Computer Systems Science & Engineering
DOI: 10.32604/csse.2023.024691
Article

Tech Science Press

Iterative Dichotomiser Posteriori Method Based Service Attack Detection in Cloud Computing

B. Dhiyanesh[1,*], K. Karthick[2], R. Radha[3] and Anita Venaik[4]

[1]Hindusthan College of Engineering and Technology, Coimbatore, 641032, India
[2]Sona College of Technology, Salem, 636005, India
[3]Karpagam Institute of Technology, Coimbatore, 641105, India
[4]Amity Business School, Amity University, Noida, 201301, India
*Corresponding Author: B. Dhiyanesh. Email: dhiyanu87@gmail.com

Received: 27 October 2021; Accepted: 24 January 2022

Abstract: Cloud computing (CC) is an advanced technology that provides access to predictive resources and data sharing. The cloud environment represents the right type regarding cloud usage model ownership, size, and rights to access. It introduces the scope and nature of cloud computing. In recent times, all processes are fed into the system for which consumer data and cache size are required. One of the most security issues in the cloud environment is Distributed Denial of Service (DDoS) attacks, responsible for cloud server overloading. This proposed system ID3 (Iterative Dichotomiser 3) Maximum Multifactor Dimensionality Posteriori Method (ID3-MMDP) is used to overcome the drawback and a relatively simple way to execute and for the detection of (DDoS) attack. First, the proposed ID3-MMDP method calls for the resources of the cloud platform and then implements the attack detection technology based on information entropy to detect DDoS attacks. Since because the entropy value can show the discrete or aggregated characteristics of the current data set, it can be used for the detection of abnormal data flow, User-uploaded data, ID3-MMDP system checks and read risk measurement and processing, bug rating file size changes, or file name changes and changes in the format design of the data size entropy value. Unique properties can be used whenever the program approaches any data error to detect abnormal data services. Finally, the experiment also verifies the DDoS attack detection capability algorithm.

Keywords: ID3 (Iterative dichotomiser 3) maximum multifactor dimensionality posterior method (ID3-MMDP); distributed denial of service (DDoS) attacks; detection of abnormal data flow; SK measurement and processing; bug rating file size

1 Introduction

This has evolved from various existing technologies such as cloud computing phases, application computing, and service-oriented architecture. By using cloud computing, many companies can invest large sums of new infrastructure, software licenses and expand without building big data centers. The handling of abnormal data network traffic is still a critical issue that needs to be resolved because the abnormality may relate to the service at a particular moment.

Denial affects all parties, and distributed denial of service (DDoS) attacks are a severe problem extending cloud computing. The primary purpose of a DDoS attack is that the service attempts to restrict access to the machine or service rather than destroying the service itself-even if it is interrupted. This type of attack makes the network unable to provide regular services by targeting the network bandwidth or connectivity. Therefore, the methods and resources that can carry out and cover up this kind of attack are considerably evolved. This problem needs to be solved as soon as possible. Otherwise, the expenditures of biology and users of cloud services will increase with greater risk exposure simultaneously. In the rest of this article, DDoS attacks are defined, and second, some mechanisms used to mitigate DDoS attacks are summarized and discussed.

2 Related Work

Software-defined Networking (SDN) can be used to detect and slow down network-based, HTTP DDoS-based network attacks to assist security systems [1]. To run our simulation environment on the Mininet virtual machine, the Open Network Operating System (ONOS) controller is the closest option to a real-world product network [2].

Combined with intra-regional and inter-domain DDoS attack protection, Security Chain (SC) allows effective mitigation, including a continuous attack, and an effective mitigation path near the onset of the attack. Most of these are useless to augment horrendous traffic and can significantly reduce the cost of messaging across multiple sectors. As far as I know, on-chain-SC is the first solution proposed to resolve DDoS attacks, blockchain, and smart deals on inter-technology to mitigate this two-domain and SDN combination. Access to Ropsten for Chain-SC activation is suspended on the ethereal test network [3–5].

Blockchain technology is used to overcome the SOC (Security Operations Center), trust, and integrity issues on the decentralized denial of service data exchange platform [6]. The DDoS attack vector is called a multiplex asymmetric DDoS attack that uses multiple options differently [7].

A novel DDoS detection framework is implemented using the Pursuit algorithm that matches the type of resource degradation DDoS attack detection. Multiple properties are used for network traffic to detect low-density DDoS attacks [8] simultaneously.

The Denial of Service (DDoS) attack has severely affected network availability for decades, yet robust security mechanisms are against it. However, Emerging Software Limited Network (SDN) offers a new way to protect against DDoS attacks. This article proposes two methods to detect DDoS attacks in SDN [9,10]. Dynamically selected algorithms from the framework classification algorithms are ready to detect different DDoS ways that use fussy logic [11]. Utility Layered Distribution Service Denial (UL-DDoS) Attacks and Al-DDoS attack's magic can make many intrusion prevention methods ineffective and pose a significant threat to websites [12].

Application Layer DDoS Assistance in Understanding these Job Attempts uses the Full Spectrum of Attack These attacks can perform critical functions [13]. An accurate method is used to diagnose DDoS attacks by Exceeding Ratio Measurements (ERM). The proposed method is based on the difference between the probability distribution and the number of flows [14].

Denial of Service (DDoS) attacks prevent online services from being voted on by traffic from multiple sources. Therefore, an effective method is proposed to detect DDoS attacks from massive data traffic jams [15]. In the development model of the novel botnet, the optimal design of the attack strategy is estimated on the DDoS, and the expected impact function refers to the attack. The associated DDoS approach reduces the variational problem to attack [16].

Denial Service Spread (DDoS) attacks are the second most popular cybercrime attack after information theft. DDoS TCP flood attacks, which deplete cloud resources and increase bandwidth, can affect the entire cloud computing program in a short period [17]. Emerging Network Operation Virtualized (NFV) technology Network Services Publishing demand reduces ownership hardware size and introduces new operating opportunities [18].

The deep convolutional neural network (DCNN) automatically learns the optimization function of the original data distribution. It does not use the deep reinforcement learning Q-network to make a decisive decision to protect against attacks [19]. The infiltration detection and security model for CPSS (Cloud-Physical-Social Organization) are standard infiltration analysis properties. They can effectively detect large-scale Low-Rate (LR) DDoS attacks, particularly in the marginal environment [20].

This section presented the using methods described by various authors. These methods contain some limitations in introducing the proposed method. This method gives better results compared to the previous system.

3 Implementation of the Proposed System

The ID3 (Iterative Dichotomiser 3) Maximum Multifactor Dimensionality Posteriori Method (ID3-MMDP) system is based on the risk value, and then different state detection details are updated. For the proposed defense mechanism, the behavior differences between the allocation strategy of attackers and ordinary users are to be analyzed. Data errors cause damage to the data values in the program, resulting in incorrect intermediate values and final output files. Fault tolerance should include improving the reliability and integrity of the proposed system.

Setting up the same server cloud environment together behind the load balancer is considered. The average rate of request arrival and R requests per unit time and the load balancer are in a steady-state S distributed to the cloud data center, and the details are shown in the above Fig. 1.

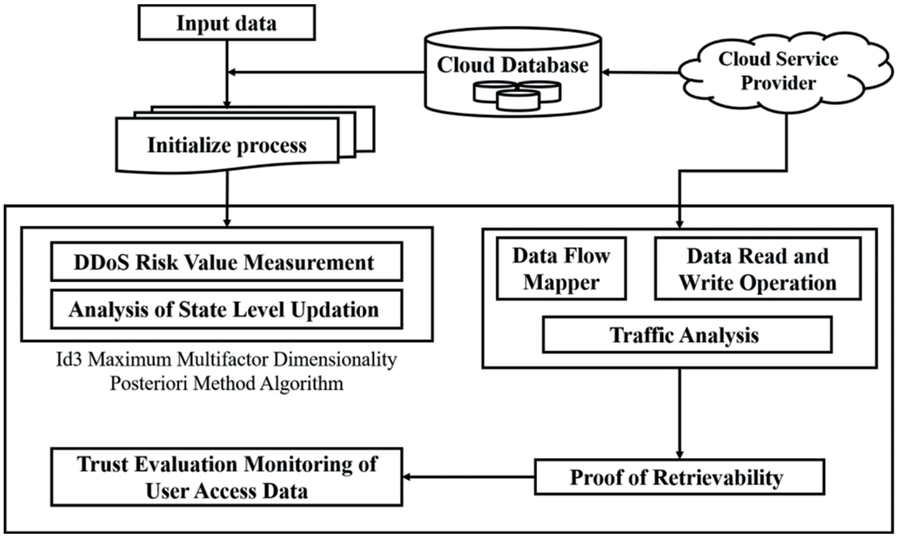
Input data
Cloud Database
Cloud Service Provider
Initialize process
DDoS Risk Value Measurement
Analysis of State Level Updation
Id3 Maximum Multifactor Dimensionality Posteriori Method Algorithm
Data Flow Mapper
Data Read and Write Operation
Traffic Analysis
Trust Evaluation Monitoring of User Access Data
Proof of Retrievability

Figure 1: Proposed system block diagram

3.1 *Risk Value Measurement*

A risk indicator measures the potential impact of a threat on the probability that a particular property will occur. It provides valuable information to assess the overall security status of cloud computing. There is no fixed allocation to the expected risk of each event. It has an initial value that can transform into a show and connect with other dynamics. The proposed system logically activates the communication machine, i.e., the rule tree used. The engine uses Eq. (1) to define the risk value of the warning trigger whenever the panel increases with each other, and the risk level is greater than or equal to one:

$$\text{RiskR} = (\text{Assert Value} * \text{assert priority} * \text{Detection Reliability})/\text{Fn} \tag{1}$$

where

Av-(Assert Value) Value of DDoS resource

Ap-(assert priority) the method of setting the value of shooting shots after a dangerous alert is accepted according to the average

Dr-(Detection Reliability)/) The probability of a contact level DDoS having a limited attack is

Fn-Normalize factor standard defined by the administrator in IDS configuration

Analysis of state Level Updation

Step1: Assuming that the cloud system can be moduled by N number of different states N = {n1, n2,…nn}

Step2: Define the security states S = {s1, s2, s3…sn} and also these states change over time S = {s1, s2, s3…sn} where Sn∈N.

Step3: The system is tracked by S host H-based s and generates observation of most messages coming from H symbol set $H^t m$ m = {m1, m2,…mn} where m∈ H^t

Step4: It's an empty team that gathers final release possibilities. It describes the severity of each warning in a definite state. These values should be calculated on the basis that the alarm intensity will be allocated to sources that are not functionally based.

$$\text{S} = (m^n * H^t * N^n * \text{Ap})$$

Step5: Define cloud entities E and their resource level

$$E = \sum_{n-1}^{n} \lambda E$$

// where m is the number of messages that is denoted as m = m1, m2, m3…mn

(L, M, H, V) The predictive intensity is then compared to one of the four priorities that will reflect the system's state, as we have explained in the ID3-MMDP.

3.2 *Traffic Analysis*

The previously transferred data of the transformation field of some neighbors and incremental address data for each state S are addressed. Cloud server extracted transition field is calculated by the transition path set and the records in the database cloud. Before the data is forwarded to its destination, the transfer data of each S will have a transfer address field and its address field.

Traffic analysis algorithm steps:

Step1: Analyze the number of S and traffic log T_{log}

Step2: Identify the route source SA and destination DA, data D

```
Step3: Data. size () to apply each data to identify the size and number of data
Step4: If P == original data then
            To identify the SA = $P_{(SA.Address)}.xxx.xxx.xxx.xxx$,
    DA = $P_{(DA.Address)}.(xxx.xxx.xxx.xxx)$
    Transmission time sequence Ts = Current time.
            Transmission Range Tr = $P_{(Tr.Address)}.(xxx.xxx.xxx.xxx)$
$T_{log} = \left( \sum_{i=o}^{p} \{ P_{(DA.Address)} \cdot (xxx.xxx.xxx.xx(i)) | P_{(SA.Address)} \cdot (xxx.xxx.xxx.xx(i)), +\text{Ts} + \text{Tr} \} \right)$    (2)
            End if
Step5: Go to step3.
Step6: Stop.
```

3.3 Trust Evaluation Monitoring of User Access Data

Data access to data failures caused by individual events can flow into web mining applications in large distributed systems. Therefore, it suggests a reliable service-oriented planning algorithm for data flow reliability to indicate service. The general belief that directs trust is defined as a trust which is as follows:

$$Trust_i = Ts_i * \ D(T_r) + \quad (1 - \quad Ts_i) * R(U_i) \tag{3}$$

$D(U_i)$ a direct belief in the service i^{th} through history-based experiences using the service by users. Recommendation trust $R(U_i)$ denoted by the Service among other users. It can calculate as follows, the service, direct trust recommended weight of trust W_i Denote:

$$W_i = 1 - \frac{1}{k}(2) \tag{4}$$

where k denotes the number of times of the i^{th} service. The credit rating is that transmission and data storage and data read/write times are the best, and data stream errors are very time-consuming.

4 Result and Discussion

The proposed ID3-MMDP has been implemented using the simulation tool visual studio and the programming language .Net. .Net will support both window and web applications. Id3 Maximum Multifactor Dimensionality Posteriori Method (ID3-MMDP) algorithm is used to classify the data representing network traffic flows, including standard and Distributed Denial of Service (DDoS) traffic.

Above Tab. 1 shows the proposed ID3-MMDP, which needs the resources. This section is compared to the proposed ID3 (Iterative Dichotomiser 3) Maximum Multifactor Dimensionality Posteriori Method (ID3-MMDP), and existing Ad boost Shuffled Leaping Optimal Selection (ASLOS) enhanced history-based IP filtering scheme (eHIPF), Naive Bayes, and Fuzzy Logic System (FLS) methods.

Fig. 2 shows the systematic analysis of packet flow performance based on the number of traffic that occurs. The previous eHIPF provides 154 with ms, Naïve Bayes provides 165 with ms, and FLS provides 172 with ms, ASLOS provides 132 with ms, and the proposed ID3-MMDP provides 124 with ms.

Tab. 2 shows the classification accuracy level. Accuracy refers to the number of intruder instances to detect divided by the number of intruder instances present in the dataset.

Table 1: Simulation parameter

Parameter	Value
Tool name	Visual studio 2012
Front end	Asp.Net
Back end	SQL (Structured Query Language)
Total number of data's	1200

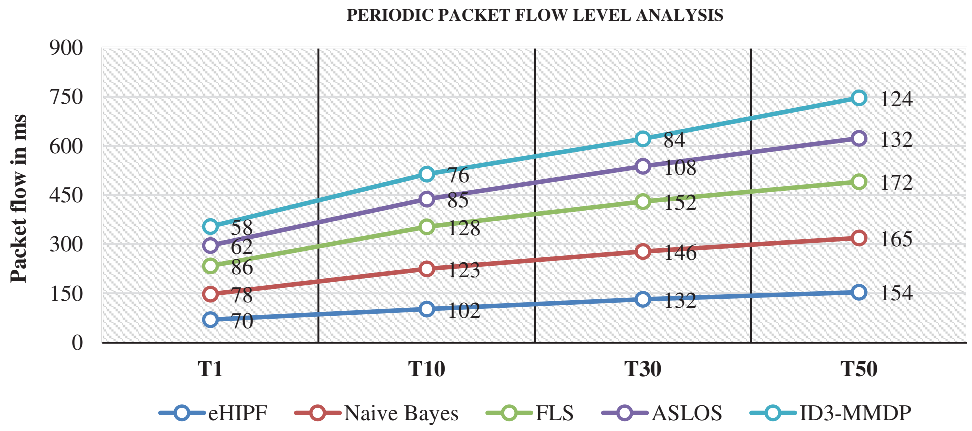

Figure 2: Periodic analysis of packet flow

Table 2: Analysis of accuracy

Algorithm	eHIPF	Naïve Bayes	FLS	ASLOS	ID3-MMDP
Analysis of accuracy in %	62	71	79	85	88

The formula to estimate the Accuracy is,

$$\text{Accuracy} = \frac{Number\ of\ intrusion\ detected}{Total\ number\ of\ intrusion\ present} * 100 \tag{5}$$

Above Fig. 3 shows that the DDoS dataset classification accuracy level is compared with existing methods, and the proposed ID3-MMDP gives better accuracy than the previous systems.

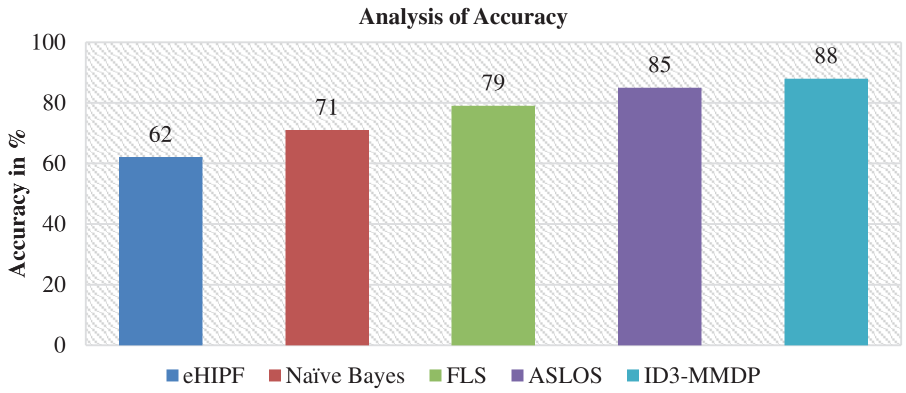

Figure 3: Analysis of accuracy

Fig. 4 shows the metric values during the attack time analysis. The attack time index is higher than today, but the attack power is high in the standard time, and the packet rate index is higher than the existing methods.

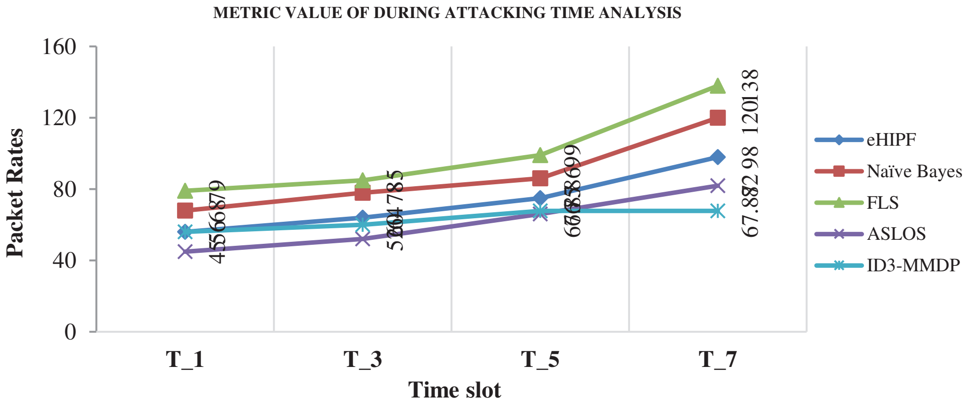

Figure 4: Metric value of during attacking time analysis

The above Fig. 5 presented about the analysis of risk evaluation speed is compared with the previous and proposed method. Hence the proposed ID3-MMDP gives better results compared with other methods.

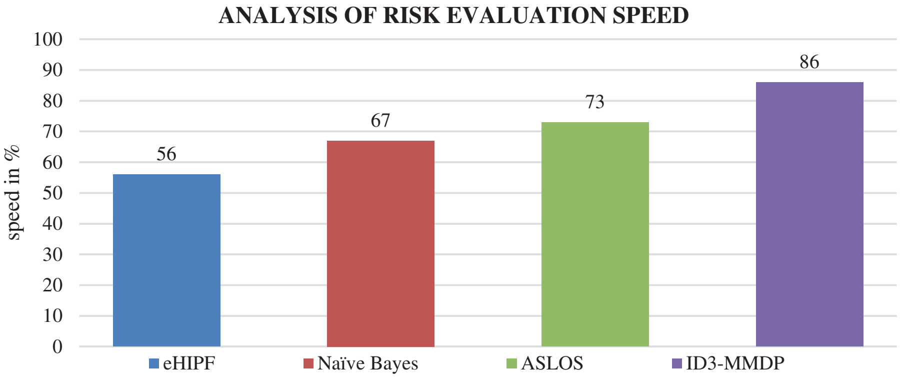

Figure 5: Analysis of risk evaluation speed

5 Conclusion

DDoS attack in the cloud differs from other attacks on infrastructure in fixed application space. A comprehensive introduction to attack methods, results and attack intensity has not been given. This novel approach is an attempt to explore the task and design infrastructure to facilitate the collection of essential requirements for the DDoS Cloud. These requirements include optimization of the five critical factors in the director attack. Experiences of this type have shown that combat against DDoS attacks in a cloud environment with pure transport filtration is not sufficient. ID3-MMDP recommends minimizing damage and availability when considering stabilization, collaboration, resource management, and dealing with DDoS attacks in cloud computing. ID3-MMDP provides a multi-level flow-based warning collaboration DDoS detection solution framework to effectively design effective mitigation solutions. The proposed ID3-MMDP gives the periodic analysis of parameters. It indicates that the packet flow is 124 with ms, accuracy is 88%, and metric value during attacking time analysis is 67.87 packet rate, analysis of risk evaluation speed is 86%.

Funding Statement: The authors received no specific funding for this study

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] K. Hong, Y. Kim, H. Choi and J. Park, “SDN-assisted slow HTTP DDoS attack defense method,” *IEEE Communications Letters*, vol. 22, no. 4, pp. 688–691, 2018.

[2] J. A. Pérez-Díaz, I. A. Valdovinos, K. K. R. Choo and D. Zhu, “A flexible SDN-based architecture for identifying and mitigating low-rate DDoS attacks using machine learning,” *IEEE Access*, vol. 8, pp. 155859–155872, 2020.

[3] Z. A. E. Houda, A. S. Hafid and L. Khoukhi, “Cochain-SC: An intra-and inter-domain DDoS mitigation scheme based on blockchain using SDN and smart contract,” *IEEE Access*, vol. 7, pp. 98893–98907, 2019.

[4] B. Dhiyanesh, S. Sakthivel, R. Radha and S. S. Kumar, “Threshold based DDoS mitigation with fog layer in cloud environment,” *J. Ambient Intell Human Comput*, vol. 12, pp. 7039–7050, 2020.

[5] S. Dubey and S. Agrawal, “QoS driven task scheduling in cloud computing,” *International Journal of Computer Applications Technology and Research*, vol. 2, no. 5, pp. 595–600, 2013.

[6] A. Praseed and P. S. Thilagam, “Multiplexed asymmetric attacks: Next-generation DDoS on HTTP/2 servers,” *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1790–1800, 2020.

[7] D. Erhan and E. Anarim, “Hybrid DDoS detection framework using matching pursuit algorithm,” *IEEE Access*, vol. 8, pp. 118912–118923, 2020.

[8] S. Dong and M. Sarem, “DDoS attack detection method based on improved KNN with the degree of DDoS attack in software-defined networks,” *IEEE Access*, vol. 8, pp. 5039–5048, 2020.

[9] S. Kasthuripriya, B. Dhiyanesh and S. Sakthivel, “LFTSM-local flow trust-based service monitoring approach for preventing the packet during data transfer in cloud,” *Asian Journal of Information Technology*, vol. 15, pp. 3927–3931, 2016.

[10] A. Alsirhani, S. Sampalli and P. Bodorik, “DDoS detection system: Using a set of classification algorithms controlled by fuzzy logic system in apache spark,” *IEEE Transactions on Network and Service Management*, vol. 16, no. 3, pp. 936–949, 2019.

[11] Z. Liu, Y. Cao, M. Zhu and W. Ge, “Umbrella: Enabling ISPs to offer readily deployable and privacy-preserving DDoS prevention services,” *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 4, pp. 1098–1108, 2019.

[12] H. Lin, S. Cao, J. Wu, Z. Cao and F. Wang, “Identifying application-layer DDoS attacks based on request rhythm matrices,” *IEEE Access*, vol. 7, pp. 164480–164491, 2019.

[13] A. Praseed and P. S. Thilagam, “Modelling behavioral dynamics for asymmetric application layer DDoS detection,” *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 617–626, 2021.

[14] B. Dhiyanesh and S. Sakthivel, “Secure data storage auditing service using third party auditor in cloud computing,” *IJAER International Journal of Applied Engineering Research*, vol. 10, no. 37, pp. 28037–28044, 2015.

[15] A. Praseed and P. S. Thilagam, “DDoS attacks at the application layer: Challenges and research perspectives for safeguarding web applications,” *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 661–685, 2019.

[16] L. Zhou, K. Sood and Y. Xiang, “ERM: An accurate approach to detect DDoS attacks using entropy rate measurement,” *IEEE Communications Letters*, vol. 23, no. 10, pp. 1700–1703, 2019.

[17] B. Dhiyanesh, “Dynamic resource allocation for machine to cloud communications robotics cloud,” in *2012 Int. Conf. on Emerging Trends in Electrical Engineering and Energy Management (ICETEEEM)*, Chennai, India, pp. 451–454, 2012.

[18] Y. Gu, K. Li, Z. Guo and Y. Wang, "Semi-supervised K-means DDoS detection method using hybrid feature selection algorithm," *IEEE Access*, vol. 7, pp. 64351–64365, 2019.

[19] K. Huang, L. Yang, X. Yang, Y. Xiang and Y. Y. Tang, "A low-cost distributed denial-of-service attack architecture," *IEEE Access*, vol. 8, pp. 42111–42119, 2020.

[20] B. Dhiyanesh and K. S. Sathiyapriya, "Image inpainting and image denoising in wavelet domain using fast curve evolution algorithm," in *2012 IEEE Int. Conf. on Advanced Communication Control and Computing Technologies (ICACCCT)*, Ramanathapuram, India, pp. 166–169, 2012.