

MAD-SE: ADAPTIVE THRESHOLD-BASED STACK ENSEMBLE APPROACH FOR THE DETECTION OF DDOS ATTACK IN CLOUD

Rajesh Kumar Pateriya, Priyanka Verma* and Dharam Singh

Received: August 16, 2021; Revised: November 25, 2021; Accepted: December 29, 2021

Abstract

At present, cyber-attacks are steadily increasing in the cloud network. TCP, ICMP, UDP protocol-based Distributed Denial of Service (DDoS) attacks are the major contributors for making the cloud-based system unsafe. The rate of growth of DDoS cyber-attack is a severe and challenging problem in the network. In the literature, to handle such attacks, various feature selection, and classification techniques are used. In these methods, for the collection of optimal attributes, static thresholding methods are applied. However, when the various variant of DDoS causes a DDoS attack, the size of packets and attribute's value is significantly changed. Thus, the methods utilizing static statistics are not suitable for a dynamic network. Therefore, an adaptive threshold-based Mean Absolute Deviation technique (MAD) is used to overcome these drawbacks. Moreover, in this work, the Stacked Ensemble (SE) approach is utilized instead of the single classification algorithm for the classification purpose. The proposed approach comprises of three components; (1) data pre-processing, (2) optimal attribute selection, and (3) detection and prevention system from DDoS attacks. In this work, to evaluate the proposed approach, a standard NSL-KDD dataset is used. It is observed that MAD with SE beats all other combinations. In conventional methods, selecting a single classifier may not perform well because it works well on training data, but it poorly classifies the non-viewed new data. The stack ensemble approach removes this issue. Moreover TCP, UDP, and ICMP-based DDoS flooding attacks can also be easily noticed and classified by MAD-SE.

Keywords: Cloud computing, Dynamic threshold, DDoS attack, Ensemble learning, Machine learning

Introduction

Cloud based services are growing rapidly every day in several prospects because of its endlessness and varied skill. Simultaneously, the number of information security violations has sharply increased, due to this, the vital interest of computer security research is in network security.

The offensive network traffic such as DDoS is the most significant affecting hazards for cloud services. So, appropriate action should be taken to defend cloud resources from these attacks. Cloud computing delivers on-demand computing services that provide its resources and services custom-built

Department of Computer Science and Engineering, Maulana Azad National Institute of Technology (MANIT), M.P., India.
E-mail: 303priyanka.verma@gmail.com

* Corresponding author

to the users. To access cloud services and resources, many companies hire computing infrastructure. In this way, the cloud helps millions of companies in reducing their maintenance cost for IT infrastructure. These services are provided as reported by the end-user (Zissis and Lekkas, 2012). Cloud services are also used in business, education, e-health (Riad *et al.*, 2019), entertainment, management, and social networking.

Nowadays, businesses and operations move to the cloud, and cloud providers are becoming prime targets for malicious attacks. A challenging part in hindering the evolution of cloud computing is the security (Aldossary and Allen, 2016). The most important feature of cloud computing is resource sharing, virtualization, multitenancy, auto-scaling. For resource exhaustion, the attacker exploits the anomalies to launch various attacks like DoS and DDoS attacks (Hamza *et al.*, 2020). Verisign reported IT services that during the first quarter of 2015 that cloud platforms (PaaS and SaaS) were the most commonly targeted industry. A DDoS attack is intended to overpower the website servers, so it can no longer respond to authentic user requests. If a DDoS attack is successful, it renders a website useless for hours or even days. Thus, eventually result in a loss of revenue, customer trust, and brand authority. Financial gain, cyberwar for military advantage, political ideologies, cyberbullying, and trolling are the psychological motivation behind the majority of DDoS cyber-attack. DDoS attacks cause huge damages and appear to be treacherous in the cloud.

Multitenancy, virtualization, resource sharing, and auto-scaling are the features that help the attacker raise the circulation of attacks. Due to vulnerabilities (Peng *et al.*, 2007) on the internet, IP spoofing has become easier for the attacker. In the cloud network, for detection and classification of DDoS attacks, various modules of solutions exist. These modules are based on genetic algorithms, data mining, machine learning, bio-inspired, and neural networks (Somani *et al.*, 2017a; Somani *et al.*, 2017b; Chaudhary *et al.*, 2018). In the DDoS defense process, these methods exhaust more resources and generate various overheads. These approaches result in low accuracy, have more training and testing time, and give a high false alarm rate. Furthermore, the existing approach depends on statistics to select an attribute for the classification of request (Koc *et al.*, 2012; Wang and Gombault, 2008; Hoz *et al.*, 2015; Hajimirzaei and Navimipour, 2018; Thaseen and Kumar, 2017; Mazini *et al.*, 2019).

Therefore, this work proposes MAD-SE, MAD threshold for attribute selection, and stack ensemble for classification of attack and normal

request for DDoS defense. Since thresholding makes the detection method more active and more robust in the diverse network and incoming traffic behaviors. Whereas using a stacked ensemble classifier helps in achieving the highest accuracy. The significant contributions of this paper are:

- 1). An adaptive thresholding method is used to extract optimal features rather than filter methods. These optimal features play a significant role in DDoS attack detection.
- 2). It selects optimal features by calculating the entropy and thresholding value of each attribute.
- 3). Proposed approach uses a stacked ensemble classifier instead of a single classifier.
- 4). The proposed approach achieves high accuracy and low false alarm for detecting TCP, UDP, and ICMP-based DDoS attacks.

The remainder section of the paper is organized as; Section 2 presents the material and methods used. Experimental analysis is shown in section 3, and section 4 concludes the work.

Related Work

This section presents the detailed description of DDoS attack, followed by existing attribute selection and classification techniques to defend against DDoS attack in cloud network.

DDoS Overview

The most advanced form of DoS (Denial of Service) attack is DDoS (Distributed Denial of Service) and DDoS attacks occur more frequently. It is tough to trace them, as they became more powerful by using the internet architecture. DDoS can expand its weapons in a distributed way on the internet and create destructive traffic by assembling these forces. There are three kinds of DDoS cyber-attack (1) Volumetric attack, (2) Fragmentation attack, (3) Application layer attack.

The attacker finds out the vulnerable host machine by creating the troops. By using these troops, it produces large number. of traffic to flood the target system. It used a lot of methods to find vulnerable host machines (1) Hitlist scanning, (2) Local subnet scanning, (3) Random scanning, (4) Permutation scanning, (5) Topological scanning.

These vulnerabilities help the attacker use the host machine as a zombie machine by efficiently exploiting the system. To compromise the host machine attacker installs attacking tools like LOIC, XOIC, DDoSIM, DVOSET, R-U-Dead-Yet After propagating the malicious code, so that these machines can work under the guidance of the attacker. Techniques used for the propagation of malicious code are (1) Autonomous propagation, (2) Central source propagation, (3) Back chaining propagation.

Now, we study the former research paper that is appropriate to this field. (Somani *et al.*, 2017a) show analysis on DDoS attacks and how it has distinct and high consequences in the cloud environment regarding the fixed network. One more audit on DDoS (Chaudhary *et al.*, 2018), reveals the effects of cyber-attack on cloud and fog computing infrastructure. In (Inayat *et al.*, 2017), the author reviews intrusion detection and response systems deployed to utilize cloud resources in mobile devices securely.

Feature selection technique

The filter feature selection method is a pre-processing phase for choosing optimal features from a dataset. number of optimally selected attribute plays a major role in classification problems; it reduces the dimensionality of the data set. (Wang and Gombault, 2008) suggested a filter selection technique to select most of the network traffic features using chi-squared and information gain (IG). To diagnose the DDoS, (Thaseen and Kumar, 2017) apply Chi-squared attribute selection and multiclass SVM. (Özçelik and Brooks, 2015) suggest an entropy-based technique for DDoS detection. (Qi *et al.*, 2013) represent a dynamic entropy mechanism for DDoS defense. (Osaniye *et al.*, 2016) uses Information gain (IG), chi-squared, reliefF, and gain ratio as multiple filters for attribute selection to identify and classify attack requests. Moreover, to detect DDoS attacks in IoT (Jia *et al.*, 2020) proposed an edge-centric 'FlowGuard' scheme to provide a complete defense against IoT DDoS attacks. FlowGuard consists of two major components, i.e., flow filtration and DDoS attack

detection. The proposed approach is evaluated on the CICDDoS2019 dataset combined with a generated dataset.

However, in existing work for DDoS defense, various entropy and feature-based technique are used. But due to the static nature of approaches, these models have some limitations. It is more challenging work in diagnosing the DDoS attack in varying network conditions in the cloud environment. To overcome these issues, the proposed approach suggests an effective technique, and it also helps improve the performance of cloud infrastructure by detecting the DDoS cyber-attack.

Materials and Methods

In order to protect the cloud network from DDoS attacks, the proposed approach is proficient for the classification of attack and benign requests. The proposed method comprises of three components: (1) data pre-processing, (2) optimal attribute selection and, (3) detection and prevention system. Figure 1 shows the workflow of the proposed approach. Initially, the attributes are extracted from the traffic stream, and the encoding technique is applied, and then further, the data is normalized in the data pre-processing section. Secondly, with the help of adaptive thresholding techniques (MAD), optimal attributes are selected. Finally, using the stacked ensemble learning technique, classification of the traffic data into DDoS and benign requests. After identifying DDoS requests, they are blocked and discarded, and benign requests gain access to use the cloud resources.

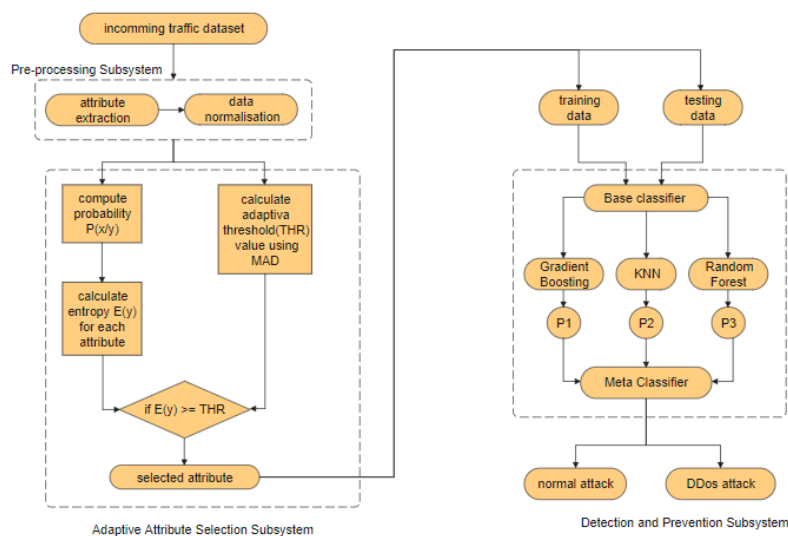


Figure 1. Workflow of proposed MAD-SE approach

Data pre-processing

The cloud network contains several Network Interface Devices (NID), also called Network Interface Unit (NIU). It is an interface between customer and network provider local loop, one of these NID is selected to monitor arrived packet behavior.

To monitor the behavior of network traffic in cloud users, select one of the NID. By using this NID, packet information is stored in a log file. These packets have various information like source IP, flags, destination IP, header length, payload, source port, and destination port. The attributes are extracted from the packet's information and are used for attack detection.

In this work, a standard NSL-KDD dataset is utilized to evaluate the proposed approach. Algorithm 1 represents the steps of data pre-processing.

The NSL-KDD consists of 41 attributes, and on these attributes, apply one-hot and label encoding technique. After applying one-hot label encoding, the dimensionality of NSL-KDD dataset is increased. Table 1 Shows the dimension change from input layer to output layer after applying one-hot encoding. As the NSL-KDD dataset consists of 41 independent attributes, out of which it consists of three categorical attributes such as flag, protocol, and service. Protocol contains three unique values, flag contains ten unique values, and service contains 65 unique values. Therefore the after applying the one-hot encoding the dimension of the dataset is increased to 116 labels. Then further, the data is normalized using min-max. Min-max normalization (Han *et al.*, 2011) helps to bring the dataset in an appropriate range. In normalization, a linear transformation is performed on encoded data by using Equation (1).

$$v' = \frac{v - \min(x)}{\max(x) - \min(x)} (b - a) + a \quad (1)$$

Where v' is the new value for each entry in attribute x , v is the old value for each entry in attribute x , and b, a is the max and min value of the range. $\min(x)$, $\max(x)$ is the min and max absolute value of attribute x . Further, normalized data is passed to the attribute selection module.

Algorithm 1 data Pre-processing

Input: NSL-KDD dataset (NKD)

Output: Normalized NKD

- 1). Extract the attributes from the NKD and apply encoding technique
- 2). Normalize NKD using min-max normalisation Equation (1)
- 3). Passed normalized data in attribute selection module

Optimal attribute selection

In this module attributes from the pre-processed data are selected using Algorithm 2. First we calculate the probability of all attribute using Equation (2).

$$p(a/b) = p(a, b)/p(b) \quad (2)$$

We use this probability to calculate the entropy for each attribute. Measurement of randomness or uncertainty related to a Random Variable (RV), called entropy (E). In this case, RV is data coming over the network. On increasing the randomness, it also increases the entropy. The more random it is, the more entropy it contains.

To analyse traffic behaviour during the DDoS attack, Shannon's entropy (Shannon, 2001) is used to measure the randomness of the dataset against every attribute. In protocol-based classification, DDoS attacks are UDP, TCP, ICMP protocol-based flooding attack (Sree and Bhanu, 2018). Calculation of entropy for every attribute of the dataset is done using Equation (3).

Table 1. Shows the dimension change from input layer to output layer after applying one-hot encoding

Input Layer	Output Layer
Duration, Src_bytes, Dst_bytes, Land, Wrong_fragment, Urgent, Hot, Num_failed_logins, Logged_in, Num_compromised, Root_shell, Su_attempted, Num_root, Num_file_creations, Num_shells, Num_access_files, Num_outbound_cmds, Is_hot_login, Is_guest_login, Count, Srv_count, Serror_rate, Srv_serror_rate, Rerror_rate, Srv_rerror_rate, Same_srv_rate, Diff_srv_rate, Srv_diff_host_rate, Dst_host_count, Dst_host_srv_count, Dst_host_same_srv_rate, Dst_host_diff_srv_rate, Dst_host_same_src_port_rate, Dst_host_srv_diff_host_rate, Dst_host_serror_rate, Dst_host_srv_serror_rate, Dst_host_rerror_rate, Dst_host_srv_rerror_rate	No change (38 attributes)
Protocol type	Protocol_1 to Protocol_3
Service	Service_1 to Service_65
Flag	Flag_1 to Flag_10

$$E(b_i) = - \sum p(b_i, a) \log(p(b_i, a)/p(a)) \quad (3)$$

Algorithm 2 Optimal attribute selection module**Input:** Normalize data NKD**Output:** Optimal attribute set (A_opt)

- 1). Calculate the probability $P(x/y)$ and entropy $E(y)$ for each attribute using Equation (2) and Equation (3).
- 2). By using MAD, calculate threshold value (THR)
- 3). if $(E(y) \geq \text{THR})$
 add y to A_opt
 else
 delete attribute y
- 4). Partition A_opt into T_train and T_test for training and testing purpose.
- 5). Pass these T_train and T_test into Detection and Prevention Subsystem

For the classification and identification of requests, the crucial aspect is attribute selection. By selecting the suitable number of attribute, the dimensionality of the dataset is reduced. It also reduces computational complexity and increases efficiency by deleting non-essential attributes. In this module, the attribute which has more entropy value than MAD threshold value are selected as the optimal attribute for training the stack ensemble classifier. The adaptive threshold value is calculated by applying the mean absolute deviation on the incoming data.

In the present literature, for the collection of the optimal attribute, static thresholding methods are applied. And when cyber-attack occurs by various variants of DDoS, the size of packets and attribute's value is substantially changed. Therefore, static threshold-based methods do not achieve optimal results in varying network traffic condition (Verma *et al.*, 2020). The static thresholding value chosen by one network state will not work properly for others. Therefore, the major limitations of static threshold based techniques are (Wang and Gombult, 2008; Koc *et al.*, 2012; Hoz *et al.*, 2015; Yang *et al.*, 2019a; Verma *et al.*, 2020); (1) these methods are not capable of detecting varying changes in cloud environment caused by DDoS attack in the network traffic, (2) static entropy-based techniques cannot detect the attack in real time and may suffer from spoofing, and (3) unknown attacks are also not detected by these methods.

Therefore, in this work we use Mean Absolute Deviation (MAD) adaptive thresholding technique to overcome these drawbacks. MAD thresholding method is used as follows for calculation of threshold value.

$$MAD = \text{mean}(|y - \text{mean}(y)|)$$

$$T_{min} = \text{mean}(y) + a * MAD$$

$$T_{min} = \text{mean}(y) - a * MAD$$

where a is decided by the user to select k most attribute and a is usually set to 3 to 5.5 (Yang *et al.*, 2019b). In our case it is set to 5.5.

Using MAD 29 attributes are selected from the 116 attributes that are resulted after hot ending as mentioned in data pre-processing section.

Detection and prevention system

The stacked ensemble model is also known as a multiple classifier systems. It first selects various kinds of base classifiers. These are trained using training data, and this learner's output is merged to make a new data set for the meta-learner. Meta classifier trained on a new dataset. Errors of base learners are identified by meta-learner, and it adjusts them for an optimistic solution. This mode iterates with K times for K -fold cross-validation to minimize error.

In conventional methods, a single classifier may perform badly because it works well on training data, but it poorly classifies the non-viewed new data. The stack ensemble approach removes this issue.

Algorithm 3 represents the steps of the detection and prevention system. Gradient Boosting, KNN, Random Forest are the base learners, and logistic regression is used as a meta-classifier in the stack ensemble model used in this work.

Algorithm 3 Detection and Prevention System**Input:** T_train and T_test**Output:** DDoS or benign class.

- 1). learn level-1 base classifiers, no. of learner=3
 1. learn
GradientBoostingClassifier(n_estimators=100)
 2. learn
RandomForestClassifier(n_estimators=100)
 3. learn KNeighborsClassifier ()
- 2). construct new dataset of prediction of Gradient Boosting, Random Forest, and KNN
- 3). learn meta-classifier on new dataset using Logistic regression
- 4). Meta classifier classify T_test in either DDoS request or benign request
 1. Benign class requests are permitted to utilize the cloud services.
 2. DDoS class requests are rejected and update the black list

In the prevention system, all attacked requests are consigned for further processing. This system warns the network when a DDoS attack is detected and takes suitable action. Source IP of the attacked packet is put into the blocklist so that it will not be permitted in the future, and non-attacked packets are permitted to utilize cloud resources.

Results and Discussion

For experimental evaluation, Python 3.7.3 is used to execute and estimate the proposed method on Microsoft window 10, 64-bit processor, 8 GB RAM with Intel(R) Core (TM) i5-8250U CPU@2.50 GHz on HP system. The proposed work is analyzed against NSL-KDD dataset. It is an updated version of the KDD cup99 data set. The dataset consists of 4 attack traces, out of which only DoS attack and benign request are helpful to train and test the proposed method.

The proposed approach is compared with existing feature selection techniques, and it is observed that the ReliefF method performs worst for all the classifiers compared to all the techniques. Similarly, other techniques such as Information Gain, Chi-Squared also do not work effectively in all prospects. However, MAD with different classifiers achieves the best results. From Table 2, it is also determined that MAD with stack ensemble gives excellent outcomes for F1-score, accuracy, and Root Mean Square Error (RMSE) over the other thresholding techniques. Table 2 shows that MAD-

SE attains 99.355% accuracy, which is better than information Gain, Chi-Squared, and ReliefF. Similarly, MAD-SE also attains the best F1-score, low FPR 0.007 as compared to other techniques. The primary reason for the outperformance of MAD-SE are:

- Features are selected based on incoming traffic stream.
- It combines the best prediction from two or more base classifiers by the meta-learning algorithm.
- Stacking allows using the strength of each individual base classifier, by using their output.

In a protocol-based DDoS attack, the effectiveness of MAD-SE is represented in Table 3. These protocols are TCP, ICMP, UDP. For TCP-based DDoS attacks, MAD-SE achieves the highest accuracy of 99.92%, 99.92% TNR and 0.0007 FPR. Similarly, for ICMP and UDP-based DDoS attack, MAD-SE achieves 99.76% and 99.80% accuracy, respectively. Moreover, MAD-SE also results in low FPR of 0.0024 and 0.0014 respectively for ICMP and UDP based DDoS attack.

Table 3. Evaluation of MAD-SE for TCP, UDP, and ICMP based DDoS attack

Protocol	Accuracy	TPR(%)	TNR(%)	FPR	FNR
TCP	99.923	99.923	99.923	0.0007	0.0007
ICMP	99.762	99.759	99.765	0.0023	0.0024
UDP	99.801	99.858	99.006	0.0099	0.0014

Table 2. Comparison of MAD-SE with other feature selection and classification techniques

Technique	Classifier	Accuracy(%)	TPR(%)	TNR(%)	FPR	FNR	F1-Score	RMSE
Information Gain	RF	98.8669	99.8372	97.4378	0.0256	0.0016	0.9906	0.1063
	GBM	98.8036	99.8047	97.3222	0.0267	0.0019	0.9901	0.1093
	SVM	93.6958	98.7372	86.2357	0.1376	0.0126	0.9492	0.2511
	KNN	98.9784	99.2254	98.6129	0.0138	0.0077	0.9914	0.1011
Chi-Squared	SE	98.9713	99.1538	98.9693	0.0103	0.0084	0.9922	0.0959
	RF	98.1251	98.7628	97.1658	0.0283	0.0123	0.9844	0.1369
	GBM	97.8558	99.4525	95.4536	0.0454	0.0054	0.9823	0.1464
	SVM	96.4704	98.9223	92.7816	0.0721	0.0107	0.9711	0.1878
	KNN	98.1329	98.8145	97.1074	0.0289	0.0118	0.9845	0.1366
ReliefF	SE	98.1692	98.7542	97.2891	0.0271	0.0179	0.9848	0.1353
	RF	93.3474	98.5429	85.5308	0.1446	0.0145	0.9467	0.2579
	GBM	92.3686	98.5688	83.0404	0.1695	0.0143	0.9394	0.2762
	SVM	93.3448	98.5386	85.5308	0.1446	0.01461	0.9467	0.2579
	KNN	94.6799	98.5429	85.5308	0.1446	0.01457	0.9467	0.2579
MAD	SE	93.3474	98.5429	85.5308	0.1446	0.01457	0.9467	0.2579
	RF	98.5048	98.0537	99.1812	0.0081	0.0056	0.9874	0.1221
	GBM	98.2326	97.7283	98.979	0.0102	0.0227	0.985	0.1329
	SVM	86.8906	87.9125	85.3785	0.1462	0.1208	0.8889	0.6321
	KNN	98.9667	98.9975	98.9212	0.0107	0.0101	0.9913	0.1016
	SE	99.3552	99.4597	99.2005	0.0079	0.0054	0.9945	0.0802

Conclusion

Due to TCP, ICMP, UDP protocol-based DDoS attacks, a cloud-based system is unsafe. The rate of growth of DDoS attacks is a serious and challenging problem in any infrastructure. The DDoS attack is not only a serious threat to traditional networks but also to cloud infrastructure. To avoid the existing issues of DDoS attacks over cloud network proposed method is helpful. The proposed method uses an adaptive hybrid technique MAD-SE for attribute selection and classification to classify incoming traffic. The proposed approach is effective in the classification of TCP, ICMP, and UDP-based DDoS attacks. MAD-SE delivers 99.335% accuracy, 94.459% detection rate and 0.9945 F1 score and 0.0007 FPR. Result reveals that the proposed approach outperforms other attribute selection techniques. Thus, MAD-SE precisely upgrades accuracy, false-positive rate, detection rate, precision, and F1 score with low resource consumption.

Acknowledgement

The implementation has been performed in Cyber Security lab of Maulana Azad National Institute of Technology (MANIT), Bhopal. The authors would like to acknowledge MANIT, Bhopal, and MHRD, Government of India for providing resources for the implementation of this work.

References

- Aldossary, S., and Allen, W. (2016). Data security, privacy, availability and integrity in cloud computing: issues and current solutions. *Int. J. of Advanced Computer Sci and App.*, 7(4):485-498.
- Chaudhary, D., Bhushan, K., and Gupta, B.B. (2018). Survey on DDoS attacks and defense mechanisms in cloud and fog computing. *Int. J. of E-Services and Mobile Applications (IJESMA)*, 10(3):61-83.
- Hoz De la, E., Hoz De La, E., Ortiz, A., Ortega, J., and Prieto, B. (2015). PCA filtering and probabilistic SOM for network intrusion detection. *Neurocomputing*, 164:71-81.
- Hajimirzaei, B. and Navimipour, N.J. (2019). Intrusion detection for cloud computing using neural networks and artificial bee colony optimization algorithm. *ICT Express*, 5(1):56-59.
- Hamza, R., Yan, Z., Muhammad, K., Bellavista, P., and Titouna, F. (2020). A privacy-preserving cryptosystem for IoT E-healthcare. *Information Sci.*, 527:493-510.
- Han, J., Pei, J., and Kamber, M. (2011). *Data mining: concepts and techniques*. Elsevier.
- Inayat, Z., Gani, A., Anuar, N.B., Anwar, S., and Khan, M.K. (2017). Cloud-based intrusion detection and response system: open research issues, and solutions. *Arabian J. for Sci. and Eng.*, 42(2):399-423.
- Jia, Y., Zhong, F., Alrawais, A., Gong, B., and Cheng, X. (2020). Flowguard: An intelligent edge defense mechanism against IoT DDoS attacks. *IEEE Internet of Things Journal*, 7(10):9,552-9,562.
- Koc, L., Mazzuchi, T.A., and Sarkani, S. (2012). A network intrusion detection system based on a Hidden Naïve Bayes multiclass classifier. *Expert Systems with Applications*, 39(18):13,492-13,500.
- Mazini, M., Shirazi, B., and Mahdavi, I. (2019). Anomaly network-based intrusion detection system using a reliable hybrid artificial bee colony and AdaBoost algorithms. *Journal of King Saud University-Computer and Information Sci.*, 31(4):541-553.
- Osanaiye, O., Cai, H., Choo, K.K.R., Dehghantanha, A., Xu, Z., and Dlodlo, M. (2016). Ensemble-based multi-filter feature selection method for DDoS detection in cloud computing. *EURASIP J. on Wireless Communications and Networking*, 2016(1):1-10.
- Özçelik, İ. and Brooks, R.R. (2015). Deceiving entropy based DoS detection. *Computers and Security*, 48:234-245.
- Peng, T., Leckie, C., and Ramamohanarao, K. (2007). Survey of network-based defense mechanisms countering the DoS and DDoS problems. *ACM Computing Surveys (CSUR)*, 39(1):3-es.
- Riad, K., Hamza, R., and Yan, H. (2019). Sensitive and energetic IoT access control for managing cloud electronic health records. *IEEE Access*, 7:86,384-86,393.
- Shannon, C.E. (2001). A mathematical theory of communication. *ACM SIGMOBILE mobile computing and communications review*, 5(1):3-55.
- Somani, G., Gaur, M. S., Sanghi, D., Conti, M., Rajarajan, M., and Buyya, R. (2017a). Combating DDoS attacks in the cloud: requirements, trends, and future directions. *IEEE Cloud Computing*, 4(1):22-32.
- Somani, G., Gaur, M.S., Sanghi, D., Conti, M., and Buyya, R. (2017b). DDoS attacks in cloud computing: Issues, taxonomy, and future directions. *Computer Communications*, 107:30-48.
- Sree, T.R., and Bhanu, S.M.S. (2018). Detection of http flooding attacks in cloud using dynamic entropy method. *Arabian J. for Sci. and Eng.*, 43(12):6,995-7,014.
- Thaseen, I.S., and Kumar, C.A. (2017). Intrusion detection model using fusion of chi-square feature selection and multi class SVM. *J. of King Saud University-Computer and Information Sci.*, 29(4):462-472.
- Verma, P., Tapaswi, S., and Godfrey, W.W. (2020). An adaptive threshold-based attribute selection to classify requests under DDoS attack in cloud-based systems. *Arabian J. for Sci. and Eng.*, 45(4):2,813-2,834.
- Wang, W., and Gombault, S. (2008). Efficient detection of DDoS attacks with important attributes. In: 2008 Third International Conference on Risks and Security of Internet and Systems, pp. 61-67.
- Yang, C. (2019a). Anomaly network traffic detection algorithm based on information entropy measurement under the cloud computing environment. *Cluster Computing*, 22(4):8,309-8,317.
- Yang, J., Rahardja, S., and Fränti, P. (2019). Outlier detection: how to threshold outlier scores?. In *Proceedings of the international conference on artificial intelligence, information processing and cloud computing*, pp. 1-6.
- Zissis, D. and Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation computer systems*, 28(3):583-592.