

# SYN Flood Attack Detection in Cloud Computing using Support Vector Machine

Zerina Mašetić<sup>1</sup>, Dino Kečo<sup>1</sup>, Nejdet Dođru<sup>1</sup>, Kemal Hajdarević<sup>2</sup>

<sup>1</sup>International Burch University, Francuske revolucije bb, Sarajevo, Bosnia and Herzegovina

<sup>2</sup>Faculty of Electrical Engineering, University of Sarajevo, Zmaja od Bosne bb, Sarajevo, Bosnia and Herzegovina

**Abstract** – Cloud computing is a trending technology, as it reduces the cost of running a business. However, many companies are skeptic moving about towards cloud due to the security concerns. Based on the Cloud Security Alliance report, Denial of Service (DoS) attacks are among top 12 attacks in the cloud computing. Therefore, it is important to develop a mechanism for detection and prevention of these attacks. The aim of this paper is to evaluate Support Vector Machine (SVM) algorithm in creating the model for classification of DoS attacks and normal network behaviors. The study was performed in several phases: a) attack simulation, b) data collection, c) feature selection, and d) classification. The proposed model achieved 100% classification accuracy with true positive rate (TPR) of 100%. SVM showed outstanding performance in DoS attack detection and proves that it serves as a valuable asset in the network security area.

**Keywords** – Cloud computing, SYN flood, DoS attack, Support Vector Machine.

---

DOI: 10.18421/TEM64-15


<https://dx.doi.org/10.18421/TEM64-15>

**Corresponding author:** Zerina Mašetić,  
International Burch University, Francuske revolucije  
bb, Sarajevo, Bosnia and Herzegovina  
**Email:** [zerina.masetic@ibu.edu.ba](mailto:zerina.masetic@ibu.edu.ba)

Received: 09 September 2017

Accepted: 30 October 2017

Published: 27 November 2017

 © 2017 Zerina Mašetić et al; published by UIKTEN. This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 3.0 License.

The article is published with Open Access at [www.temjournal.com](http://www.temjournal.com)

## 1. Introduction

Cloud computing is a technology that delivers IT resources and applications as a service, over the Internet, with pay-as-you-go pricing. It consists of a number of individual computing nodes with corresponding networking and storage subsystems [1]. This service - based thinking has changed the way in which technology departments deliver computing technology and applications, i.e. more efficiently [2].

Since security is the essential part of every system, it is important to keep the integrity of the data being kept in the cloud and to ensure safe access to cloud resources. However, advancements in technology have created new and amplified existing security issues and risks in the cloud. Some of the malicious activities that have occurred in the cloud computing since October 2012 are [3]:

- Exposure of VMware source code
- Distributed Denial of Service (DDoS) attack on the DigitalOcean, cloud hosting service provider
- Attacking Software as a Service (SaaS) and Platform as a Service (PaaS) infrastructure with Trojan Zeus
- Accessing Amazon Elastic Compute Cloud (EC2) and deleting the customer database and most backups by an attacker
- DDoS attacks using Amazon Cloud Services

Denial of Service (DoS) attack is a type of an attack where attacker prevents a legitimate user from accessing some information and services. The most common DoS attack is when attacker “floods” a network, sending too many requests to a specific web server at once. This action prevents legitimate users accessing a website, as the server can process only a certain number of requests at the time [4]. In a distributed denial-of-service (DDoS) attack, attacker uses more computers, which are geographically distributed, to launch the attack [4].

Additionally, Cloud Security Alliance (CSA), a not-for-profit organization that promotes the use of best practices to provide security assurance within cloud computing [5], issued a report for 2016, identifying top 12 cloud computing threats [2], conducting a survey of industry experts based on their cloud security issues and opinion. This report serves as a guide to cloud user and cloud vendors, and can help them in making right decisions about risk management within a cloud. Furthermore, it focuses on threats that are specifically related to the shared, on-demand nature of the cloud computing. Threat analysis was conducted by CSA experts, considering survey results, and STRIDE Threat Model [6] and NIST Risk Management Framework [7], for successfully managing information technology risk. Based on their research, among the others, such as data breaches, malicious insiders, and insecure interfaces and APIs are also DoS attacks [2].

Therefore, it is important to work more in the area of security and to minimize the security risk in the cloud. Furthermore, cloud service providers (CSP) need to implement strong protection system on their cloud infrastructure.

The aim of this paper is to present the cloud computing threat detection model that can help CSP protect their infrastructure from potential malware actions. More specifically, the aim is to detect potential Denial of Service (DoS) attack in the cloud computing, using Support Vector Machine (SVM) machine learning algorithm.

The rest of this paper is organized as follows: Section II outlines the review of the most cloud computing threats and solutions provided by the other authors. Section III introduces materials and methodologies we used in our experimental study. In Section IV we will present our results through a number of performance metrics. Section V introduces discussion and our contribution, and we will conclude the paper with Section VI.

## 2. Literature Review

One step in securing the cloud services from different attacks is the detection of attacks based on different parameters that describe that attack. Therefore, developing and implementing a protection system in the cloud is crucial.

An approach taken for developing a detection system is the application of machine learning algorithms. Khorshed, Ali and Wasimi [8] proposed a classification model based on the performance data, such as CPU, memory, disk and network usage from the hypervisor and guest operating system, for DoS attack detection. For the classification, authors used C4.5 algorithm and obtained 93.47%

classification accuracy. Khorshed et al. [9] integrated three layers: Internet of Things (IoT), Cloud Computing and intelligence of Big Data, and collected performance data from all three layers. Furthermore, they combined the data together and applied machine learning algorithms for detection of 18 different cyber-attacks. The best overall performance was obtained with RF algorithm, with 93.9% classification accuracy. Moreover, some of the attacks among 18 attacks are DoS attacks, specifically SYN flood, HTTP flood and ICMP flood DoS attacks on Cloud level. The authors obtained 98%, 94.5%, and 73.7% true positive (TP) rate, respectively, for correctly classifying these types of DoS attacks with RF algorithm, and 0.1% FP for all three cases. Chen et al. [10] proposed the cloud computing based network monitoring and threat detection system. In their work, they simulated Distributed Denial of Service (DDoS) attack and applied k-means clustering and Naive Bayes algorithms for attack detection on the real-world network traffic data from Chicago Equinix Data Center. Their results show that k-means clustering algorithm achieved TP rate of 90% and false (FP) rate of 0.5% and Naive Bayes algorithm achieved TP rate of 90% and 1.8% FP rate. Pandeewari and Kumar [11] proposed an anomaly detection system based on the hybrid model of Fuzzy C-Means clustering and Artificial Neural Networks (ANN) on the DARPA's KDD Cup 1999 data and compared the performance with Naive Bayes and classic ANN. The proposed classification system was developed for detecting different attacks, among which are DoS attacks. Their system achieved 99.96% accuracy, 97.2% TP and 5.33% FP rate for classifying DoS attacks. Furthermore, Amiri et al. [12] proposed a feature selection technique for intrusion detection system, based on the mutual information (MI). Additionally, they applied Least Square Support Vector Machine (LS-SVM) machine learning algorithm for KDD Cup 1999 data classification. The proposed system achieved 84.11% classification accuracy for DoS attacks, 78.69% TP rate and 0.73% FP rate, with MI feature selection algorithm. Kumar, Lal, and Sharma [13] proposed a system consisting of a packet sniffer, a feature extractor, and a classifier, for detecting different DoS attacks on VMs in the cloud. Specifically, they applied one-class Support Vector Machine (SVM) classifier on the network traffic dataset for classification of ICMP flood, Ping-of-Death, UDP flood, SYN flood, TCP land and DNS flood attacks and achieved classification accuracy of 100%, 94%, 97%, 96%, 98% and 99% respectively.

Considering the statistics shown in [3] and the report from CSA [2], DoS attacks are still one of the biggest concerns in the cloud computing. Therefore, we propose a model for DoS attack identification and

detection in the cloud computing, using SVM classifier. SVM is a method efficient to achieve an excellent performance, and it has not been applied much in previous studies.

### 3. Materials and Methods

Our proposed approach consists of several steps, shown in Fig. 1. The first step is environment setup. Furthermore, we simulated the attack generation and collected the data using network traffic capture tool Wireshark. Using the TShark, we extracted the fields from packet capture necessary for the classification. Collected data is used for the classification after the relevant features are selected using Genetic Algorithm (GA).

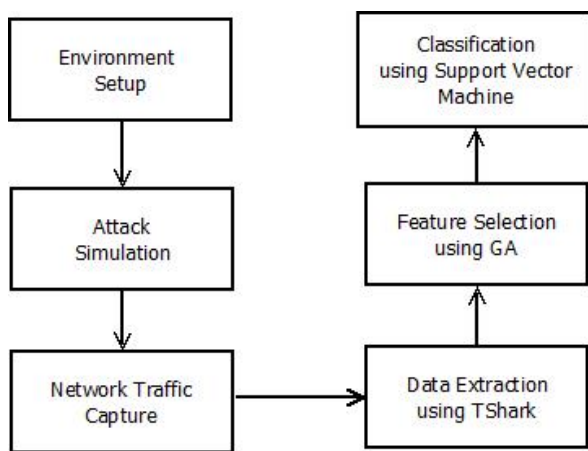


Figure 1. Block diagram of the classification system

#### 3.1. Experiment Design

In our experiment, we set up the environment consisting of three types of virtual machines (VMs), shown in Fig. 2., using VirtualBox 5.1.22, installed on computers with following specifications: Windows 8 operating system with 8 GB RAM and processor Intel(R) Core(TM) i5-45900 CPU @ 3.30GHz. The reason for using VMs is to protect our computers from the potential threats during the DoS attack simulation.

On one computer we installed Windows Server 2012 R2 with 4 GB RAM VM. Additionally, we installed Internet Information Services (IIS) with Web Server role, on which we hosted a website, and this is our victim (target) machine. On the second one, we installed Kali Linux with 4 GB RAM, whose task is to perform a DoS attack. On the third computer, 5 VMs (VM3- VM7) are installed and all of them represent the normal users who periodically access the website, hosted on the server. On this VMs, we installed Windows 7 with 1 GB RAM.

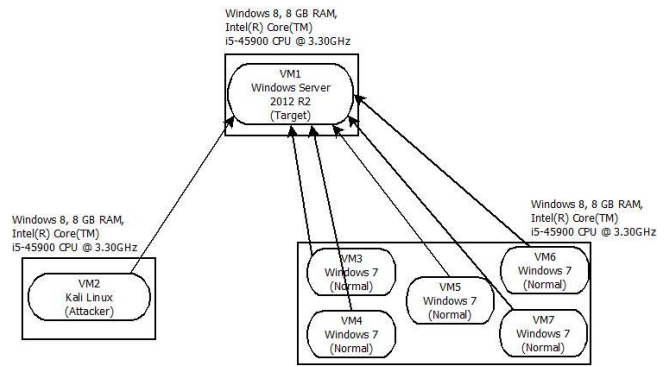


Figure 2. Logical diagram of the experimental design

#### 3.2. DoS Attack Simulation

The next step is an attack simulation. The attack is performed using network security tool hping3 from Kali Linux machine. Hping3 is a command-line TCP/IP packet analyzer. Furthermore, it supports TCP, UDP, ICMP and RAW-IP protocols [14]. The attack performed using hping3 is TCP SYN flood attack, which exploits a part of a normal 3-way handshake to exhaust the server resources and make it unresponsive [15]. In a normal 3-way, (1) client sends SYN (synchronize) message to request the connection, then (2) the server responds with SYN-ACK (synchronize-acknowledge) message back to the client, and finally (3) the client responds with ACK (acknowledge) message, and the connection is established (Fig. 3.). However, in TCP SYN flood, the attacker repeatedly sends SYN requests to a server, and the server responds with an SYN-ACK message, not knowing whether it is an attack or legitimate request. However, client attacker never sends final ACK or, if the IP address is spoofed, never receives SYN-ACK from the server. Therefore, the connection will never be established; the number of half-opened connections will be increasing; legitimate clients' requests will be denied and server can even crash or malfunction (Fig. 4.).

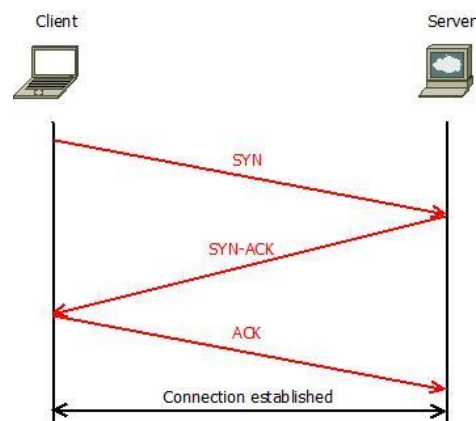


Figure 3. TCP three-way handshake

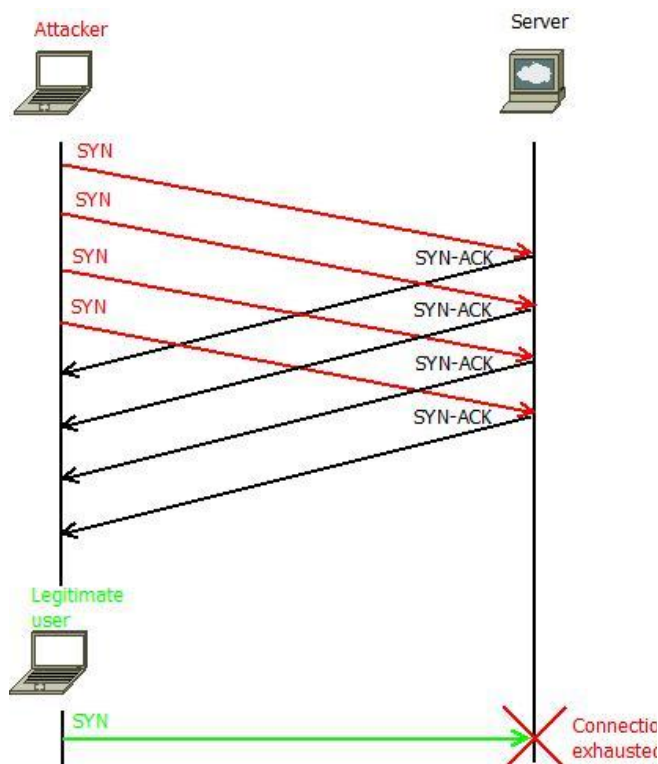


Figure 4. Progression of a TCP SYN flood

Network traffic is monitored and captured with Wireshark [16], which allowed us to see what is happening on the network on each layer of TCP/IP stack during the attack.

### 3.3. Dataset

The dataset is created by extracting the fields out of packets from Wireshark using TShark [17]. Using TShark, we extracted fields that indicate the DoS attack is happening, such as source and destination IP address, source and destination port, packet length, sequence and acknowledgment numbers, TCP flags, time-to-live (TTL).

The result of this extraction is a dataset of 7126 instances, where 4999 were from the attacker machine and 2127 instances were from the legitimate users.

### 3.4. Feature Selection

However, not all features are relevant to making a prediction. Therefore, it is important to do a feature selection and select the most relevant features that describe the attack. Additionally, feature selection is useful for removing features that create noise in a dataset. Furthermore, feature selection will enable machine learning algorithms to run faster, reducing the complexity of a model, and improving the accuracy, as most relevant input features are selected for the input. In this paper, we applied Genetic Algorithm (GA) feature selection described in [18],

[19]. GA is built as a parallel algorithm in MapReduce programming paradigm, allowing the input data processing in a distributed manner. This algorithm implements natural population selection, where it selects the individuals randomly to be parents and uses them to produce offspring for the next generation, until the optimal solution is found [20]. MapReduce is a programming paradigm for distributed computing, based on the two main functions: map and reduce. Map function takes set of data as input and returns elements broken into tuples, as key-value pairs. Reduce function takes the output of map function as its input and combines it into a smaller set of tuples, which is a new output [18].

Features of most importance ranked and selected by the GA are a source and destination port, sequence and acknowledgement numbers, SYN and ACK TCP flags and TTL. Therefore, we only consider these features for the classification.

### 3.5. Support Vector Machine (SVM)

The last step in the proposed classification system is the process of data classification using machine learning algorithm. In our approach, we have chosen SVM machine learning algorithm as a classifier. SVM concept is first presented by Boser, Guyon & Vapnik [21] and used for function estimation. It is presented as training algorithm used for maximizing the margin between training patterns and decision boundaries [22].

SVM is a hyperplane used to split positive and negative datasets of examples, by maximizing the margin. It belongs to a category of kernel methods since they solve the problems of quadratic increase in memory. It is very important when it comes to the features storing and time required for calculating the classifier's discriminant function by avoiding mapping the data into the high – dimensional feature space [23].

Hyperplane in SVM is created by following formula [22], [24]:

$$x : f(x) = x^T \beta + \beta_0 = 0,$$

where  $\beta$  is a unit vector.

Then, a classification rule by the  $f(x)$  function is created:

$$G(x) = \text{sign}[x^T \beta + \beta_0].$$

Now, the hyperplane for maximizing the margin between training points for classes DoS attack and

Normal behavior is created and classes are separable. The margin is expressed by formula:

$$M = \frac{1}{\|\beta\|},$$

and the optimization problem is presented by:

$$\max_{\beta, \beta_0, \|\beta\|=1} M$$

Margin in M units away from hyperplane from both sides.

In this research, we used Linear kernel for SVM classifier. It resulted in small computational time, whereas the classification accuracy significantly increased.

#### 4. Results

In this study, DoS attack classification system is proposed. The total number of 7126 feature vectors, where 4999 belong to cases which describe DoS attack and 2127 belong to cases which describe normal network traffic behavior, is extracted using TShark from the .pcap file. Consequently, we applied SVM machine learning algorithm to evaluate the performance of the proposed system.

##### 4.1. Performance Evaluation

The performance of the machine learning algorithm is evaluated using different approaches. The efficient statistical method is cross-validation, in which dataset is divided into the equal number of folds or partitions, where one fold is used for testing and the rest is used for training. Furthermore, this process is repeated as many times as a number of folds, where each fold serves as a testing and the rest serve as training samples. In this study, 10-fold cross validation is applied, where the dataset is divided into 10 folds of equal size. The model is tested on 1-fold and remaining 9 folds are used for training. The process is repeated 10 times and average cross validation accuracy is found [22].

Furthermore, we additionally considered sensitivity, specificity, average classification accuracy, F-measure and ROC curve as performance evaluation metrics.

- a) Sensitivity is a term that describes how good a classifier can recognize positive samples and is defined by [25]:

$$Sensitivity = \frac{TP}{TP + FN} \times 100$$

where TP is the number of true positive samples and FN is the number of false negative samples.

Sensitivity defines the number of DoS attack cases classified as such.

- b) Specificity is a term that describes how good a classifier can recognize negative samples and is defined by [25]:

$$Specificity = \frac{TN}{TN + FP} \times 100$$

where TN is the number of true negative samples and FP is the number of false positive samples.

Specificity defines the number of normal traffic behavior cases classified as such.

- c) Accuracy is a term that describes the average value of sensitivity and specificity, defined by a formula [25]:

$$Accuracy = \frac{Sensitivity + Specificity}{2}$$

- d) F - measure is a statistical index that shows the performance and efficiency of the model, and checks for the potential imbalance problems. It is defined by a formula [22], [26]:

$$F - measure = \frac{2TP_i}{2TP_i + FP_i + FN_i}$$

where  $TP_i$  is the true positive rate of the  $i^{th}$  class,  $FP_i$  is the false positive rate of the  $i^{th}$  class and  $FN_i$  is the false negative rate of the  $i^{th}$  class.

- e) ROC curve is used to show the discrimination ability of different statistical methods and is created by plotting the number of true positive values on y axis and number of false positive values on x-axis. Then, classification performance is measured by the means of area under the curve (AUC). The bigger the area is, the better classification model is [22], [25].

Additionally, we considered the computational time of the classifier required to build a classification model.



### 4.2. Experimental Results

An automated classifier that classifies network traffic behavior into two categories: normal behavior and DoS attack is designed. The whole dataset is divided into 10 partitions and 10-fold cross validation is applied. Finally, the average result of all folds is found and average accuracy is calculated. Additionally, experiments are done to examine the classification ability of the proposed algorithm in attack classification and detection.

We analyzed the classification performance of SVM classifier through following statistical indices: sensitivity or true positive rate (TPR), specificity or true negative rate (TNR), and classification accuracy. Furthermore, we included F-measure and ROC curve for performance evaluation. All statistical parameters are given in Table 1.

Table 1 - Performance evaluation of SVM algorithm for DoS attack classification

|            | TPR (%) | TNR (%) | Accuracy (%) | F-measure | ROC Area |
|------------|---------|---------|--------------|-----------|----------|
| DoS        | 100     | 100     | 100          | 1         | 1        |
| Normal     | 100     | 100     | 100          | 1         | 1        |
| Average    | 100     | 100     | 100          | 1         | 1        |
| Comp. time | 0.16 s  |         |              |           |          |

From Table 1., SVM classifier performed great when it comes to all statistical indices. It reached classification accuracy of 100% with both classes, F-measure and ROC curve of value 1. This shows that SVM classifier is able to successfully classify network traffic and determine whether it belongs to a class denoted as DoS attack or to the class denoted as normal network behavior.

Table 2. - Comparison of the results achieved in this study with the results from previous studies

| Authors                      | Methodology   | Data  | Attack   | Accuracy (%)                      | TP (%)                                | FP (%)                                  |
|------------------------------|---|---|--|-----------------------------------|---------------------------------------|---|
| Khorshed, Ali and Wasimi [8] | C4.5 decision tree  | Performance data: CPU, memory, disk and network usage   | RDoS<br>SYN flood<br>HTTP flood  | Overall 93.47                     | -                                     | -                                       |
| Khorshed et al [9]           | Random forest   | Performance data: CPU, memory, disk and network usage   | SYN flood<br>HTTP flood<br>ICMP flood  | Overall 93.9                      | 98<br>94.5<br>73.7                    | 0.1<br>0.1<br>0.1                       |
| Chen et al. [10]             | K-means clustering<br>Naive Bayes                                       | Network traffic data: source and dest. IP, source and dest. Port, package length and timestamp                    | DDoS   | -                                 | 90<br>90                              | 0.5<br>1.8                              |
| Pandeeswari and Kumar [11]   | Hybrid of Fuzzy C-Means clustering and Artificial Neural Networks (ANN) | Network traffic data: KDD 99 dataset  | DoS  | 99.96                             | 97.2                                  | 5.33                                    |
| Amiri et al. [12]            | Least Square Support Vector Machine (LSSVM)                             | Network traffic data: KDD 99 dataset  | DoS  | 84.11                             | 78.6<br>9                             | 0.73                                    |
| Kumar, Lal and Sharma [13]   | One-class Support Vector Machine  | Network traffic data: source and dest. IP, bytes of data transferred, protocol                                    | ICMP flood<br>Ping-of-Death<br>UDP flood<br>SYN flood<br>TCP Land<br>DNS flood | 100<br>94<br>97<br>96<br>98<br>99 | 100<br>100<br>97<br>100<br>100<br>100 | 0<br>12<br>2.85<br>7.69<br>4.55<br>2.85 |
| Our proposed model           | Support Vector Machine  | Network traffic features: source and dest. port, sequence and acknowledgement numbers, ack and syn flags, ip ttl. | SYN flood  | 100                               | 100                                   | 0                                       |

These results show that TP rate or the rate at which SVM classifier successfully classified all

instanced belong to a group of DoS attack is 100%, meaning that all instances are correctly classified.

Additionally, we tested the performance of SVM classifier by applying RBF kernel and it significantly decreased the classification accuracy, misclassifying normal network behavior as DoS attack.

## 5. Discussion

The results presented in the previous section confirm the ability of SVM classifier in DoS attack classification. Considering the results presented in Table 1., SVM classifier achieved great performance shown through statistical indices: accuracy, F-measure and ROC area. It misclassified only one instance that belonged to a group of DoS attack class.

Furthermore, the selection of kernel is of key importance and affect the performance of the classifier. The optimal performance was obtained with Linear kernel. We also tried other kernels, such as RBF and Puk, but performance accuracy decreased and model computational time increased (classification accuracy was around 99,7% and computational time was around 0.86 s).

Additionally, we compared our approach and obtained results with the results of previous studies, shown in Table 2.

When we compare classification accuracy of SVM in classifying SYN flood DoS attacks, it is noticeable that SVM achieved significant advantage over other classifiers in previous studies. Even though Kumar, Lal and Sharma [13] achieved TP rate of 100% in classifying SYN flood attacks with one-class support vector machine, the overall accuracy achieved is 96% which is less than in our study. Furthermore, when we compared TP rate obtained in our study with TP rates obtained in previous studies, it is obvious that our approach gives better results, considering all statistical indices.

According to the results presented in the Table 2., the following can be emphasized:

- Even though all classifiers performed well, SVM classifier has advantage over them considering TP, FP and accuracy rates;
- Optimal performance was obtained by using Linear kernel. Performance significantly changed when it comes to the classification accuracy and computational time;
- The impressive testing performance of SVM algorithm indicates that the proposed model can be successfully used in attack detection in cloud environment, but also in similar environments.

## 6. Conclusion

In this paper, an automated classification system for DoS attack detection in the cloud computing is proposed. The data for the study is obtained by simulating the cloud environment and DoS attacks and capturing network data with Wireshark. Furthermore, we extracted the necessary features using TShark and applied GA presented in [18] for feature selection. The last step is the data classification using Support Vector Machine. SVM showed significance in DoS attack classification by achieving the classification accuracy of 100% (with TP rate of 100% and FP rate of 0%), F-measure and ROC area of 100%. These results showed that SVM classifier is valuable in the field of network attack detection, considering its classification performance, as well as the computational time of the model.

## References

- [1] N. Antonopoulos and L. Gillam, *Cloud Computing: Principles, Systems and Applications*. Springer, 2017.
- [2] CSA Top Threats Working Group. (2016). The Treacherous 12: Cloud Computing Top Threats in 2016. *Cloud Security Alliance (CSA), Feb.*
- [3] Larry G. Wlosinski.(2015). Cloud Insecurities, *ISACA Journal*, 2.
- [4] M. McDowell, Understanding denial-of-service attacks, *National Cyber Alert System, Cyber Security Tip ST04-015*. 2004, 2004.
- [5] R. Samani, B. Honan, and J. Reavis, Eds., "About the Cloud Security Alliance," in *CSA Guide to Cloud Computing*, Boston: Syngress, 2015, p. xiii.
- [6] "The STRIDE Threat Model." Available: [https://msdn.microsoft.com/en-us/library/ee823878\(v=cs.20\).aspx](https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx). [Accessed: 07-Jul-2017].
- [7] NIST, I. (2014). NIST. gov-Computer Security Division-Computer Security Resource Center.
- [8] M. T. Khorshed, A. B. Shawkat, and S. A. Wasimi, "Classifying different denial-of-service attacks in cloud computing using rule-based learning," *Security and Communication Networks*, 2012.
- [9] Khorshed, M. T., Sharma, N. A., Kumar, K., Prasad, M., Ali, A. S., & Xiang, Y. (2015, December). Integrating Internet-of-Things with the power of Cloud Computing and the intelligence of Big Data analytics—A three layered approach. In *Computer Science and Engineering (APWC on CSE), 2015 2nd Asia-Pacific World Congress on* (pp. 1-8). IEEE.
- [10] Chen, Z., Xu, G., Mahalingam, V., Ge, L., Nguyen, J., Yu, W., & Lu, C. (2016). A cloud computing based network monitoring and threat detection system for critical infrastructures. *Big Data Research*, 3, 10-23.
- [11] Pandeewari, N., & Kumar, G. (2016). Anomaly detection system in cloud environment using fuzzy clustering based ANN. *Mobile Networks and Applications*, 21(3), 494-505.

- [12] Amiri, F., Yousefi, M. R., Lucas, C., Shakery, A., & Yazdani, N. (2011). Mutual information-based feature selection for intrusion detection systems. *Journal of Network and Computer Applications*, 34(4), 1184-1199.
- [13] Kumar, R., Lal, S. P., & Sharma, A. (2016, August). Detecting Denial of Service Attacks in the Cloud. In *Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech), 2016 IEEE 14th Intl C* (pp. 309-316). IEEE.
- [14] "Appendix B - Kali Penetration Testing Tools," in *Hacking with Kali*, Boston: Syngress, 2014, pp. 201–222.
- [15] Incapsula, "TCP SYN Flood, DDoS Attack Glossary ,Incapsula." [Online]. Available: <https://www.incapsula.com/ddos/attack-glossary/syn-flood.html>. [Accessed: 10-Jul-2017].
- [16] Combs, G. (2008). Wireshark: Go deep. *ArGo Software Design Homepage*, 31.
- [17] WireShark, [Online]. Available: <https://www.wireshark.org/docs/man-pages/tshark.html>. [Accessed: 10-Jul-2017].
- [18] Kečo, D., Subasi, A., & Kevric, J. Cloud computing-based parallel genetic algorithm for gene selection in cancer classification. *Neural Computing and Applications*, 1-10.
- [19] Keco, D., & Subasi, A. (2012). Parallelization of genetic algorithms using Hadoop Map/Reduce. *SouthEast Europe Journal of Soft Computing*, 1(2).
- [20] What Is the Genetic Algorithm - MATLAB & Simulink. [Online]. Available: <https://www.mathworks.com/help/gads/what-is-the-genetic-algorithm.html?requestedDomain=www.mathworks.com>. [Accessed: 11-Jul-2017].
- [21] Boser, B. E., Guyon, I. M., & Vapnik, V. N. (1992, July). A training algorithm for optimal margin classifiers. In *Proceedings of the fifth annual workshop on Computational learning theory* (pp. 144-152). ACM.
- [22] Masetic, Z., & Subasi, A. (2016). Congestive heart failure detection using random forest classifier. *Computer methods and programs in biomedicine*, 130, 54-64.
- [23] Ben-Hur, A., & Weston, J. (2010). A user's guide to support vector machines. *Data mining techniques for the life sciences*, 223-239.
- [24] Hastie, T., Tibshirani, R., & Friedman, J. (2009). Overview of supervised learning. In *The elements of statistical learning* (pp. 9-41). Springer New York.
- [25] Rokach, L., & Maimon, O. Z. (2008). Data mining with decision trees: theory and applications. Volume 69 of Series in machine perception and artificial intelligence.
- [26] Christov, I., Gómez-Herrero, G., Krasteva, V., Jekova, I., Gotchev, A., & Egiazarian, K. (2006). Comparative study of morphological and time-frequency ECG descriptors for heartbeat classification. *Medical engineering & physics*, 28(9), 876-887.