

# Automating cloud virtual machines allocation via machine learning

Ferdaous Kamoun-Abid, Hounaida Frikha, Amel Meddeb-Makhoulf, Faouzi Zarai

NTS'COM Research Unit Sfax, ENET'COM Sfax, Sfax, Tunisia

## Article Info

### Article history:

Received Jan 3, 2024

Revised Mar 2, 2024

Accepted Mar 30, 2024

### Keywords:

Controller

Divided-cloud

Firewall

KNN

LDA-decision tree

Machine learning

Virtual machine

## ABSTRACT

In the realm of healthcare applications leveraging cloud technology, ongoing progress is evident, yet current approaches are rigid and fail to adapt to the dynamic environment, particularly when network and virtual machine (VM) resources undergo modifications mid-execution. Health data is stored and processed in the cloud as virtual resources supported by numerous VMs, necessitating critical optimization of virtual node and data placement to enhance data application processing time. Network security poses a significant challenge in the cloud due to the dynamic nature of the topology, hindering traditional firewalls' ability to inspect packet contents and leaving the network vulnerable to potential threats. To address this, we propose dividing the cloud topology into zones, each monitored by a controller to oversee individual VMs under firewall protection, a framework termed divided-cloud, aiming to minimize network congestion while strategically placing new VMs. Employing machine learning (ML) techniques, such as decision tree (DT) and linear discriminant analysis (LDA), we achieved improved accuracy rates for adding new controllers, reaching a maximum of 89%, and used the K-neighbours classifier method to determine optimal locations for new VMs, achieving an accuracy of 83%.

This is an open access article under the [CC BY-SA](#) license.



## Corresponding Author:

Ferdaous Kamoun-Abid

NTS'COM Research Unit Sfax, ENET'COM Sfax

Sfax, Tunisia

Email: abidkamounferdaous@gmail.com

## 1. INTRODUCTION

The proliferation of information utilization has led to the adoption of cloud computing, an expeditious technology that offers adaptable, cost-efficient, and easily manageable access to potent computing and storage resources on demand. The integration of cloud computing into various sectors, such as medical applications, is particularly intriguing due to its scalability and elasticity [1]. Additionally, it is a cutting-edge technology heavily influenced by modern medical monitoring systems. A major challenge faced today is the secure delivery of cloud-based services to medical clients. The challenge arises from the inability of cloud service providers (CSPs) to assure data security when shared among multiple cloud customers [2]. cloud computing represents a rapidly evolving technology that offers cost-effective, flexible, and on-demand resource access. Its cornerstone is virtualization, which minimizes initial investments. Essentially, physical machines (PMs) enable the creation of numerous virtual machines (VMs) for managing medical services and information. Nonetheless, handling cloud storage introduces fresh hurdles concerning data security.

The studies in [3], [4] examined the effects of distributed firewalls. Although previous studies have explored the impact of the added a new improvements and functionalities to traditional firewalls. But they have not explicitly addressed the influence of the rules that are set on the architecture of mobile topologies such as cloud computing.

Traditional firewalls may lose their effectiveness due to the intricate nature of various network topologies. To address this issue, a cost-effective solution known as a distributed firewall has been developed [3]. This firewall is created using open-source tools, which bring about new enhancements and functionalities. Unlike traditional firewalls that examine and restrict incoming packets based on predefined rules, distributed firewalls analyze each packet independently, leading to certain limitations. However, this method proves to be quick, affordable, and effective in specific scenarios, as demonstrated by Tudosi *et al.* [3]. In their research, the authors configure the network topology into enterprise zones, which consist of both older and newer applications. They propose the use of distributed firewalls, which include a policy distribution scheme, a security policy, and an encryption/authentication mechanism. Consequently, traditional firewalls implemented at the network boundary are no longer efficient in this context. Instead, centralized firewalls, positioned between the internal network of an establishment and the internet, are replaced by distributed firewalls [4]. These distributed firewalls define security policies using a specific language in a centralized manner, to be implemented at various points within the network. These enforcement points can be found on different equipment, such as switches, routers, or individual machines within the network. Therefore, it is imperative to enhance the security level of cloud networks and ensure the protection of sensitive information against attacks. Numerous solutions have been proposed in existing literature [5], where in distributed firewalls are employed as a preventive measure to guarantee network access control.

Within the literature, researchers have explored various methods and approaches to ensure the accurate collection of physiological parameters from patients. Consequently, when exchanging data between communicating devices in a medical environment, security measures must be strengthened. In this context, set up a real-time medical internet of thing (IoT) platform that processes information collected by the deep learning method on biological signals [6]. The result of their work is that the detection accuracy of the deep neural network is compared to that of a human expert on electrocardiogram (ECG) signals, which predicts possible future health damages. Cao *et al.* [7] worked on system called tri-storage failure recovery (Tri-SFRS) by implementing a platform based on OpenStack for the medical IoT. This work uses several combined techniques included in a multcloud architecture, such as medical information storage and overload test framework. Asghari *et al.* [8] proposed a method of medical monitoring for the cloud-based IoT platform. The main goal of this work is to predict diseases based on the medical conditions of patients with the exploitation of physiological data collected from medical records and IoT devices. This is based on the deep learning method to reduce energy consumption and application cost in the dynamic environment. This method is called cost-efficient partitioning and task scheduling (DNNECTS) work includes the following components: task sequencing, application partitioning, and scheduling Lakhan *et al.* [9]. The previously presented works in [7], [9] deploy the cloud in the medical field, without considering the security and access control of the stored medical data. Indeed, the majority of research works reported in the current literature consider the location of physical nodes and the existence of VMs to save their information. But the problem is backing up this fact regardless of security. Chamas *et al.* [10] worked on the placement algorithm of VM in the cloud. They proposed two-phase for optimization, it is composed by an online incremental VM placement (VMP) phase (iVMP) and an offline VMP reconfiguration (VMPr) phase. Samely, Chamas *et al.* [10] and Shabeera *et al.* [11] proposed a method of location of VM and data. They used the algorithm based on ant colony optimization (ACO). In addition, they are focused on reducing inter-network traffic and bandwidth usage. Their method does this by placing a number of VM and data in physical machines that are physically closer. There are several works in the cloud-based health field such as the work of [12] that used the parallel particle swarm optimization (PPSo) method to the aim of optimizing the VMs selection. In addition, to measure the performance of their VMs model, they used a chronic kidney disease (CDK) model. Moreover, in this work the model is based on machine learning (ML), which is also used in the field of COVID-19. Moreover, Mukherjee *et al.* [13] proposed an enhanced k-nearest neighbour (KNN) algorithm. This work concerned a mended KNN attempting to find an optimal value of k and examining IoT-cloud-based COVID-19 detection by the basis of ML. Because studied researchers work lacks of intrusion detection and prevention, in the field of intrusion detection, we find [14] working on detecting botnet attacks by using the random forest which is a ML method. This work based on low power consumption ML for detecting attacks. Moreover, we find many researches using the virtual private network (VPN) and the ML in the cloud environment for security [15], [16] where Jayashri and Kalaiselvi [16] methodically detail the current security requirements for intelligent systems. It leverages cloud-based cryptanalysis and insights from current ML solutions to address a range of security issues.

Oudah *et al.* [17] simulate various methods and compare their effectiveness in handling nonlinear systems, it was determined that the use of fuzzy logic control provides optimal performance, effectively minimizing packet delivery delay and reducing packet loss. But they do not work on the notion of information security. Scientists in [18] introduces a modular attack detection tool comprising three classifiers using user attributes such as username, device ID and IP address. Their study is focused on multi-layer

perceptron, random forest algorithm and variations of support vector machine as types of classifiers. This work lacks the implementation of their work in a complex topology like cloud computing.

Indeed, the focus of this paper revolves around the distribution of firewalls and the management of distributed data through controllers. Our primary objective is to enhance cloud security and optimize communication costs between existing security devices within the cloud, while also considering load balancing. This is achieved through the following:

- The subdivision of the cloud network into zones, with each zone supervised by a dedicated firewall and each set of zones controlled by a controller. To accomplish this, we utilize the “decision tree” (DT) algorithm in the field of ML to optimize this process.
- The VM affiliation is established using the classification method with the “K-neighbors classifier” algorithm.
- Homomorphic encryption is employed for the exchange of rules and blocking information to ensure the security of the distributed firewall topology.

To present our work, the remaining part of this paper is presented as follows. Section 2 proposed solution presents. In section 3 details the methodology of proposed architecture. In section 4 we describe the results of our simulation. Finally, section 5 concludes the article and presents some future work.

## 2. PROPOSED DIVIDED-CLOUD ARCHITECTURE

The primary focus of our research is the distribution of firewalls/controllers through the migration of blocking rules among adjacent firewalls. This approach is based on our previously published study by [19]. Consequently, the main objective of dividing the environment is to minimize cross-network traffic and bandwidth usage by strategically placing the necessary number of controllers, VMs, and data in physically closer PMs.

Traditionally, firewalls are primarily utilized in small to medium-sized networks, as distributed firewalls are not suitable for more complex and dynamic networks like cloud networks, as mentioned by [20]. Therefore, when it comes to securing medical data stored in the cloud, we propose the utilization of distributed firewalls (DFs) and distributed controllers (DIC) at the cloud level. To achieve this, we introduce a cloud architecture known as divided-cloud. Figure 1 illustrates the proposed architecture, which divides the topology into zones. Each zone consists of a set of VMs and a controller. The network incorporates various biological sensors that are strategically placed on different parts of the human body and can be implanted under the patient's skin. This information is collected, stored, and accessed via a smartphone on the divided-cloud. Furthermore, the gathered medical data is transmitted and stored in the cloud using a VPN as mentioned by [21], [22].

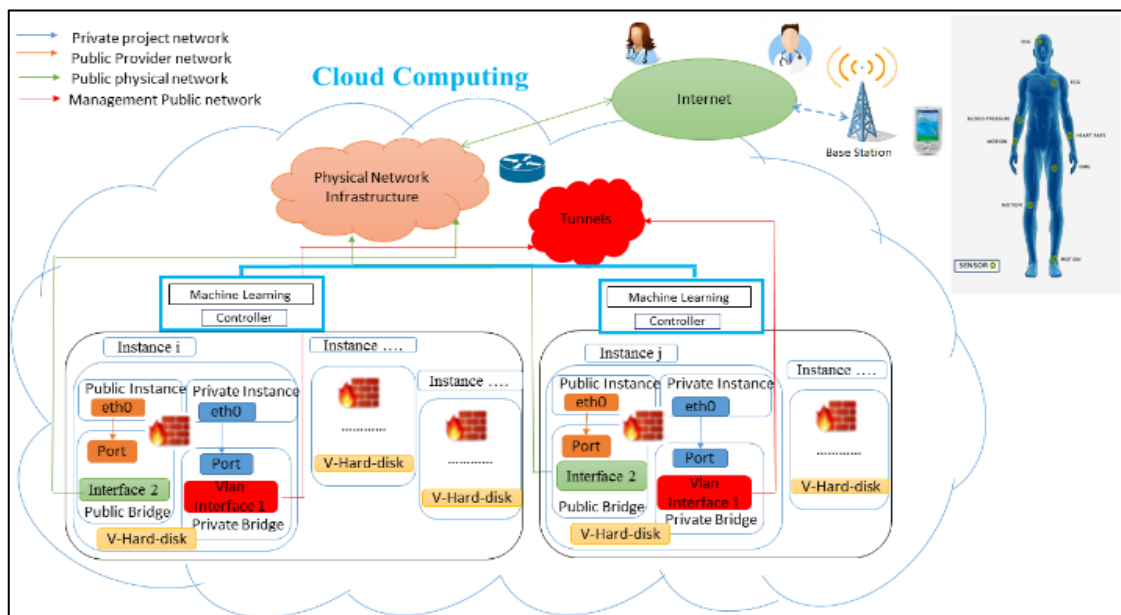


Figure 1. Proposed structure of divided-cloud

The cloud network consists of a group of VMs that are safeguarded by a firewall to regulate network access. To enable collaboration, the firewall blocks traffic and notifies neighbouring firewalls about the prohibited traffic. To achieve this, we suggest dividing the architecture into zones overseen by a controller, which helps minimize network overload when exchanging access control list ACL rules.

When a new instance needs to be added, it is essential to determine which zone it should belong to. This process is carried out using the KNN algorithm of ML. Alternatively, if a new zone needs to be added, a new controller must also be added. This step is based on the combination execution of the “DT” algorithm and “Linear discriminant analysis (LDA) algorithm”. The algorithm LDA is a supervised learning tool that seeks to create linear combinations of initial features that maximize the separation between classes in the data [23].

Our objective is to minimize the number of controllers by employing a ML classification algorithm. We propose classifying a new VM (i.e., determining its zone) to reduce the exchange of rules between topology components. Due to the variability of cloud topology, this work focuses on two aspects: (i) the need to add a new zone (and a new controller) based on the “DT” algorithm, and (ii) the classification of a VM when adding a new VM (to determine its zone) using the “K-Neighbours Classifier” learning algorithm.

The main concept of this study is to efficiently distribute the distributed intrusion detection and cooperation (DIC) in the divided-cloud network. Cooperation is achieved through monitoring functions, which involve migrating blocking information (when a VM detects a malicious packet) only to its neighbouring VMs.

### 3. DIVIDED-CLOUD METHOD

#### 3.1.1. Incremental DIC

To optimize the number of controllers, we propose using the “DT” ML method to determine when to add a new zone supervised by a new controller, as shown in Figure 2. We define the following set of metrics:

- Number of VMs per data center (DC): This refers to the number of VMs connected to a DC, with each VM only connected to one DC.
- Zone: index zone representing the number of existing zones in the topologies (we deploy 4 zones in our work).
- Number of firewalls per controller: this indicates the number of firewalls controlled by the same controller (we consider a range of 1 to 100 in our example).
- Number of VMs per zone: this represents the number of VMs present in a zone, with the zone’s capacity limited by a threshold set by the security administrator.
- Type of resource allocation: this is a string field with a size of 20 bits.

#### 3.1.2. Progressive DIC

To enhance the efficiency of controller allocation, we suggest employing the LDA-DT approach of ML to determine the addition of a new zone supervised by a new controller, as demonstrated in Figure 2. In this step we used LDA to project data into a lower dimensional space. Therefore, in this approach, we define the following set of metrics:

- Number of VMs per DC: the quantity of VMs associated with a single DC (a VM cannot be connected to two different DCs).
- Zone: index zone: number of controllers: the number of existing zones in the network topologies (in our study, we deploy 4 zones).
- Number of firewalls per controller: the number of firewalls controlled by the same controller (for our example, we utilized a range from 1 to 100).
- Number of VMs per zone: the number of VMs present within a zone (in our model, the zones have a capacity restricted by a threshold defined by the security administrator).
- Type of resource allocation: this is a string field. Therefore, the size of this field must be 20 bits.

Due to the dynamic nature of the cloud topology, we propose executing a constant time interval for every new VM creation. After running the learning process, the obtained results, which include the classification of the number of firewalls (FW) present in a zone, the number of VMs supervised by a FW, and the number of VMs existing in the same DC, are used to decide whether to add a new controller. As depicted in the flowchart in Figure 3, if the number of existing VMs in a zone exceeds a threshold value (S1), the next comparison is performed. Otherwise, the decision classifies as NULL. The subsequent step involves comparing the number of Firewalls present in an area. If this number surpasses a threshold value (S2), the decision classifies as 1 (indicating the addition of a new controller). Otherwise, it becomes

necessary to compare the number of VMs per DC to a threshold value (S3). If this number is greater than S3, the decision classifies as 1. Otherwise, the decision classifies as NULL. It should be noted that the thresholds (S1, S2, and S3) are determined by the cloud provider. In summary, comparisons resulting in a decision class of NULL indicate that adding a new controller is not necessary. On the other hand, comparisons resulting in a decision class of 1 indicate the need to add a controller.

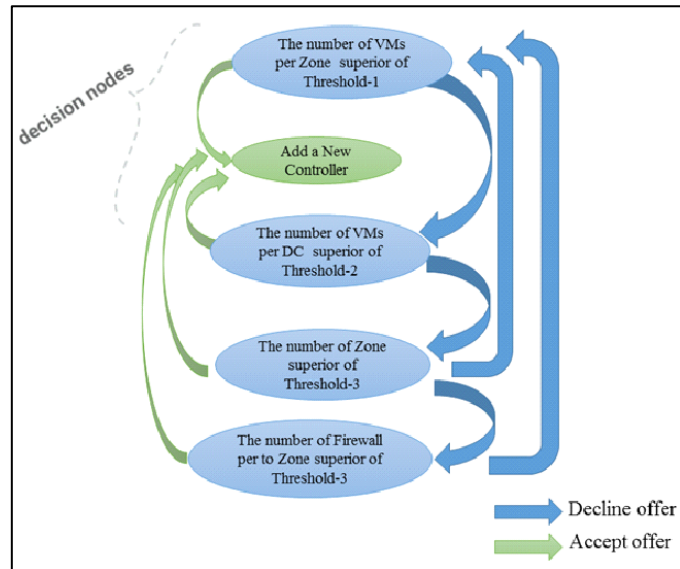


Figure 2. DT for adding a new controller

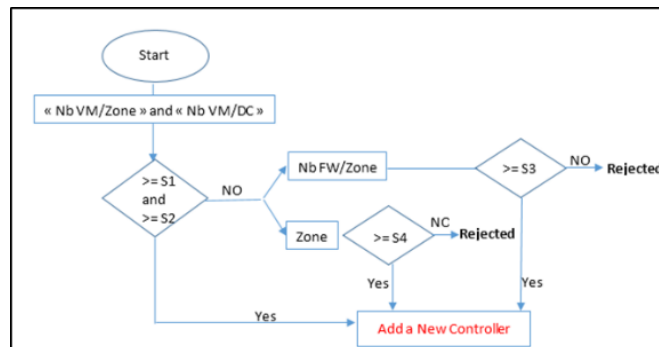


Figure 3. Flowchart representing incremental DIC

**3.1.3. VM classification overview**

A cloud zone consists of multiple VMs. When creating a new VM, it is necessary to determine the appropriate zone assignment and the maximum number of VMs per zone that can be supervised by a single controller. To achieve this, an ML classification algorithm called KNN is utilized. The purpose of this algorithm is to minimize network overload in terms of network flow control [24]. It works by calculating the distances between the sampled points and their nearest neighbours. Various types of distances, such as gaussian [25], are employed to identify the nearest neighbours.

The classification process is based on the following parameters:

- Round trip time (RTT): Indicates the proximity between VMs (i.e., the distance between them).
- Similarity of services provided by a VM.
- Number of VMs controlled by a single controller (i.e., the number of VMs existing in the same zone).
- Number of users connected per zone.

Figure 4 describes the membership of a new VM. The creation of a new VM does not require a distance calculation between existing VMs in different zones to make the decision to which the zone belongs.

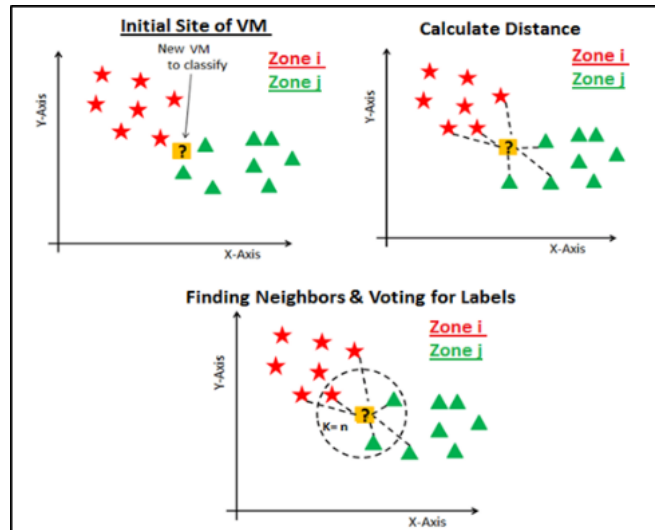


Figure 4. “K-neighbors classifier” to classify a VM

### 3.2. Ensuring secure information exchange

Our architecture is built upon distributed controllers connected to firewalls. Its primary objective is to manage and facilitate the exchange of rules between interconnected firewalls. Since information is transmitted over wireless links, it is crucial to safeguard the transmitted data against malicious attacks. As the transfer channels remain open, ensuring data security and confidentiality is one of the key requirements for transmitting data between controllers. To address this, we employ encryption techniques to ensure that the data is only accessible to authorized controllers, enabling them to perform necessary operations. The controller’s operation involves the exchange of rules between firewalls within the same zone, based on ACLs and the blocking data stored in a list referred to as the “new-list”. This list comprises the following parameters:

- Blocked information-packet: contains the header data of the blocked packet.
- Number of attempts.

To enhance security, the data, including the blocking data, is encrypted to maintain complete secrecy. However, traditional cryptography only offers partial solutions to this problem, allowing the controller to decide whether to migrate the data. To handle these data securely, they are encrypted. Moreover, if the controller needs to perform calculations on the data, it can be done on the encrypted data itself. The controller then transmits the encrypted result to the neighbour controller, which decrypts it and obtains the desired result in plain text. A novel cryptographic technique called homomorphic cryptography [26] provides a solution that ensures security while allowing authorized individuals to manipulate the encrypted data.

The main purpose is to protect exchange data at transfer phase level. Moreover, to protect data, symmetric encryption guarantees the better confidentiality [27]. Therefore, we used Parlier’s cryptosystem [28] for encryption of blocking data that determine end class (migrate data or not) and to transfer them securely. It is based on an additive homomorphism. Figure 5 shows the used encrypted and exchanged message format.

- Nonce: a unique random number used to ensure non-repetition. This field is allocated 8 bits.
- ID-controller-source and ID-controller-destination: these fields represent the identification of the source and destination controllers involved in the message exchange. The controller is a network component identified by its IP address. (This field is allocated 32 bits).
- Data: contains the information being sent to the other controller (the information stored in the new-list). The data from the packet header is sent in this field. Therefore, it is allocated 120 bits.
- Class: contains a binary value of either 0 or 1. This field represents the decision to migrate the information or not.

Nonce	ID-controller-source	ID-controller-destination	Data	Class (migrate information)
-------	----------------------	---------------------------	------	-----------------------------

Figure 5. Format exchange message

### 3.2.1. Paillier cryptosystem

In our research, we propose the utilization of the Paillier cryptosystem [29] to ensure the confidentiality of information. The selection of this algorithm is based on its simplicity, fast execution time, and flexibility of implementation [30]. It can be employed in both hardware and software environments simultaneously. The algorithm is based on an additive homomorphism, which means that with only the public key and the cipher of  $m_1$  and  $m_2$ , it is possible to compute the cipher of  $m_1+m_2$ . The parameters of the Paillier Cryptosystem are presented in Table 1.

Table 1. Parameters of the Paillier Cryptosystem

Parameter	Description	Location
$p, q$	Random prime number	Source-VM
Public key generation	$N$	
Private key generation	$\phi$	
$m_1, m_2$	Cipher text (Blocking data and migration ACL rule)	
$C$	Encrypted message (Exchange message)	
$M$	Decrypted message (Exchange message)	Destination-VM

The Paillier cryptosystem is defined as follows [31], [32]:

i). Key generation:

- Select two large, independent, and random prime numbers:  $p$  and  $q$ .
- Compute the public key,  $N$ , and the private key,  $\phi$ , using (1 and 2) [14].

$$N = p * q \tag{1}$$

$$\phi = (p - 1) * (q - 1) \tag{2}$$

ii). Encryption

Let  $m$  a message to be encrypted with  $0 < m < N$ .

Let  $r$  be a random integer such that  $0 < r < N$ .

The encrypted message in the (3):

$$C = (1 + N)^m * r^N \text{ mod } N^2 \tag{3}$$

### 3.2.2. Analysis of information

To make the information shared in the network accessible and comprehensible to healthcare professionals, we employ the same cryptographic system as the paillier algorithm during the decryption phase. Decryption: to find the plain text  $m$ ; to ascertain the plain text  $m$ :

$$c = r^N \text{ mod } N$$

hence, we obtain:

$$r = C^{N-1 \text{ mod } \phi} \text{ mod } N$$

the result decrypted message corresponds with (4):

$$m = \frac{(C * r^{-N} \text{ mod } N^2) - 1}{N} \tag{4}$$

## 4. RESULTS AND DISCUSSION

During the experiments, the training inputs consist of the extracted parameters from these records, which are used to determine whether to add a new controller and classify a new VM in our architecture. i) the training input parameters employed for adding a new controller include: the number of VMs per zone and per DC, the number of firewalls per controller, the number of controllers, the zone index (we deploy 4 zones in our work), and the type of resource allocation; ii) the training input parameters for the classification of a new VM include: the RTT, the similarity service per VM, the number of VMs per controller, and the number of users connected per zone.

We evaluate our models (DT and classification) using ML techniques. The evaluation of the prediction models involves calculating true positive (TP), false positive (FP), true negative (TN), false negative (FN), precision, and accuracy [33], [34] where: TP: represents the accurate identification of data. It indicates that the predicted values match the actual values. FP: refers to misidentified data. TN: corresponds to correctly rejected data. FN: corresponds to incorrectly rejected data. Accuracy is calculated using (5).

$$Accuracy = \frac{(TP+TN)}{TP+TN+FP+FN} \tag{5}$$

In this section, our focus is on the results of the confusion matrix (Cm) as presented in (6). Additionally, we illustrate the accuracy (Acc) of LDA-DT for the addition of a new controller and KNN for assigning a new VM to a specific zone.

$$Cm = \begin{matrix} TP & FP \\ FN & TN \end{matrix} \tag{6}$$

Our system takes place with two phases presented previously and summarized in what follows. In the initial step: the scenario of adding a new controller:

Below are the outcomes of our dataset analysis.

- Complete training set of the classifier model.
- Algorithm utilized: DT.
- Bagging with 100 iterations and basic learner.

In the subsequent phase: the scenario of classifying a new VM:

The results of our examination of the dataset are exhibited below.

- Classifier model (complete training set).
- Algorithm used: KNN.
- Bagging with 120 iterations and basic learner.

**4.1. Integration of a new controller**

In this section, we suggest the ML LDA-DT algorithm, which is founded on the Gini coefficient. The computation of the Gini coefficient is performed in a stochastic manner, as depicted in Figure 6. Figure 6 portrays the selection of parameters during the learning process in the DT algorithm. This selection is a highly important stage in our outcome, as it decides whether to include a new controller or not. Specifically, when we encounter a non-zero Gini index, we consider other parameters in our database to arrive at the final decision.

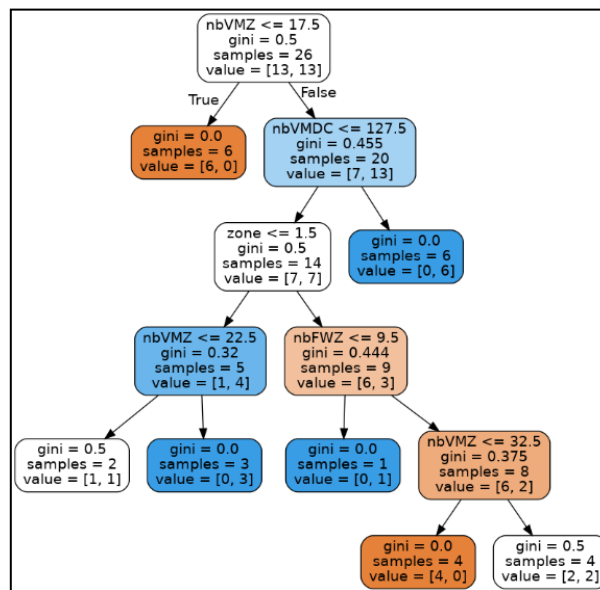


Figure 6. Selection of learning parameters based on the Gini index calculation



Figure 7 demonstrates the change in accuracy in relation to the learning rate using the LDA-DT algorithm during the process of adding a new controller. From this outcome, we observe that the algorithm achieves its maximum accuracy of 89% when the learning rate is set at 80%, confirming the effectiveness of our approach. We used DT only we found that the value ACC=0.83 and when we added LDA as a feature extraction algorithm the values of ACC are high for this, we worked by LDA-DT. This study explored an accuracy for the addition of a new controller to avoid useless addition and benefit from minimizations of network saturation.

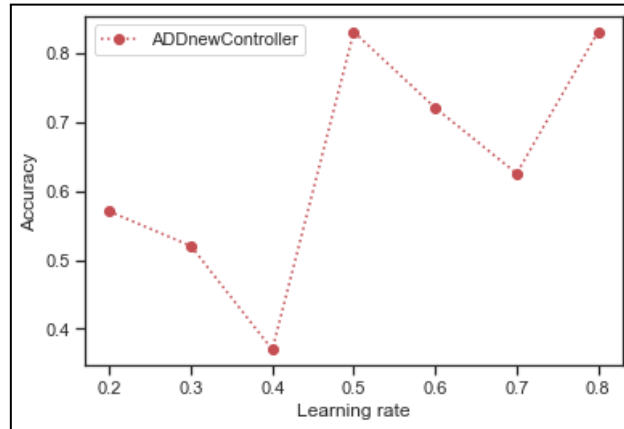


Figure 7. Variation of accuracy based on learning rate for the addition of a new controller

**4.2. Zone selection**

The distances between the VMs are calculated using KNN, which determines the zone to which a newly added zone belongs. Figure 8 presents the fluctuation in accuracy as a function of the learning rate using the KNN learning algorithm for the classification of VMs into their respective zones. Based on these outcomes, we observe that the algorithm attains its highest accuracy of 83% when the learning rate is set at 70%. According to this curve, we note that accuracy increases as the learning rate increases, thereby emphasizing the efficiency of our algorithm.

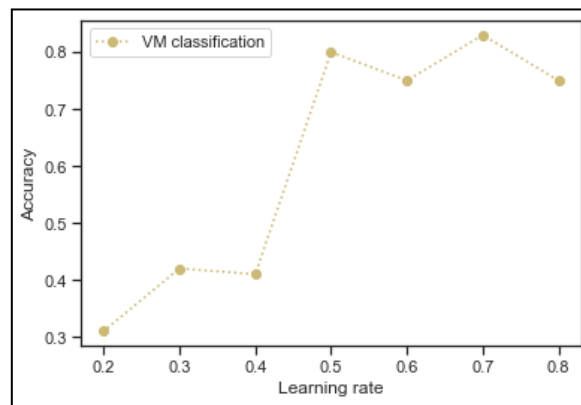


Figure 8. Variation of accuracy based on learning rate for VM classification

With a learning rate of 70%, the confusion matrix is provided as follows:

$$C_m = \begin{bmatrix} 3 & 1 & 0 \\ 2 & 3 & 0 \\ 0 & 4 & 0 \\ 1 & 0 & 0 \end{bmatrix}$$

from Cm, we have FN = 0, which represents the incorrectly rejected data, thereby demonstrating the efficiency of our algorithm and the absence of misplaced VMs. The execution time of our contribution amounts to 4.2 seconds, which is reduced compared to the work of [11]. Our proposed method can benefit in terms of execution time without having a negative impact on information security.

## 5. CONCLUSION

Our proposal is to segment the cloud architecture for healthcare applications to ensure security. This can be done by using distributed firewalls and controllers. We also studied the best location for a new VM and the need for an extra controller. Moreover, we used a homomorphic encryption algorithm to protect the data privacy among the different elements in our system. Our method includes smart and secure systems with learning and processing abilities. Recent observations suggest that manipulating the location of VMs and new controllers to best accuracy with low execution time. The simulation results show that our program effectively preserves data security. We achieved a maximum accuracy of 83% by using the LDA-DT algorithm. Likewise, the KNN algorithm gave a maximum accuracy of 89% with a NULL value for FN. We found that using distributed firewalls and adding VMs and controllers in their locations minimizes cloud network overload and we used Pailler cryptography method to increase the level of security. The method proposed in this study have a significantly higher proportion of handling new controller additions and putting a new VM into their slots compared to using traditional firewalls. Future studies could explore more security in collecting patient information with feasible means such as using the KALMAN filter to produce reduced noise from network hardware interference. We also intend to investigate other learning algorithms to improve the overall performance of our solution.




## REFERENCES

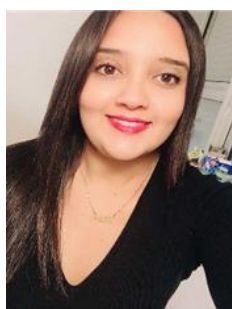
- [1] L. Sun, X. Jiang, H. Ren, and Y. Guo, "Edge-cloud computing and artificial intelligence in internet of medical things: architecture, technology and application," *IEEE Access*, vol. 8, pp. 101079–101092, 2020, doi: 10.1109/ACCESS.2020.2997831.
- [2] S. Pearson and A. Benameur, "Privacy, security and trust issues arising from cloud computing," in *2010 IEEE Second International Conference on Cloud Computing Technology and Science*, IEEE, Nov. 2010, pp. 693–702. doi: 10.1109/CloudCom.2010.66.
- [3] A. D. Tudosi, D. G. Balan, and A. D. Potorač, "Secure network architecture based on distributed firewalls," in *2022 International Conference on Development and Application Systems (DAS)*, IEEE, May 2022, pp. 85–90. doi: 10.1109/DAS54948.2022.9786092.
- [4] E. P. da Costa-Júnior, S. T. Medeiros, C. E. da Silva, and M. Madruga, "An architecture for self-adaptive distributed firewall," in *Anais do XVI Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSEG 2016)*, Sociedade Brasileira de Computação - SBC, Nov. 2016, pp. 338–351. doi: 10.5753/sbseg.2016.19318.
- [5] S. Ioannidis, A. D. Keromytis, S. M. Bellovin, and J. M. Smith, "Implementing a distributed firewall," in *Proceedings of the 7th ACM conference on Computer and Communications Security*, New York, NY, USA: ACM, Nov. 2000, pp. 190–199. doi: 10.1145/352600.353052.
- [6] J. Granados, H. Chu, Z. Zou, and L.-R. Zheng, "Towards workload-balanced, live deep learning analytics for confidentiality-aware IoT medical Platforms," in *2019 IEEE International Conference on Artificial Intelligence Circuits and Systems (AICAS)*, IEEE, Mar. 2019, pp. 62–66. doi: 10.1109/AICAS.2019.8771558.
- [7] R. Cao, Z. Tang, C. Liu, and B. Veeravalli, "A scalable multicloud storage architecture for cloud-supported medical internet of things," *IEEE Internet of Things Journal*, vol. 7, no. 3, pp. 1641–1654, Mar. 2020, doi: 10.1109/IIOT.2019.2946296.
- [8] P. Asghari, A. M. Rahmani, and H. Haj Seyyed Javadi, "A medical monitoring scheme and health-medical service composition model in cloud-based IoT platform," *Transactions on Emerging Telecommunications Technologies*, vol. 30, no. 6, Jun. 2019, doi: 10.1002/ett.3637.
- [9] A. Lakhani, Q.-U.-A. Mastoi, M. Elhoseny, M. S. Memon, and M. A. Mohammed, "Deep neural network-based application partitioning and scheduling for hospitals and medical enterprises using IoT assisted mobile fog cloud," *Enterprise Information Systems*, vol. 16, no. 7, Jul. 2022, doi: 10.1080/17517575.2021.1883122.
- [10] N. Chamas, F. Lopez-Pires, and B. Baran, "Two-phase virtual machine placement algorithms for cloud computing: an experimental evaluation under uncertainty," in *2017 XLIII Latin American Computer Conference (CLEI)*, IEEE, Sep. 2017, pp. 1–10. doi: 10.1109/CLEI.2017.8226393.
- [11] T. P. Shabeera, S. D. Madhu Kumar, S. M. Salam, and K. M. Krishnan, "Optimizing VM allocation and data placement for data-intensive applications in cloud using ACO metaheuristic algorithm," *Engineering Science and Technology, an International Journal*, vol. 20, no. 2, pp. 616–628, Apr. 2017, doi: 10.1016/j.jestch.2016.11.006.
- [12] A. Abdelaziz, M. Elhoseny, A. S. Salama, and A. M. Riad, "A machine learning model for improving healthcare services on cloud computing environment," *Measurement*, vol. 119, pp. 117–128, Apr. 2018, doi: 10.1016/j.measurement.2018.01.022.
- [13] R. Mukherjee *et al.*, "IoT-cloud based healthcare model for COVID-19 detection: an enhanced k-Nearest Neighbour classifier based approach," *Computing*, vol. 105, no. 4, pp. 849–869, Apr. 2023, doi: 10.1007/s00607-021-00951-9.
- [14] R. Zagrouba and R. Al-Hajri, "Machine learning based attacks detection and countermeasures in IoT," *International Journal of Communication Networks and Information Security (IJCNIS)*, vol. 13, no. 2, Apr. 2022, doi: 10.17762/ijcnis.v13i2.4943.
- [15] S. Rajasoundaran *et al.*, "Machine learning based deep job exploration and secure transactions in virtual private cloud systems," *Computers & Security*, vol. 109, p. 102379, Oct. 2021, doi: 10.1016/j.cose.2021.102379.
- [16] N. Jayashri and K. Kalaiselvi, "Cloud cryptography for cloud data analytics in IoT," in *Machine Learning Approach for Cloud Data Analytics in IoT*, Wiley, 2021, pp. 119–142. doi: 10.1002/9781119785873.ch6.




- [17] M. K. Oudah, M. Q. Sulttan, and S. W. Shneen, "Fuzzy type 1 PID controllers design for TCP/AQM wireless networks," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 21, no. 1, p. 118, Jan. 2021, doi: 10.11591/ijeecs.v21.i1.pp118-127.
- [18] D. Dikii, S. Arustamov, and A. Grishentsev, "DoS attacks detection in MQTT networks," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 21, no. 1, p. 601, Jan. 2021, doi: 10.11591/ijeecs.v21.i1.pp601-608.
- [19] F. Kamoun-Abid, A. Meddeb-Makhlouf, F. Zarai, and Guizani, "Distributed and cooperative firewall/controller in cloud environments," in *Proceedings of the 13th International Conference on Availability, Reliability and Security*, New York, NY, USA: ACM, Aug. 2018, pp. 1–10. doi: 10.1145/3230833.3230857.
- [20] J. Zhou and A. Sengupta, "Context-aware distributed firewall," *U.S. Patent No. 9. P 692-727*, 27 Jun. 2017.
- [21] R. M. Hicks, *Implementing Always On VPN*. Berkeley, CA: Apress, 2022. doi: 10.1007/978-1-4842-7741-6.
- [22] K. Sha, T. A. Yang, W. Wei, and S. Davari, "A survey of edge computing-based designs for IoT security," *Digital Communications and Networks*, vol. 6, no. 2, pp. 195–202, May 2020, doi: 10.1016/j.dcan.2019.08.006.
- [23] E. E. D. Hemdan, W. El-Shafai, and A. Sayed, "CR19: a framework for preliminary detection of COVID-19 in cough audio signals using machine learning algorithms for automated medical diagnosis applications," *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, no. 9, pp. 11715–11727, 2023, doi: 10.1007/s12652-022-03732-0.
- [24] A. A. Soofi and A. Awan, "Classification techniques in machine learning: applications and issues," *Journal of Basic & Applied Sciences*, vol. 13, pp. 459–465, Jan. 2017, doi: 10.6000/1927-5129.2017.13.76.
- [25] O. Kherif, Y. Benmahamed, M. Tegar, A. Boubakeur, and S. S. M. Ghoneim, "Accuracy improvement of power transformer faults diagnostic using KNN classifier with decision tree principle," *IEEE Access*, vol. 9, pp. 81693–81701, 2021, doi: 10.1109/ACCESS.2021.3086135.
- [26] N. Patel, P. Oza, and S. Agrawal, "Homomorphic cryptography and its applications in various domains," in *Lecture Notes in Networks and Systems*, vol. 55, 2019, pp. 269–278. doi: 10.1007/978-981-13-2324-9\_27.
- [27] S. Belguith, A. Jemai, and R. Attia, "Enhancing data security in cloud computing using a lightweight cryptographic algorithm," *11th International Conference on Autonomic and Autonomous Systems*, pp. 98–103, 2015.
- [28] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Advances in Cryptology — EUROCRYPT '99*, vol. 1592, Berlin, Heidelberg: Springer Berlin Heidelberg, 1999, pp. 223–238. doi: 10.1007/3-540-48910-X\_16.
- [29] N. Fazio, R. Gennaro, T. Jafarikhah, and W. E. Skeith, "Homomorphic secret sharing from paillier encryption," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 10592 LNCS, 2017, pp. 381–399. doi: 10.1007/978-3-319-68637-0\_23.
- [30] K. El Makkaoui, A. Ezzati, and A. Beni-Hssane, "Securely adapt a paillier encryption scheme to protect the data confidentiality in the cloud environment," in *ACM International Conference Proceeding Series*, New York, NY, USA: ACM, Nov. 2016, pp. 1–3. doi: 10.1145/3010089.3016026.
- [31] Michael O'Keefe, "The paillier cryptosystem," Mathematics Department April 18, 2008, P1-16.
- [32] T. Sridokmai and S. Prakancharoen, "The homomorphic other property of Paillier cryptosystem," in *Proceedings 2015 International Conference on Science and Technology, TICST 2015*, IEEE, Nov. 2015, pp. 356–359. doi: 10.1109/TICST.2015.7369385.
- [33] M. Grandini, E. Bagli, and G. Visani, "Metrics for multi-class classification: an overview," Aug. 2020, [Online]. Available: <http://arxiv.org/abs/2008.05756>
- [34] F. Hounaida, O. Fokapu, C.-A. Larbi, M. M. Amel, and Z. Faouzi, "ST-based deep learning analysis of COVID-19 patients," *International Journal of Biology and Biomedical Engineering*, vol. 16, pp. 321–329, Jul. 2022, doi: 10.46300/91011.2022.16.39.

## BIOGRAPHIES OF AUTHORS






**Ferdaous Kamoun-Abid**    received her engineering diploma in telecommunications from the National School of Electronic and Telecommunications, University of Sfax, Sfax, Tunisia in 2016. She is currently a doctor degree in Computer Systems Engineering at the National Engineering School of Sfax. She is a member of the NTS'COM research unit. Her research interests are in fields of security of cloud computing. Affiliations: NTS'Com Research Unit, ENET'COM, University of Sfax, Tunisia. She can be contacted at email: [abidkamounferdaous@gmail.com](mailto:abidkamounferdaous@gmail.com).






**Hounaida Frikha**    she is currently a Ph.D. student in Information and Communication Science and Technologies at the National School of Electronics and Telecommunications of Sfax. She is a member of the NTS'COM research unit. She works as a research engineer at the University of Polytechnique Hauts de France. She is the coordinator of courses and programs of excellence in the European alliance EUNICE. His research interests include the areas of wireless medical network security and COVID-19. Affiliations: NTS'Com research unit, ENET'COM, University of Sfax, Tunisia. She can be contacted at email: [frikhahounaida95@gmail.com](mailto:frikhahounaida95@gmail.com).



**Amel Meddeb-Makhoulf**    is currently a post-doctoral fellow at the high school of engineering in electronics and communications (ENET'COM), Sfax, Tunisia. She received the engineering degree (in 2001), the master degree in communications (in 2003), and the Ph.D. degree (2010) from the Engineering School of Communications (SUP'COM, Tunisia). From September 2001 to August 2004, she worked as a project chief of the certification unit in NDCA (National Digital Certification Authority), the root certification authority in Tunisia, where she participates to the establishment of the Tunisian public key infrastructure. She also collaborates in the security audit projects. From September 2004 to September 2010, she worked as a teacher assistant in telecommunications in the Engineering School of Communications (SUP'COM, TUNISIA), where she teaches security courses and supervised Engineer projects. Since September 2010, she works as an assistant professor in the Engineering School of Electronics and Telecommunications of Sfax (ENET'COM). She is a member of NTS'COM Laboratory in ENET'COM. Her research interests are in the area of network security with special emphasis on security of vehicular networks, security of cloud networks, authentication protocols and security of Body Sensor networks. Affiliations: NTS'Com research unit, ENET'COM, University of Sfax, Tunisia. She can be contacted at email: [amel.makhlouf@enetcom.usf.tn](mailto:amel.makhlouf@enetcom.usf.tn).



**Faouzi Zarai**    received the Engineering Diploma, Master Diploma, and Ph.D. in Information and Communication Technologies from the Engineering School of Communications (Sup'Com, Tunisia) in 2002, 2003, and 2007; respectively. He is also recipient of the habilitation degree in 2011. From 2002 to 2005 he has worked for the national digital certification agency (NDCA, Tunisia). Since 2011, he serves on the editorial boards of the International Journal of Communication Systems. He published one book and 5 chapters and co-authored more than 80 papers that have been published in international journals and conferences. Currently, Dr. Zarai is serving as an associate professor for the National School of Electronic and Telecommunications Sfax (ENET'COM). From 2008 to 2014, he has the Head of the Department of telecommunications at ENET'COM. Since 2016, he is Director of the research unit of news Technologies and Telecommunications Systems (NTS'COM). He is conducting research activities in the areas of security and Quality of services in news generations wireless networks LTE-Advanced PRO: authentication, IP taceback, seamless mobility, congestion control, admission control, and radio resource management. Affiliations: NTS'Com research unit, ENET'COM, University of Sfax, Tunisia, He can be contacted at email: [faouzifbz@gmail.com](mailto:faouzifbz@gmail.com).