PROMOTING THE SECURITY OF CLOUD COMPUTING USING HYBRID FRAMEWORKS LAYER INTRUSION DETECTION AND NEURAL NETWORK

SEYED HASAN MORTAZAVI ZARCH[1]*
Department of Computer Engineering, Faculty of Engineering, Meybod University, Meybod, Iran
hassanmortazavi@meybod.ac.ir

FARHAD JALILZADEH[2]
System administrator, Gk Software, Schoneck\Vogtland, Germany
Farhad.jalilzadeh2006@gmail.com

AHMAD HAJI SAFARI[3]
Department of Electrical Engineering, Faculty of Imam Ali, Yazd Branch, TVU, Yazd, Iran
Safari_1372@yahoo.com

MOHAMMAD HAMEDJAHEDI[4]
Network systems manager of government trading corporation of Iran
mhjahedi@gmail.com

Abstract - In this paper, cloud computing security is enhanced by the use of the intrusion detection framework and the neural network. In order to handle access to traffic in a large network and control data and applications in cloud computing, an impressive framework called the Layer Intrusion Detection Framework that can be used on different layers and classes of cloud computing can be used. You can identify the presence of normal traffic among cloud traffic. The artificial neural network data mining framework has also been used to increase accuracy and speed. Layer Intrusion Detection Framework can reduce the amount of traffic that has been analyzed and increase performance to better performance. So far, much research has been done to increase the accuracy of finding malicious traffic, which, given the limitations available, still has trouble finding these malicious traffic. In this research, we first tried to use real-time network traffic monitoring to use the network monitoring module to monitor traffic and then use the seventy extraction features of various traffic and neural networks to solve the problem and the classification was made. In this framework, in addition to the real-time monitoring of existing traffic using network monitoring software, seventeen features have been used, two of which have been used for the first time, which increase the security of cloud computing and prevent the intrusion of distractors.

Keywords: Intrusion Detection System, Cloud Computing, Neural Network.

1. Introduction

In recent years, cloud computing has become an important technology in the field of information technology. Experts in this field believe that cloud computing will transform processes in the field of information technology. The primary goal of cloud computing technology is to enable access to a huge amount of computing resources in virtualization. This work is done using aggregation of resources and creating an integrated system. In this model of computational services, the cost is also paid by the customer based on the amount and duration of the use of resources. In a general definition, the "hardware computing" and "hardware computing" datacenters are called cloud computing. Cloud computing is a new process of processing, in which distributed resources, often virtualized, are delivered as a processing service through communication networks such as local and Internet. The core of this model is service to the user on demand, without the user having to know the specific processing equipment or the location of the processing [1][2][3]. The service can be likened to a power grid that provides the energy needed to use its electrical equipment without knowing how to generate electricity and the exact location of its production, and only by connecting it through a port. Cloud computing is defined as an Internet-based computer through which shared resources, software and information are provided for computers and other services on request. The use of computational resources or custom services for consumers from cloud computing providers is robust and efficient. Cloud computing is more recent than other computational services, which is due to the unlimited capacity of resources. In addition, consumers can use the services wherever they have access. So cloud computing is unique in terms of accessibility. Cloud computing

systems contain many resources and personal information, so they are easily threatened by attackers. In particular, system administrators who potentially could be in the position of an attacker, is essential for cloud computing systems to be secured against internal and external attackers [4][5][6][7].

2. Research Methods

Cloud computing is referred to as a distributed and parallel system that includes a set of virtual computers connected to each other. These computers are dynamically presented as one or more integrated computing resources based on service level agreements, and these agreements are established during negotiations between service providers and consumers. Cloud Computing tries to dynamically create a new generation of data centers by providing services and services in virtualized networked virtual machines in such a way that users can access apps from anywhere in the world. Cloud computing is a modern service that provides large-scale computing resources to every consumer [8][9][10]. Cloud computing systems are easily threatened by various cybercrime attacks, as most cloud computing systems provide services to many who are unclear whether they are trusted. Therefore, a cloud computing system should include multiple Intrusion Detection (IDS) and (IDPS) systems to protect each virtual machine (VM) against threats. In this case, there is a relationship between the level of IDS security and system performance. The more the IDS provide a stronger security service through more rules and patterns, and then it needs more resources than security power. Therefore, the amount of resources left to consumers is reduced. Another problem with cloud computing is that high logging rates makes logins more difficult for system administrators. In the current era of the Internet, the use of cloud computing has created a huge amount of online financial transactions and the exchange of personal and sensitive information through the Internet [11][12]. The Internet-driven pursuit of curiosity or financial mismanagement will lead to various types of malware. In This paper presents an effective framework called the Layer Intrusion Detection Framework that can be used on various cloud computing layers and classes, which can be used to detect the presence of normal traffic through transmitted cloud traffic. The proposed framework uses the data mining operation, especially the data mining of an artificial neural network, to make it accurate, fast, and scalable. The layered intrusion detection system, meanwhile, can reduce the amount of traffic that has been analyzed and increase performance without affecting the main purpose. In this paper, we first tried to use real-time network traffic monitoring to use the network monitoring module to monitor traffic online and then use seventy extraction features of various traffic and neural networks of the class problem made a statement. In this framework, in addition to monitoring real-time traffic monitoring using network monitoring software, seventeen features are used, with two of the seventeen features being used for the first time. The LIDF uses an artificial neural network data mining and reduces the amount of network analyzer traffic and increases its performance by increasing its operational capability without affecting the main goal, which is an incremental framework for filtering traffic it is used to enhance the detection process and refine the next layer. The main objectives of this research are to increase security and reduce the error in the cloud penetration detection system, which aims to achieve the correct traffic volume. Both malicious and non-destructive traffic, as well as increased traffic sensitivity, will be followed.

2.1. Proposed algorithms

The proposed algorithm achieves the desired accuracy by adding two attributes. The desired features are related to the size of the package, which according to the articles and previous work has been obtained, and by combining this feature with the previous features, the final features of the new framework were obtained. The two features added to the previous features are the variance associated with the length of the packets that, due to the significant change in the length of packets sent by the attacker, the traffic associated with malicious packages has more variance than non-destructive traffic, and therefore the variance characteristic as well The new feature has been added to the framework, and the middle of the packet length is due to the fact that the packets in a malicious traffic are far more moderate. Therefore, this feature is also used as a new feature. These two features are as feature 16 and 17 in the following feature_extraction.m file.

```
%% new features
%16'th feature; variance of every chunk length
for i = 0:burst_number-1
   packet_array = zeros(chunk_length,1);
   for j = 1:chunk_length
      packet_array(j,1) = str2double(info{i*chunk_length+j,4});
   end
   features(i+1,16) = var(packet_array);
end
%% 17'th feature; median of chunk length
for i = 0:burst_number-1
   packet_array = zeros(chunk_length,1);
   for j = 1:chunk_length
      packet_array(j,1) = str2double(info{i*chunk_length+j,4});
   end
   features(i+1,17) = median(packet_array);
end
```

The output of the above code is shown in Figure 1.

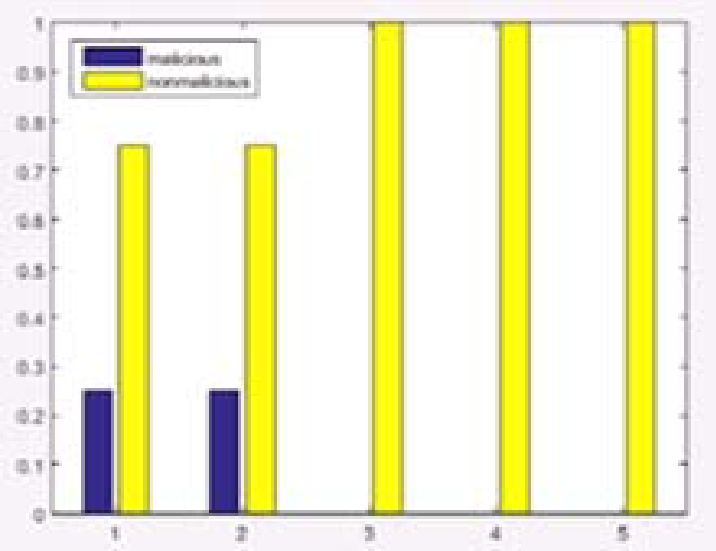

Fig. 1. This is the out-put of feature_extraction.m file

2.2. Checking the Criteria

Now we review and compare these three frameworks in three different criteria. The description of the symbols concerned is as follows:

TP: The number of destructive malware on the glued.

FP: The number of non-destructive phrases that are malware detected.

FN: The number of malicious traffic that is detected.

TN: The number of non-destructive traffic.

2.2.1. True

The following is true:

$$\text{Precision} = \text{TP} / (\text{TP} + \text{FP}) \quad (1)$$

This relationship actually gains the number of malicious badge-labels that are detected by the total number of malicious tags (both true and false). This ratio actually quantifies how much malicious traffic has been detected. In seven consecutive tests, the proposed method works with a feature that is better than the usual one. The proposed method with or without proposed features is far better than the usual method. Observations show that the use of these two features increases up to 8 percent accuracy than the one that does not use these two features. This is despite the fact that the correctness of this method has risen to the correctness of the usual method by up to 35% in the case of having a feature.

2.2.2. Sensitively

Sensitivity or sensitivity is obtained from:

$$\text{sensitively} = \text{TP} / (\text{TP} + \text{FN}) \quad (2)$$

This relationship actually shows that the framework outlined a few percent of the maliciously crafted traffic.

Given that the traffic is intended to test domestic traffic, it has fewer attacks than traffic in which the attack is.In this section, although the framework is worse than the usual framework, it's 7% worse, but because this traffic is related to home traffic, it does not have a significant effect on the framework's performance. If some packages are not filtered, there is no problem with the system. On the other hand, the framework can be used to resolve this problem without adding two additional features, which only gives one percent less sensitivity than the full 100% sensitivity of the original framework. Therefore, the proposed framework in this section also has a favorable outcome. What matters to the framework is how well our total framework works to find and filter as a whole.

2.2.3. Accuracy

Accuracy to the general form is obtained as follows:

$$\text{Accuracy} = (\text{TP} + \text{TN}) / (\text{TP} + \text{FN} + \text{TN} + \text{FP}) \quad (3)$$

In general, the relationship above explains how well our framework recognizes packets (whether destructive or non-destructive). In the most important benchmark of the framework, with two added features, 2% better than the proposed framework without these two features and 6% better than the usual framework. So overall, it has been able to increase the accuracy of packet detection accuracy by 6%.

2.2.4. F-measure

The final criterion we will discuss is the F-measure. This criterion is obtained from the following equation:

$$\text{F} - \text{measure} = (2 * \text{precision} * \text{recall}) / (\text{precision} + \text{recall}) \quad (4)$$

This criterion is a good criterion, which has less dependence on the percentage and number of tagged data. In this criterion, our framework is much better than the previous framework. The frameworks have been carefully considered with two added attributes as high as 21%, while when more features are used, accuracy has improved by one percent and reached 93% to 94%.

3. Comparison of proposed method

The precision considered in the proposed method is obtained according to Table 1:

Table 1. Comparison of method.

Precision (%)	Sensitivity (%)	Accuracy (%)	F-measure	
96	95	96	97	First round
99	99	99	99	Second round
98	99	96	97	Third round
96	85	95	96	Fourth round
96	85	99	99	Fifth round
98	99	96	97	Sixth round
96	97	96	97	Seven round

After adding these features as a new feature, once again the accuracy was calculated for the desired framework. To do this, the frameworks were compared with each other in four criteria: accuracy, sensitivity, accuracy, and F-measure. Here, 2 frameworks were compared with the proposed framework. Now, we will review the comparison of these three frameworks in three different criteria. Note that the description of the symbols concerned is as follows:

TP: The number of malicious traffic labels tagged.

FP: The number of non-destructive phrases that are malware detected.

FN: The number of malicious traffic that is detected.

TN: The number of non-destructive traffic.

4. Comparison of the precision methods with the proposed method

The comparison of this criterion is shown in Figure 2.

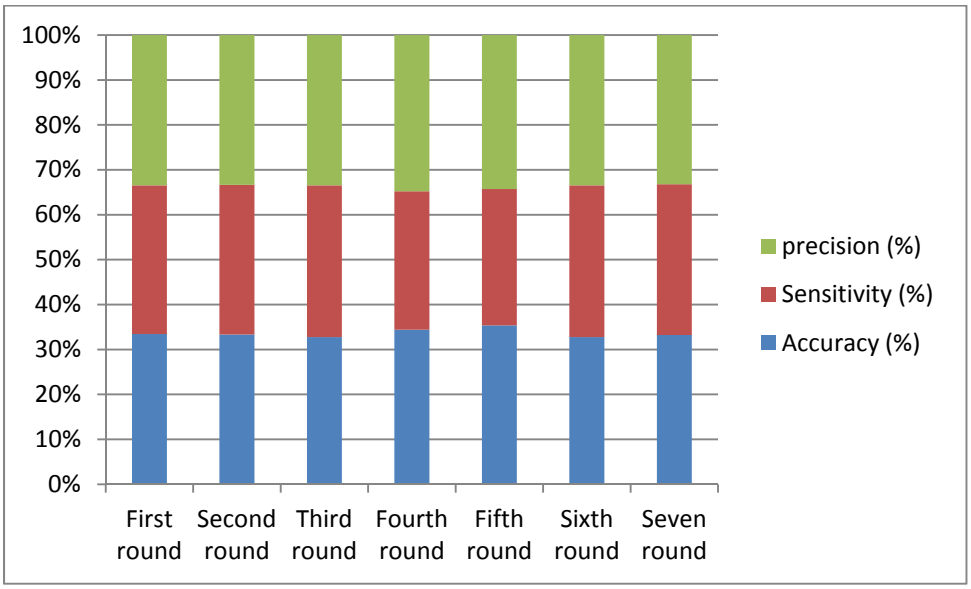

Fig.2.Comparison of the precision methods

As shown in the chart above, the blue column belongs to the proposed framework, the red pillar of the proposed framework without two proposed features, and the gray pillar represents the state of the art method, or indeed the best available method for the diagnosis provided in is [5].As seen in seven successive experiments, the proposed method works with features that are better than the usual method, and as shown in the last column, the proposed method with or without the proposed features is far better than the usual one. . Also, this chart shows how far the addition of the two features is effective in improving correctness. Observations show that the use of these two features increases up to 8 percent accuracy than the one that does not use these two features. This is despite the fact that the correctness of this method has risen to the correctness of the usual method by up to 35% in the case of having a feature.

5. Comparison of the sensitivity of the methods

The comparison of the sensitivity of the method is shown in Figure 3.

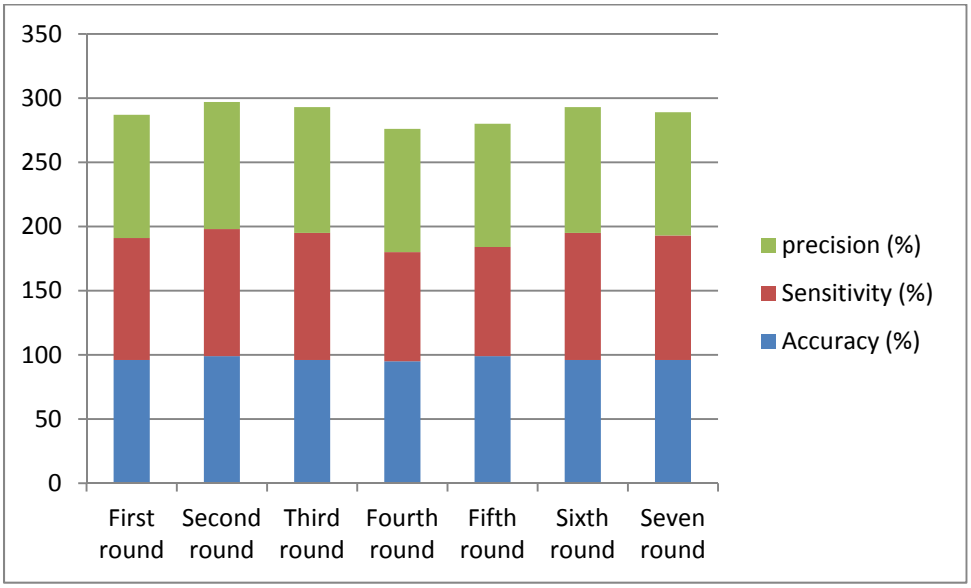

Fig. 3. Comparison of the sensitivity of the methods.

As can be seen, although the framework in this section is worse than the usual framework, it does not have much effect on the framework's performance, and the reason is, as we have said, that traffic is traffic-related. There is no problem with the system if some packages are not filtered. On the other hand, the framework can be used to eliminate this problem without adding two features, which only gives one percent worse sensitivity than the full 100% sensitivity of the original framework. Therefore, the proposed framework in this section also has a good result. What matters to the framework is how well our total framework works to find and filter as a whole.

6. Comparison of the accuracy of the methods

As shown in Figure 4, the most important criterion for the framework with two added attributes is 2% better than the framework provided without these features and 6% better than the usual framework. So, overall, it could increase the accuracy of packet detection accuracy by 6%.

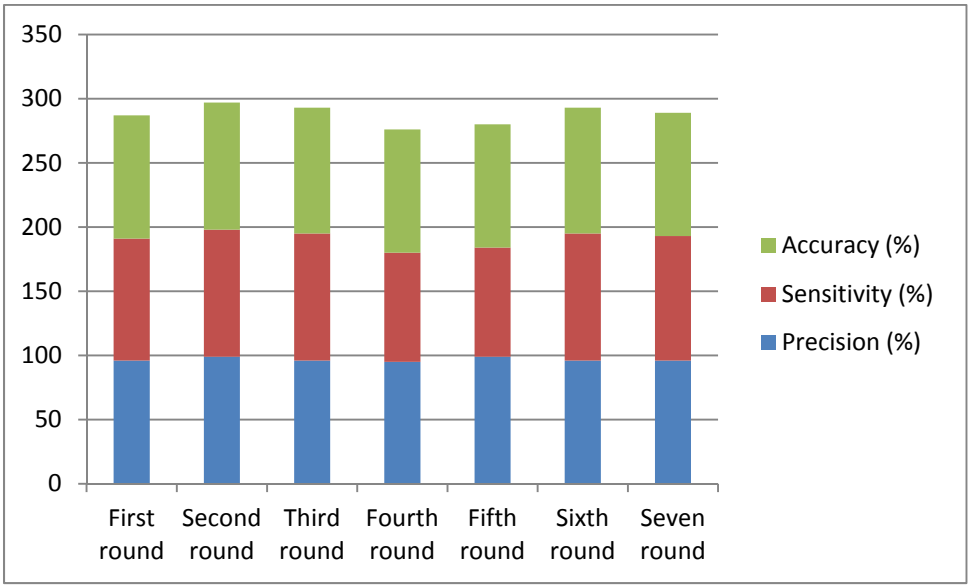

Fig. 4. Comparison of the accuracy of the methods

7. Compare F-measure

As shown in Figure 5, in this criterion, our frameworks are far better than the previous framework. The frameworks have been carefully considered with two added attributes as high as 21%, while when more features are used, accuracy has improved by one percent and reached 93% to 94%.

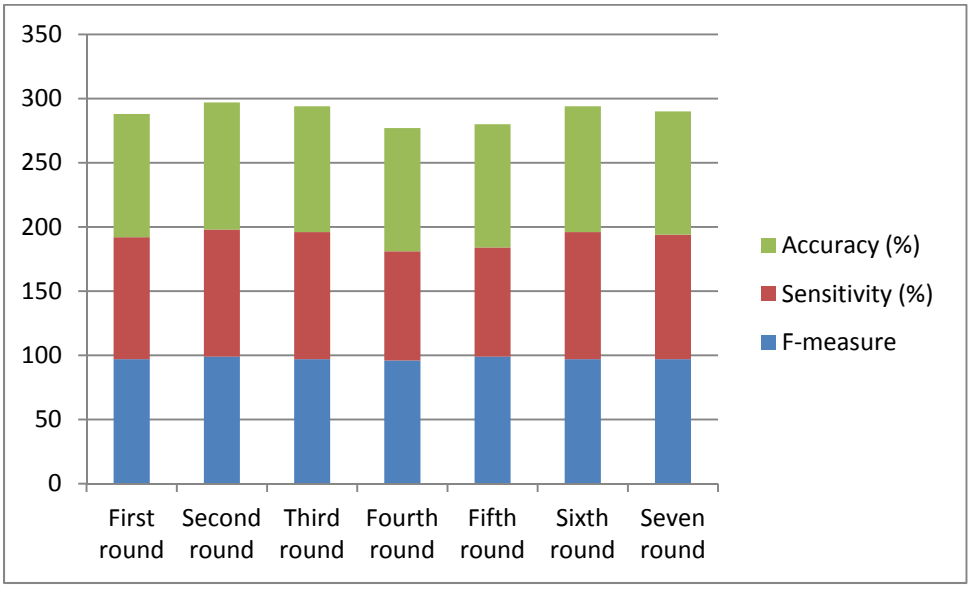

Fig. 5. Compare F-measure.

8. Conclusion

Cloud computing is a modern service that provides large-scale computing resources to every consumer. Cloud computing systems are easily threatened by various cybercrime attacks, as most cloud computing systems provide services to many who are unclear whether they are trusted. Therefore, a cloud computing system should include multiple intrusion detection systems to protect each virtual machine against threats. In this case, there is a relationship between the security level of the system's intrusion detection system and system performance. The more the system detects the nuisance, the stronger security service provided by more rules and patterns, and then needs more resources than security power. Therefore, the amount of resources left to consumers is reduced. Another problem with cloud computing is that the high logging rate makes it difficult to analyze logs for system administrators. The proposed method responds in different layers of cloud computing and can detect the presence of normal traffic among monitored cloud traffic. A layer intrusion detection system is used in the detection system, and it is finally determined that this method can detect the presence of normal and abnormal cases. Because of the layered structure, this method can be easily integrated and protected. Developing or upgrading this method is possible by modifying particular layers or adding a new layer. Therefore, layer intrusion detection is expected to be a long-term infiltration detection framework. The survey focuses solely on the topic of identifying the traffic mode under surveillance, without being aware of the type of penetration in the maladaptive traffic. In the future, attention can be drawn to the type of infiltration that examines the isolation of maladaptive traffic and identifies malicious activity in order to determine the type of malware within this traffic. In this paper, we try to identify and track malicious traffic using the concept of intrusion detection systems. Hence, by reviewing various articles, it was decided to use multilayer systems for this purpose. These systems initially identify the incoming traffic by extracting the effective features of malicious and non-destructive traffic detection and then categorizing traffic by using different classifications. In the framework presented in this study, the traffic logic software was first introduced to the system by input traffic to the system, and then, and for the first time, this traffic is given to the system in real time. After traffic is captured, traffic features are extracted according to previous work.

References

[1] Jun- Ho Lee, Min-Woo Park, Jung-Ho Eom, Tai-Myoung Chunge, " Multi-level Intrution Detection System and Log Management in Cloud Computing", Dept of Information Communication Engineering, Sungkyunkwan University, 2011.
[2] Nouf Saleh Aljurayban, Ahmed Emam, "Framework for Cloud Intrusion Detection System Service" Information System Department College of Computer and Information Sciences King Saud University, Riyadh, Saudi Arabia, 2015
[3] Mr. Rupesh R Bobde, Prof. Amit Khaparde, Prof. Dr.M. M. Raghuwanshi, "An Approach For Securing Data On Cloud Using Data Slicing And Cryptography" , IEEE Sponsored 9th International Conference on Intelligent Systems and Control (ISCO)2015.
[4] Kleber Vieira, Alexandre Schulter, Carlos Becker Westphall, Carla Merkle Westphall, "Intrusion Detection for Grid and Cloud Computing", IT Pro July/August 2010
[5] Jens Lindemann, "Towards Abuse Detection and Prevention in IaaS Cloud Computing", 2015 10th International Conference on Availability, Reliability and Security
[6] Chi-Chun Lo, Chun-Chieh Huang, Joy Ku, "A Cooperative Intrusion Detection System Framework for Cloud Computing Networks" , 2010 39th International Conference on Parallel Processing Workshops.
[7] [10] Manish Kumar, Dr. M. Hanumanthappa, "Scalable Intrusion Detection Systems Log Analysis using Cloud Computing Infrastructure", Bangalore University, Bangalore, INDIA, 2013.
[8] Lohit Kapoor; Archana Pandita; Preeti Rajput," Neural network based optimal placement strategy for service components in cloud computing," 2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA).
[9] Salim Malek; Farid Melgani; Yakoub Bazi; Naif Alajlan," Reconstructing Cloud-Contaminated Multispectral Images With Contextualized Autoencoder Neural Networks", IEEE Transactions on Geoscience and Remote Sensing,2017.
[10] Aleksandr Savchenkov; Andrew Davis; Xuan Zhao," Generalized Convolutional Neural Networks for Point Cloud Data", 2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA).
[11] W. Yassin, N.I. Udzir, Z. Muda, A. Abdullah, M.T. Abdullah, "A Cloud-Based Intrusion Detection Service Framework", Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor Darul Ehsan, Malaysia,2012.
[12] Gonzalo Mateo-García; Luis Gómez-Chova; Gustau Camps-Valls", Convolutional neural networks for multispectral image cloud masking", 2017 IEEE International Geoscience and Remote Sensing Symposium (IGARSS).