]\},$$

where $1 \le j \le n$.

An example of the membership function is the Gaussian function, defined by:

$$u_F(a) = e^{\frac{-(a-\hat{a})^2}{2\theta^2}}, \tag{1}$$

where *a* is the member, $\hat{a}$ is the center, and θ is a parameter that defines the standard deviation.

The advantages of fuzzy logic are that human reasoning can be represented in terms of if-then rules, which can be used as expert knowledge. As an example of fuzziness, we consider the concept ‘young’. There is no single quantitative value that defines the term ‘young’. The age {1 year} is definitely young and the age {100 years} is definitely not young; however, the age {35 years} may be considered young, depending on the context in which it is being considered.

B. Fuzzy Association Rules

Let $T = \{t_1, t_2, \dots, t_n\}$ be a database of transactions. $A = \{a_1, a_2, \dots, a_m\}$ is used to represents all attributes in *T* such as:

$$\forall t_j \in T,\ t_j = \{a_1, a_2, \dots, a_k\},\ 1 \le j \le n,\ 1 \le k \le m.$$

Moreover, each feature a_k is associated with a fuzzy set

$$F = \{F_{a_k}^1, \mathrm{F}_{a_k}^2, \dots, F_{a_k}^N\}.$$

Given the database *T* with a set of attributes *A* and the definitions of fuzzy sets associated with each feature in *A*, the objective is to find some interesting regularities (rules) between features values. To demonstrate this, we provide the following example (Table I), where $T = \{t_1, t_2, t_3\}$ is a sample database with three records. Here

$$A = \{a_1 = \text{speed},\ a_2 = \text{acceleration},\ a_3 = \text{distance}\}$$

represents all the features in *T*. The fuzzy set of the feature a_3 (distance), for example, is:

$$F_{a_3} = \{\text{very close, close, distant, very distant}\}.$$

TABLE I: A Sample Database

Speed	Acceleration	Distance
Slow	Decelerating	Very close
Optimum	Constant	Close
Fast	Accelerating	Distant
Too Fast	–	Very distant

IV. Proposed IDS Method

The proposed framework for intrusion detection has two distinct phases: training (Fig. 1) and detection (Fig. 4). The figures depict a schematic view of the different modules involved.

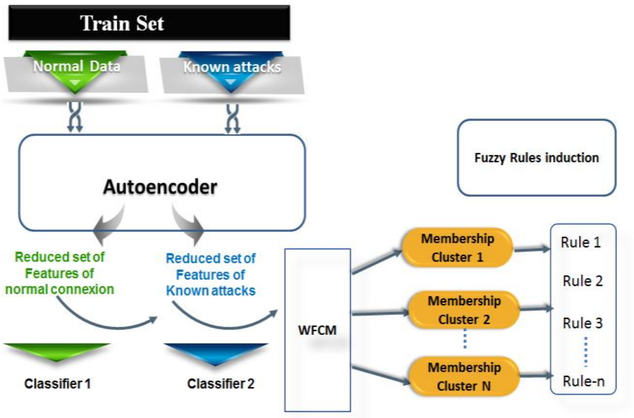

Fig. 1. Training phase.

A. Training Process

1) Feature selection using an autoencoder

As irrelevant features increase processing times and reduce detection accuracy and the efficiency of the IDS, feature selection is a fundamental preprocessing step in an IDS. First, to select the optimal subset of relevant attributes, we must remove redundant, noisy, and irrelevant features. Second, we need to decrease the computational cost without having a negative effect on the classification accuracy.

An autoencoder is a special form of a neural network designed for unsupervised learning, since there is no label variable (Fig. 2). It consists of an encoder and a decoder. The encoder transforms the input data (*X*) into high-level features (*Z*), while the decoder tries to reconstruct the input data (the reconstruction output, *Y*) using high-level features (i.e. *Z*) by minimizing the reconstruction residuals between *X* and *Y*, which are evaluated using mean squared errors or cross-entropy losses [7], [8].

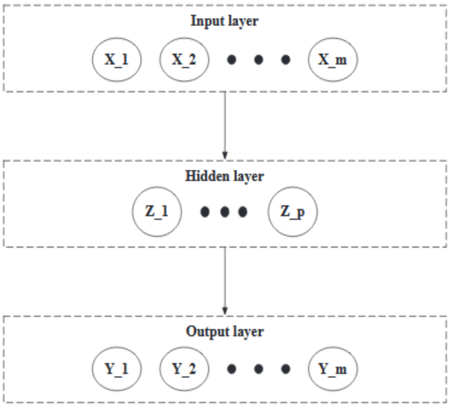

Fig. 2. The Autoencoder architecture.

Here,

$$z_i = f(W_1 \times x_i + b_1) \text{ and}$$
$$y_i = g(W_1^T \times z_i + \hat{b}_1), \tag{2}$$

where W_1 and W_1^T are weight matrices and b_1 and $\hat{b}_1$ are bias vectors.

To extract features that can distinguish normal activities from intrusion, the training data are partitioned based on their labels, such that normal transactions are in one set and the attack transactions are in another. The Autoencoder is applied on both subsets to generate robust and discriminative features for normal and attack data. Fig. 1 is a schematic diagram of this step.

After selecting the pertinent features of both models, the hybrid detection system is independently trained on misuse detection using the selected features of known attacks to build a classifier. The anomaly detection model also builds a classifier based on features selected from the normal data. Using these adaptive learning classifiers, we have improved the usability of our system. We have facilitated model construction by reducing the amount of analysis required for new data, since it is easy for the trained classifiers to label the data.

2) Fuzzy intrusion detection model

a) Fuzzy input and membership function

Fuzzy logic can be an effective way of defining network attacks by constructing if-then rules that reflect common ways of describing security attacks. However, the execution time for fuzzy rules increases exponentially with an increase in the number of features sniffed from the network; therefore, using many features is practically impossible.

On the other hand, there are no restrictions on the shape of membership functions, and in the literature we found plenty of techniques for tuning these functions [9]. However, how can we determine the membership functions with the best performance?

To deal with these two issues, we propose to use the WFCM clustering algorithm (5), which is a hard clustering method. Each data record can belong to more than one cluster with a different degree of membership in each. We assign a weight to each record.

Let $T = \{t_1, t_2, \ldots, t_n\}$ be the set of all transactions that are to be used for training and $A = \{a_1, a_2, \ldots, a_l\}$ be the set of features previously selected by the Autoencoder, such as $t_j = \{a_{1j}, a_{2j}, \ldots, a_{lj}\}, \forall j, 1 \le j \le n$. The feature vector is then $F = \{F_{a_k}^1, \mathrm{F}_{a_k}^2, \ldots, F_{a_k}^N\}, \forall k, 1 \le k \le l$,

where *N* is the desired number of fuzzy sets.

Assuming that the contribution weights of each entity in the feature vector are $w_1, w_2, \ldots, w_l$ with $w_k \ge 0, k = 1, \ldots, l$, then we have

$$t_k' = wt_k, \ \forall 1 \le k \le n, \tag{3}$$

with

$$w = \begin{bmatrix} w_1 & 0 & 0 & 0 & 0 \\ 0 & w_2 & 0 & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & 0 & w_l \end{bmatrix}.$$

The Euclidean distance between any two samples can be represented by:

$$d^2(t_k', t_j') = \left\| t_k' - t_j' \right\|^2 = (t_k' - t_j')^T (t_k' - t_j'), \forall k, j. \tag{4}$$

Substituting Eq. (3) into Eq. (4) and letting $W = w^T.w$, we have:

$$\begin{aligned} d^2(t_k', t_j') &= (t_k - t_j)^T W (t_k - t_j) \\ &= W \, \| t_k, t_j \|^2 \\ &= W d^2(t_k, t_j), \quad \forall k, j. \end{aligned} \tag{5}$$

WFCM introduces weights into each of the data dimensions to define the importance of each feature. In practical cluster analysis, the weight of each dimensional feature is not known in advance, and the matrix W needs to be optimised during the clustering.

WFCM is an iterative process involving cluster center $C = \{c_1, c_2, \ldots, c_N\}$, and membership matrix $U = \{u_{ij}\}, i = 1, \ldots, N, j = 1, \ldots, l,$ where u_{ij} denotes the grade of the *j*th feature, which belongs to the cluster of center c_i. The algorithm is as follows:

Algorithm: Weighted Fuzzy C-Means algorithm

```
Input: $A, N, m, W$, initialise cluster centers $C$
Output: $U, C$ (final centers)
While $e = \max_{1 \le i \le N} \left\{ \left\| c_{i,new} - c_{i,old} \right\|^2 \right\} \succ \xi$ ( $c_{i,new}$ and $c_{i,old}$ denote, respectively, the current and present cluster centers)
    Calculate $U$ using:
        $u_{kj} = \left[ \sum_{l=1}^{N} \left( \frac{\| a_{ij} - c_k \|}{\| a_{ij} - c_l \|} \right)^{\frac{2}{m-1}} \right]^{-1}, \forall i, j, k$
    Calculate $C$ using:
        $c_k = \frac{\sum_i^n \sum_j^l w_j u_{kj}^m a_{ij}}{\sum_i^n \sum_j^l w_j u_{kj}^m}, \forall 1 \le k \le N$
End while
```

The constrained optimization of WFCM is:

$$q = \sum_k^N \sum_i^n \sum_j^l w_j u_{k\,j}^m \, \| a_{i\,j} - c_k \|. \tag{6}$$

When the algorithm stops, we get the final cluster centers and membership matrix. Each of the data items belongs to the cluster centers (Fig. 3) that have the maximum degree of membership.

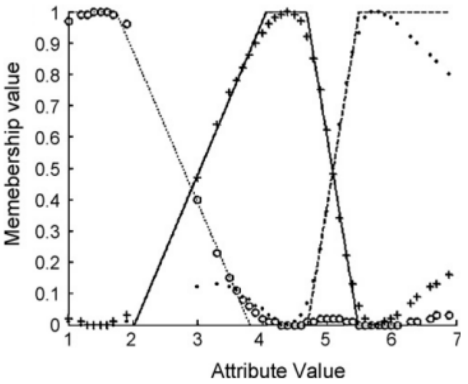

Fig. 3. Clustering-based membership function definition [4].

b) Generating Fuzzy Rules

The fuzzy rules describing the data are of the form:

If *A* is *X* then *B* is *Y*,

where *A* and *B* are sets of attributes and *X* and *Y* are fuzzy sets that describe *A* and *B*, respectively. The first part of the rule '*A* is *X*' is called the antecedent and '*B* is *Y*' is the consequent of the rule. If a rule is interesting, it should have enough significance and a high certainty factor. The significance and the certainty factor are used to determine the satisfiability of the item sets and rules.

Let $T = \{t_1, t_2, \ldots, t_n\}$ be the set of transactions, $A = \{a_1, a_2, \ldots, a_p\}$ the attribute set, $F = \{F_{a_1}, F_{a_2}, \ldots, F_{a_p}\}$ the fuzzy sets associated with the corresponding attributes in *A*, and $U = \{u_{F_1}, u_{F_2}, \ldots, u_{F_p}\}$ the set of membership functions of *A*, such that u_{F_j} represents the membership function of F_{a_j}. Each pair of $\langle a_k, F_{a_k} \rangle$ is called an item, and each pair of $\langle A, F \rangle$ is called an item set.

To generate fuzzy association rules, first, we have to find all the large item sets with a significance higher than a specified threshold. The classic significance factor of an item set is calculated by first summing all the votes for each record with respect to the specified item set, then, dividing it by the total number of records:

$$S_{(A,F)} = \frac{\sum_{t_i \in T} \prod_{a_j \in A} \left\{ \alpha_{F_j} \left(t_i \left[a_j \right] \right) \right\}}{\|T\|}, \tag{7}$$

where $\|T\|$ is the number of records in *T* and

$$\alpha_{F_j} \left(t_i \left[a_j \right] \right) = \begin{cases} u_{F_j \in A}(t_i \left[a_j \right]), & \text{if } u_{F_j} \ge \omega, \\ 0, & \text{otherwise.} \end{cases} \tag{8}$$

ω is a threshold used to avoid low membership values. $\prod_{a_j \in A} \left\{ \alpha_{F_j} \left(t_i \left[a_j \right] \right) \right\}$ is used to compute each record's vote. Other operators, such as min, could be used instead of mul (∏); however, the authors of [10] concluded that mul achieves better results.

In this work, we proposed to integrate the weights of the attributes to evaluate the relevance of an association rule. The vote of a record is calculated not only for the membership grade of each attribute a_i in that record, but also each attribute will be weighted in estimating the importance of an association rule.

The proposed formula is:

$$S_{(A,F)} = \frac{\sum_{t_i \in T} \prod_{a_j \in A} \left\{ w_j \alpha_{F_j} \left(t_i \left[a_j \right] \right) \right\}}{\|T\|}, \tag{9}$$

where w_j is the weight of feature a_j calculated by the WFCM algorithm in the previous step, and

$$\alpha_{F_j} \left(t_i \left[a_j \right] \right) = \begin{cases} u_{F_j \in F}(t_i \left[a_j \right]), & \text{if } u_{F_j} \ge \omega \text{ and } w_j \ge \theta, \\ 0, & \text{otherwise.} \end{cases} \tag{10}$$

The weight should not be less than the user-specified threshold θ, such that an attribute with low influence (weight) will not be considered. The final output of this step is a set of rules that measure the degree of support given by records. This helps us to estimate the interestingness of the generated fuzzy association rule.

B. Detection Phase

The detection phase aims to assign a label to each new connection. Fig. 4 illustrates our approach in this phase. The steps involved in operationalizing the proposed method are:

Step 1: Extract the relevant features from the new connection.

Step 2: First, the connection is analysed by the anomaly detection component. The classifier trained on normal behaviours is applied to evaluate whether the attributes deviate significantly from the normal values. Then, if the connection is declared abnormal, it will be checked by the misuse detection component.

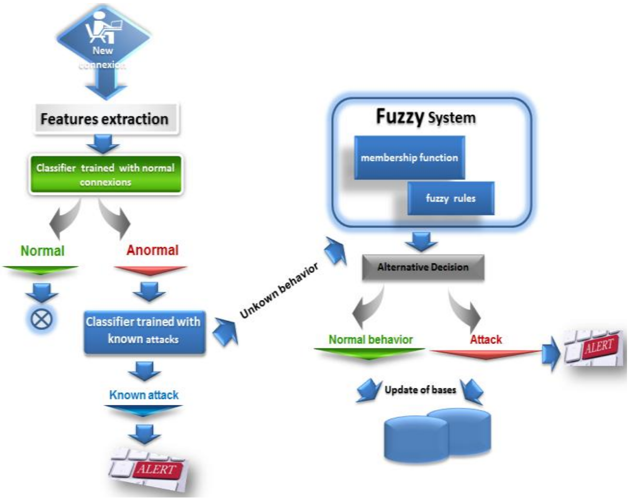

Fig. 4. Detection phase.

Step 3: If the transaction is very similar to the attacks in the training data, it will be labelled as such an attack, and the IDS will generate an attack alarm to inform the network security manager.

Step 4: Otherwise, if the new transaction is classified as an unknown behaviour, the fuzzification component uses the attributes to define the fuzzy membership values, and then it outputs a list of interesting rules that match the transaction well.

V. Conclusion

In the present work, we have proposed a hybrid fuzzy logic IDS for mitigating malicious behaviour within a network. It uses feature selection techniques, such as Autoencoder to reduce the input data and WFCM, which uses weights for each data dimension. We define a new formula for the significance of a rule. This approach aims to lower the false alarm rates, which are a very serious problem for an IDS, and it ensures the flexibility of the IDS in an environment with imprecision and uncertainty. Further work is to implement this approach using the programming language Python. This will allow us to validate our work and produce pertinent experimental results.

References

[1] G. Florez, S. A. Bridges, and R. B. Vaughn, "An improved algorithm for fuzzy data mining for intrusion detection," in *Proc. 2002 Annual Meeting of the North American Fuzzy Information Processing Society*.

[2] B. Shanmugam and N. B. Idris, "Improved intrusion detection system using fuzzy logic for detecting anamoly and misuse type of attacks," in *Proc. 2009 International Conference of Soft Computing and Pattern Recognition*, 2009, pp. 212-217.

[3] M. Botha, R. von Solms, K. Perry, E. Loubser, and G. Yamoyany, "The Utilization of Artificial Intelligence in a Hybrid Intrusion Detection System," in *Proc. the 2002 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists on Enablement Through Technology*, Republic of South Africa, 2002, pp. 149-155.

[4] A. Tajbakhsh, M. Rahmati, and A. Mirzaei, "Intrusion detection using fuzzy association rules," *Applied Soft Computing*, vol. 9, no. 2, pp. 462-469, March 2009.

[5] A. H. Hamamoto, L. F. Carvalho, L. D. H. Sampaio, T. Abrão, and M. L. Proença, "Network anomaly detection system using genetic algorithm and fuzzy logic," *Expert Systems with Applications*, vol. 92, pp. 390-402, February 2018.

[6] G. Kim, S. Lee, and S. Kim, "A novel hybrid intrusion detection method integrating anomaly detection with misuse detection," *Expert Systems with Applications*, vol. 41, no. 4, Part 2, pp. 1690-1700, March 2014.

[7] O. İrsoy and E. Alpaydın, "Unsupervised feature extraction with autoencoder trees," *Neurocomputing*, vol. 258, pp. 63-73, Oct. 2017.

[8] F. Zhuang, D. Luo, X. Jin, H. Xiong, P. Luo, and Q. He, "Representation learning via semi-supervised autoencoder for multi-task learning," in *Proc. 2015 IEEE International Conference on Data Mining*, 2015, pp. 1141-1146.

[9] E. Tombini, H. Debar, L. Me, and M. Ducasse, "A serial combination of anomaly and misuse IDSes applied to HTTP traffic," in *Proc. 20th Annual Computer Security Applications Conference*, 2004, pp. 428-437.

[10] A. Arslan and M. Kaya, "Determination of fuzzy logic membership functions using genetic algorithms," *Fuzzy Sets and Systems*, vol. 118, no. 2, pp. 297-306, march 2001.

Samira Douzi received the master degree in development quality in 2013, from the Department of Computer Science at the Faculty of Sciences Rabat Agdal. Since 2016 she is a predoctoral researcher in the Department Computer Science at the Faculty of Sciences Rabat Agdal where she is pursuing a Ph.D. degree. Her main researches interests include big data, deep learning and cyber security.

Benchaji Ibtissam received the engineer’s degree from the National School of Applied Sciences of Tangier, Morocco in 2009. She is currently a researcher at the Computer Science Department of University Mohammed V, Rabat, Morocco under the supervision of Prof. EL OUAHIDI Bouabid. Her current research interests include machine learning techniques for anomaly and fraud detection.

Bouabid El Ouahidi is a university professor and ex head of the Computer Science Department. He received Ph.D. Degree in computer security from the. University of Caen-France. His research interests include open distributed systems, quality of services of distributed applications, big data, cyber security and machine learning.