Research Article

International Journal of Advanced Computer Research, Vol 6(27)
ISSN (Print): 2249-7277 ISSN (Online): 2277-7970
http://dx.doi.org/10.19101/IJACR.2016.626020

The conjectural framework for detecting DDoS attack using enhanced entropy based threshold technique (EEB-TT) in cloud environment

A. Manimaran[1*] and M. Durairaj[2]
Research Scholar, School of Computer Science, Engineering and Applications, Bharathidasan University, Tiruchirappalli, India[1]
Assistant Professor, School of Computer Science, Engineering and Applications, Bharathidasan University, Tiruchirappalli, India[2]

Received: 30-June-2016; Revised: 16-September-2016; Accepted: 23-September-2016

Abstract
A major threat to cloud infrastructure network is distributed denial of service (DDoS) attacks. It makes the resources unavailable for its anticipated users, which can be accomplished through malicious virtual machines (VMs) in a hypervisor layer of cloud datacenter. Less protection in VMs leads to DDoS attacks on cloud environment. Traditional approaches used data flow based method, but that is not efficient for attack detection in distributed cloud environment. In a cloud environment, malicious tenants use the cloud resources to initiate DDoS attacks at cloud datacenter level. This paper proposes a theoretical framework of entropy information theory based attack detection method, which is based on finding probability distribution of malicious VMs attributes to effectively address this issue.

Keywords
DDoS attack, Resource availability, Cloud computing, Datacenter, Entropy information theory.

1.Introduction
Cloud Computing provides broad network access to distributed resources. The power of the cloud computing is resource sharing in a distributed environment across the virtual machines [1]. The cost for resource sharing generally depends upon the usage and demand. Therefore, cloud providers achieve better resource utilization through statistical multiplexing using on-demand computing model. The cloud users need not pay extra amount for resource over-provisioning by using dynamic scaling [2]. DDoS attacks have been a key challenge to the researchers and significant security issue to the cloud computing environment [3, 4]. DDoS attackers can send huge number of forged requests from many zombie computers to the cloud server for making cloud resource unavailable. DDoS attacker's intention is to reduce the cloud server's resource capacity and denial the resource to the legitimate users [5]. To instigate DDoS attacks, attackers take advantage of cloud datacenter vulnerabilities that resides in its VMs computation, storage, and network resources [6].

In information theory, entropy is a measure of the uncertainty related to a random variable, which is used to analyze the data and detect the attackers [7]. The VMs attributes are correlated to apply entropy information theory to detect the malicious users. VMs attributes are network usage, CPU usage, memory usage, and disk IO usage. Based on these attributes status pattern, this work proposes a novel framework for detecting DDoS attacks. Legal VMs reveal the similar status patterns and malicious VMs disclose the similar status patterns in a cloud server [8]. Using this technique, malicious VMs are identified and relevant attack behaviors are discovered by applying entropy information theory. This paper proposes a novel framework for DDoS attack detection in the cloud datacenter based on four tiers, namely cloud infrastructure, cloud infrastructure management, attack detection, and administrator management.

2.Mechanisms to address DDoS attacks
Chen et al. [9] designed a rule based detection mechanism against distributed denial of service attacks. This mechanism consists of two modules: detection and response, which identify the network traffic with suspicious behavior. Detection phase notices the flow aggregation with arrival rate to

*Author for correspondence

identify overloading behavior. Response module has three parts to discard the malicious traffic; they are attackers, monitoring server, and victim host. The system performance analysis proves the following criteria: minimum cost to detect the attack traffic, reduce false positive and false negative rate, and maximum resource utilization. The main drawback of this mechanism combines threshold value which is not suitable for high-speed network.

VM profile based optimized network attack pattern detection scheme was proposed by Gupta et al. [10]. Proposed method works based on rule based and threshold based approach to detect DDoS attacks on cloud environment. It creates individual profiles for each VM and for all possible attack patterns (rule based) and classifies the network traffic from different VM's in the cloud. Patterns on VM profile and threshold values can be checked for detecting spoofed packets. Pattern rules are the number of packets (N) and the repetition value of the pattern (M) used to gain the correct network behavior of a rule. The drawback of this method is not concentrating on other DDoS attack methods except the transmission control protocol (TCP) synchronization (SYN) flood attack.

Singh et al. [11] proposed threshold based approach to detect DDoS attack in cloud computing. In this approach, the normal behavior and abnormal behavior methods to detect DDoS attack were analyzed. Signature based and anomaly based DDoS mechanisms were introduced with the use of dynamic and multi threshold based algorithmic approach.

Shin et al. [12] designed a new probabilistic approach called advanced probabilistic approach for network intrusion (APAN) to forecast possible attacks. The techniques k-means clustering and Markov chain model are used to identify potential attacks. K-means clustering is used for classifying network states and Markov chain is for classifying probabilistic model. The network outlier factor is to determine incoming anomaly traffic and the proposed system tested with entropy of source IP, port addresses and destination IP, port addresses.

Ahmed et al. [13] discussed the types of network denial of service attacks and also classified the methods of security defenses, then compared each method. Challenges of cloud server prevention of DDoS attack have been clearly explained and solutions were given. Machine learning based DDoS attack detection and prevention mechanisms for cloud environment was mentioned and explained. They concluded that the cloud security is based on the three schemes detecting attacks, monitoring/ identifying attack, and filtering to discard attack.

Prasad et al. [14] developed a framework using an entropy based approach to detect DDoS attacks. This has numerous hops prior to the victim and traces the source of attack by manipulating the entropy at each monitor in the threat monitoring system.

Jun et al. [15] proposed a methodology based on traffic volume and entropy of packet header fields which can together work and filter the malicious packets to detect DDoS attacks. Primarily traffic volume information is used for initial detection process and if the traffic volume exceeds the threshold value, then entropy technique is applied to discover the number of packets per second received from the suspicious flows.

Jeyanthi et al. [16] developed entropy based mechanism to detect and discriminate DDoS attacks from flash events approach. The entropy based approach is well suited for differentiating legal users and attackers. This work validated the usefulness of the entropy based DDoS flash crowds.

3.Novel framework for DDoS attack detection

The enhanced entropy based threshold technique (EEB-TT) DDoS attack detection system is proposed in this work, which is divided into four tiers that are cloud infrastructure tier, cloud infrastructure management tier, attack detection tier, and cloud administrator management tier. Cloud Infrastructure tier is the essential to offer cloud services to the users and it is monitored by administrators. Cloud infrastructure management tier oversees the VMs management, system image management, and cloud network management. Core part of the detection system is attack detection tier, which enables the EEB-TT algorithm to detect the malicious VMs in an efficient manner. Administrator management tier supervises the cloud network administrators and it is responsible for providing Application Programming Interfaces (APIs) for cloud tenant and virtual machine management. The overall framework of the proposed work is shown in *Figure 1*.

Attack detection tier is divided into three modules namely, VM status gathering modules, namely, attack identify module, and cloud control module. Initially, in VM status gathering module, the attributes are

CPU usage, IO usage, Memory usage, and network throughput. These attributes, details are gathered and stored in the VM status database. Cloud infrastructure management tier consists of log audit module and VM status database communicates with the log audit module through standard remote procedure call interface. In order to filter out the idle VMs, each and every VMs status is retrieved from log audit module and check whether the VMs IO, CPU usage, Memory usage, and Network throughput are low, then discard those VMs status and store rest of the VMs status into the VMs status database. In *Figure 2*, the flow for VM status gathering is depicted.

Second module named as attack identify module, query the VMs status from the VMs status database and applies proposed entropy detection algorithm called enhanced entropy based threshold algorithm (EEB-TA) to calculate the entropy value for cloud datacenter. This module preserves entropy queue for dynamically update the entropy value in the entropy queue by replacing the entropy value when the latest entropy comes in, the oldest entropy leaves the queue. The entropy queue plays a role of slide window and verifies the distribution of entropy variables. Set the dynamic threshold value to discard the malicious VMs and based on the entropy value in the slide window dynamically change the threshold value for attack detection efficiency. To detect DDoS attack, check the entropy value in the slide window, if the entropy value is less than the threshold value, then it will be considered as a legitimate VM otherwise it will be considered as malicious VM. The attack detection result is reported to the cloud control module. This is shown in *Figure 3*.

The algorithm for our proposed framework is as given below.

Algorithm:
Input: *VM Resources*
Output: *Classify VM as legal or malicious*

// VM status gathering
Step 1: Gather virtual machine Status
Step 2: Retrieve resources from the virtual machine database
Step 3: Store the resources in the virtual machine status database
Step 4: Check whether the VM is Idle
    Go to step 5
  Else
    Go to step 7
Step 5: VM is identified Idle
Step 6: Ignore the VM
Step 7: Store the detail of active VM in VM database

// Attack identification
Step 8: Retrieve the active VM resources from VM database
Step 9: Apply entropy detection algorithm to find the entropy value
Step 10: Store entropy value in entropy queue
Step 11: Check if entropy value is greater than the threshold value
    Go to Step 12
  Else
    Go to Step 14.
Step 12: Identified as the attacker
Step 13: The attacker information is stored
Step 14: User is legal.
Step 15: Legal user detail is stored in the cloud datacenter.

// Cloud controller
Step 16: Retrieve attack information.
Step 17: Retrieve the entropy value of the attacker.
Step 18: Apply administration policies to store the entropy value.
Step 19: Store the detail in the admin database
Step 20: Process is stopped

Finally, cloud control module exploits based on the results obtained from entropy detection. This module retrieves the detection result from the attack identify module and it applies administrative policies based on the obtained results. All the communications are persuaded through remote procedure call (RPC) presented by cloud infrastructure tier. Finally, it reports the detection result to the administrator management tier as shown in *Figure 4*.

4.Conclusion and future work

DDoS attacks detection techniques which are available today has a number of drawbacks. Detecting such kind of attack threats at earlier stage improve the resource availability. Hence, this paper proposed an EEB-TT framework for detecting DDoS attacks on cloud environment. This paper studied the possibility of DDoS attack using information entropy to discover the attack with the idea of similarity among VMs status patterns. The proposed EEB-TT framework is a technique which detects DDoS attacks and directs the cloud datacenters to distribute the workload among different VMs equally by applying information entropy. The future direction of this work is experimenting the same framework in the cloud environment and observe whether the

results obtain can satisfy the requirement to secure the Cloud in order to increase the resource availability.

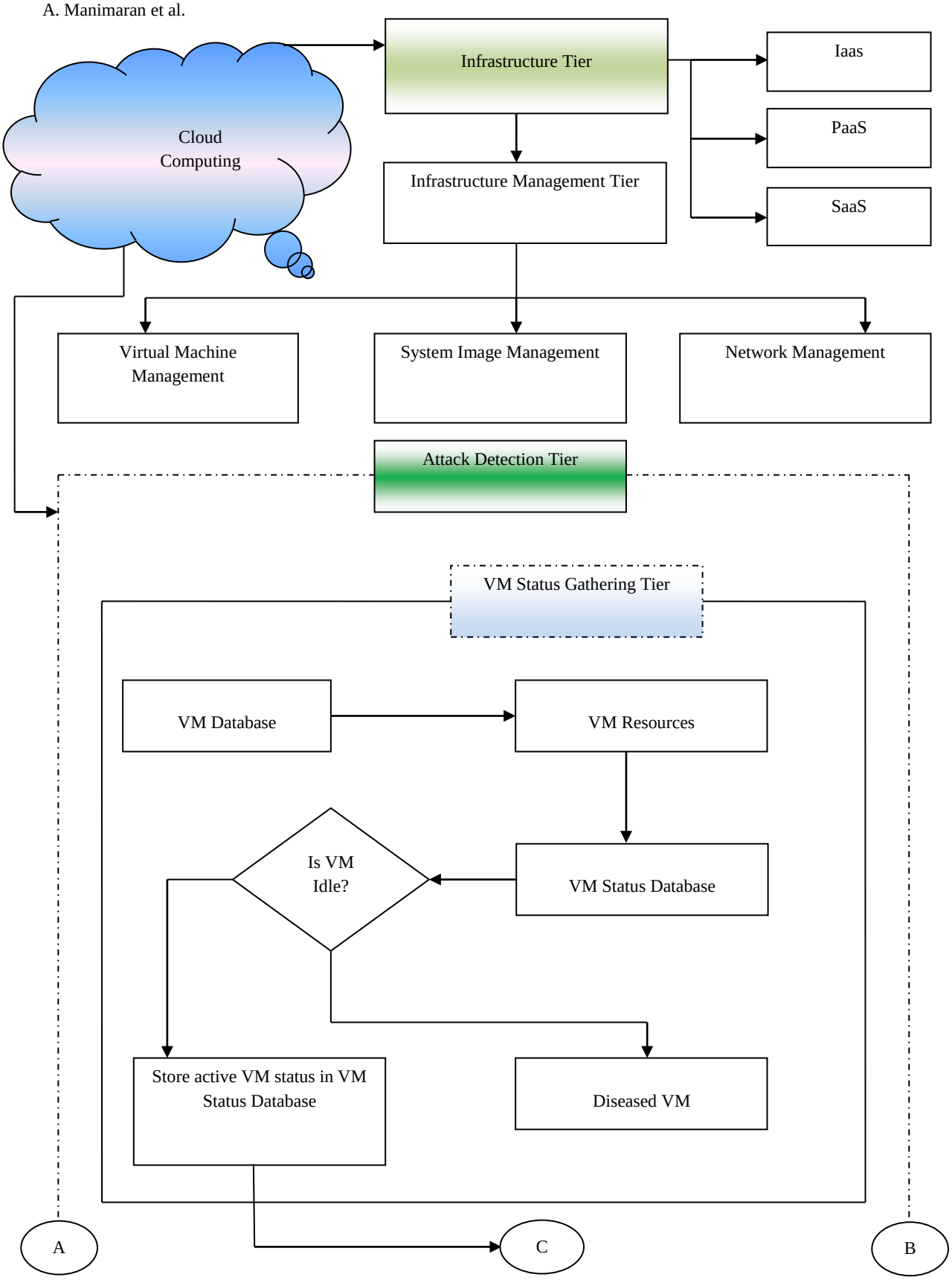
Acknowledgment
None.

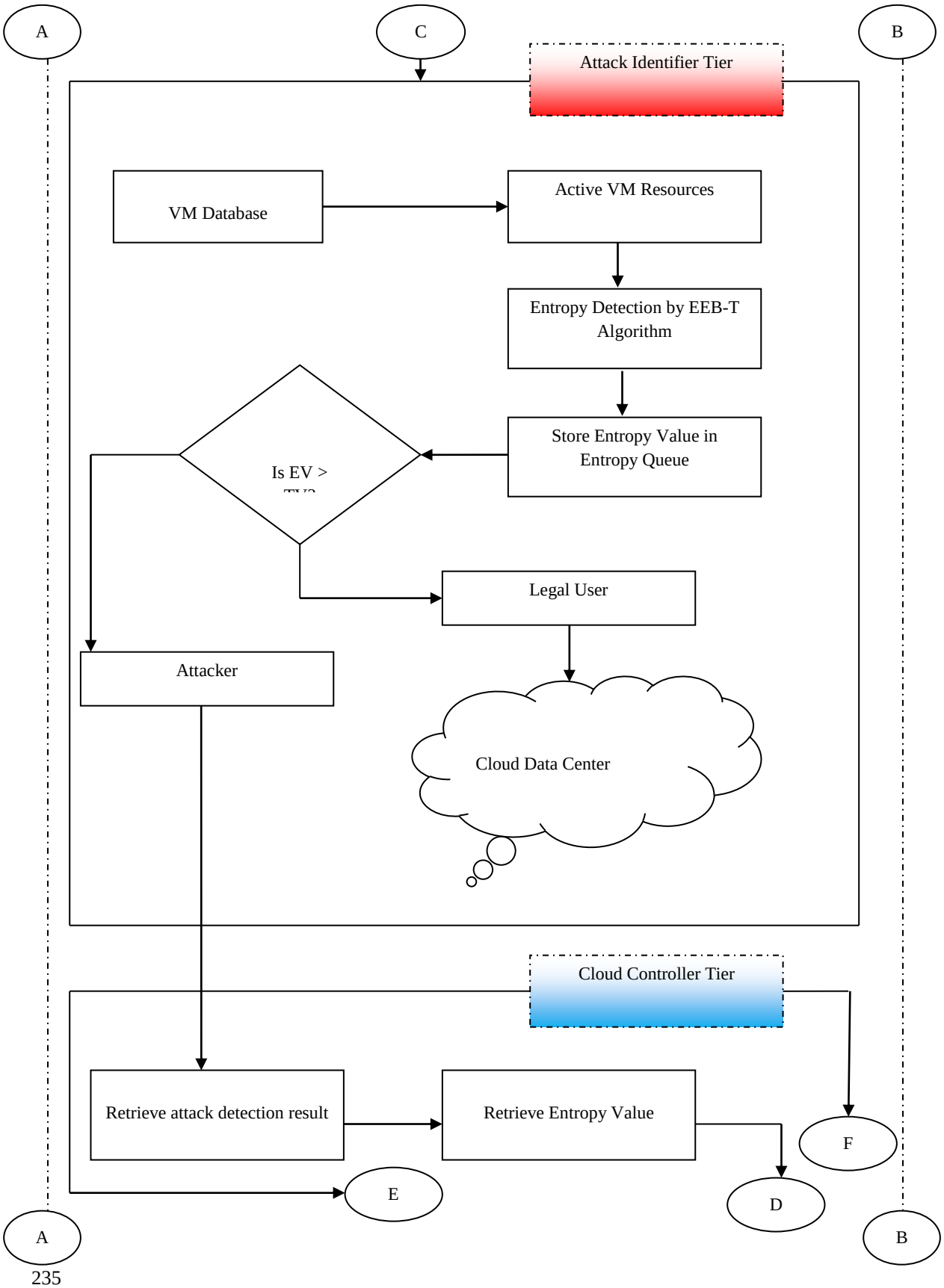
Conflicts of interest
The authors have no conflicts of interest to declare.

References
[1] Durairaj M, Manimaran A. A study on securing cloud environment from DDoS attack to preserve data availability. The International Journal of Science and Technoledge.2015; 3(2):63-72.
[2] Mustafa S, Nazir B, Hayat A, Madani SA. Resource management in cloud computing: Taxonomy, prospects, and challenges. Computers & Electrical Engineering. 2015; 47: 186-203.
[3] Girma A, Garuba M, Li J, Liu C. Analysis of DDoS attacks and an introduction of a hybrid statistical model to detect DDoS attacks on cloud computing environment. In 12th international conference on information technology-new generations (ITNG) 2015 (pp. 212-7). IEEE.
[4] Durairaj M, Manimaran A. An Extemporized confidence based filtering technique to mitigate DDoS attack in cloud environment. International Journal of Control Theory and Applications. 2015; 8(5):2405-13.
[5] Durairaj M, Manimaran A. Theoretical framework of TCP SYN flood DDoS attack detection mechanism using spoofed IP in cloud environment. International Journal of Emerging Technologies in Computational and Applied Sciences. 2015; 13(1): 42-8.
[6] Durairaj M, Kannan P. A study on virtualization techniques and challenges in cloud computing. International Journal of Scientific &Technology Research. 2014; 3(11):147-51.
[7] Liu T, Wang Z, Wang H, Lu K. An entropy-based method for attack detection in large scale network. International Journal of Computers Communications & Control. 2014; 7(3):509-17.
[8] Somani G, Gaur MS, Sanghi D, Conti M, Buyya R. DDoS Attacks in cloud computing: Issues, Taxonomy, and Future Directions. ACM Computing Surveys. 2015; 1(1): 1-44.
[9] Chen CL, Chen HC. A rule-based detection mechanism against distributed denial of service attacks. In the third international conference on digital enterprise and information systems (DEIS2015) 2015 (pp. 38-45).
[10] Gupta S, Kumar P. VM profile based optimized network attack pattern detection scheme for DDoS attacks in cloud. In international symposium on security in computing and communication 2013 (pp. 255-61). Springer Berlin Heidelberg.
[11] Singh B, Panda DS, Samra DG. Threshold based approach to detect DDoS attacks in cloud. International Journal of Innovative Research in Information Security. 2014; 3(2):22-8.
[12] Shin S, Lee S, Kim H, Kim S. Advanced probabilistic approach for network intrusion forecasting and detection. Expert Systems with Applications.2013; 40(1):315-22.
[13] Ahmed ES, Elatif RE. Network denial of service threat security on cloud computing a survey. International Journal of Scientific Research in Science, Engineering and Technology. 2015; 1(5):341-50.
[14] Prasad KM, Reddy AR, Rao KV. An efficient detection of flooding attacks to Internet threat monitors (ITM) using entropy variations under low traffic. In computing communication & networking technologies (ICCCNT), 2012 third international conference on 2012 (pp. 1-11). IEEE.
[15] Jun JH, Ahn CW, Kim SH. DDoS attack detection by using packet sampling and flow features. In proceedings of the 29th annual ACM symposium on applied computing 2014 (pp. 711-2). ACM.
[16] Jeyanthi N, Iyengar NC. An entropy based approach to detect and distinguish DDoS attacks from flash crowds in VoIP networks. International Journal of Network Security. 2012; 14(5):257-69.

Manimaran. A is currently a PhD research scholar, School of Computer Science, Engineering and Applications, Bharathidasan University, Trichy, Tamilnadu, India. He has three years teaching experience and his research interests include network security, cloud computing and cloud security. He has published 5 research articles in international journals.
Email: manimaranbdu@gmail.com

Dr. M. Durairaj is an Assistant Professor in School of Computer Science, Engineering and Applications, Bharathidasan University, Tiruchirappalli, Tamilnadu. He completed his Ph.D. in Computer Science as a full time research scholar at Bharathidasan University on April, 2011. Prior to that, he received a master's degree (M.C.A.) in 1997 and bachelor degree (B.Sc. in Computer Science) in 1993 from Bharathidasan University. His Ph.D. work was to study different possibilities and device a methodology for hybridizing two Machine-learning techniques for making an effective prediction system for processing clinical / medical data. At present, he is Assistant Professor in Computer Science at Bharathidasan University, prior to this he was Research Associate at National Research Centre on Rapeseed-Mustard (Indian Council of Agricultural Research) for 12 years. He has 70 publications to his credit. His area of research includes Data Mining, Soft Computing, Cloud Computing and Big Data Analytics.


Cloud Computing
Infrastructure Tier
Iaas
PaaS
SaaS
Infrastructure Management Tier
Virtual Machine Management
System Image Management
Network Management
Attack Detection Tier
VM Status Gathering Tier
VM Database
VM Resources
Is VM Idle?
VM Status Database
Store active VM status in VM Status Database
Diseased VM
A
C
B


A
C
B
Attack Identifier Tier
VM Database
Active VM Resources
Entropy Detection by EEB-T Algorithm
Store Entropy Value in Entropy Queue
Is EV >
Legal User
Attacker
Cloud Data Center
Cloud Controller Tier
Retrieve attack detection result
Retrieve Entropy Value
F
E
D
A
B

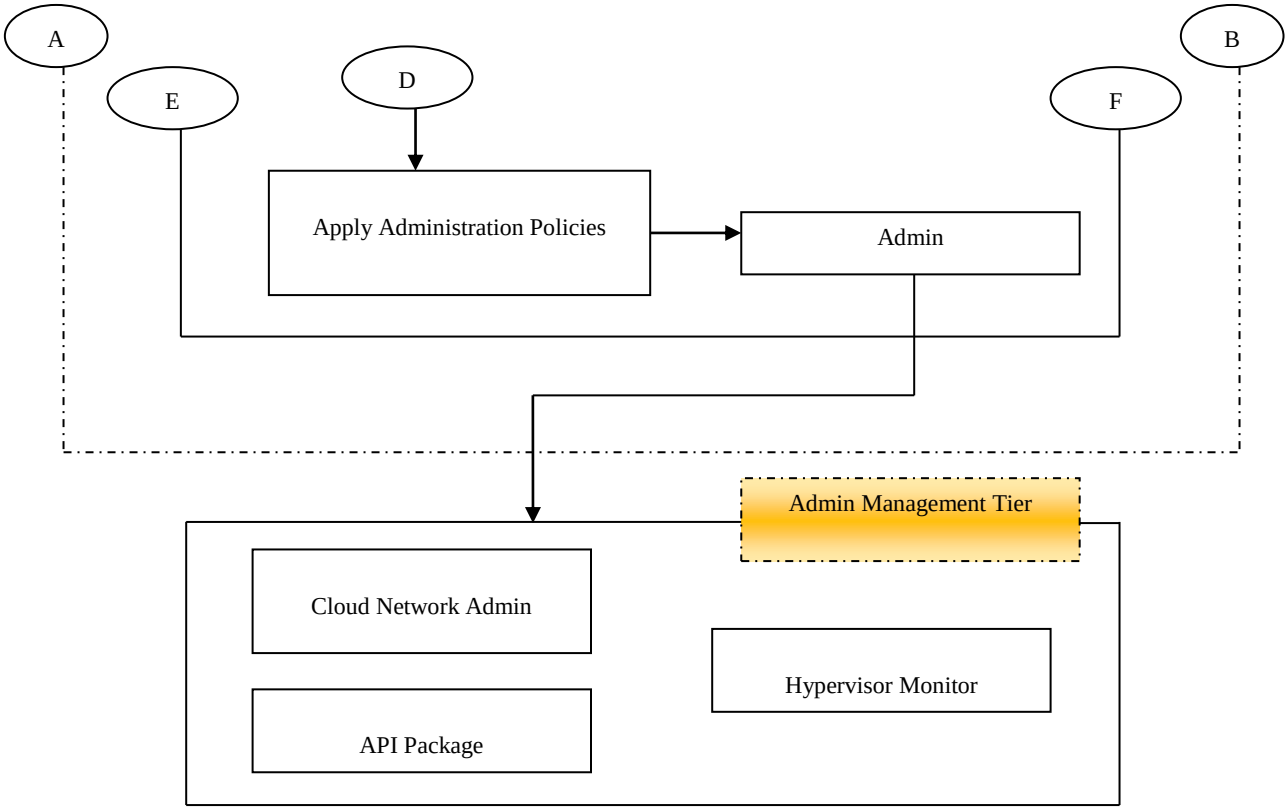


Figure 1 Overall architecture for EEB-TT

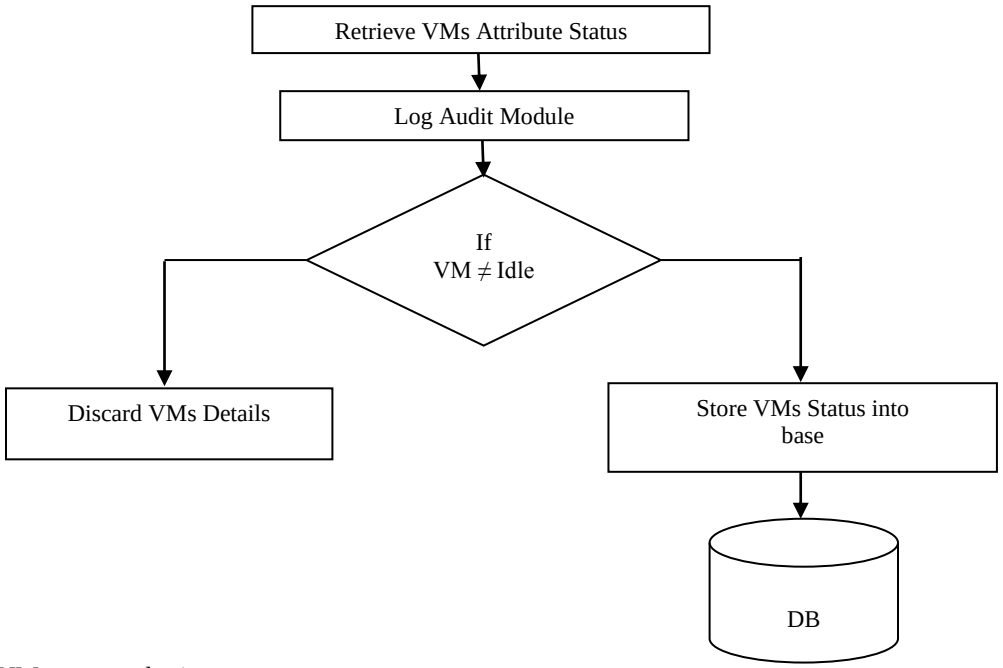


Figure 2 VM status gathering

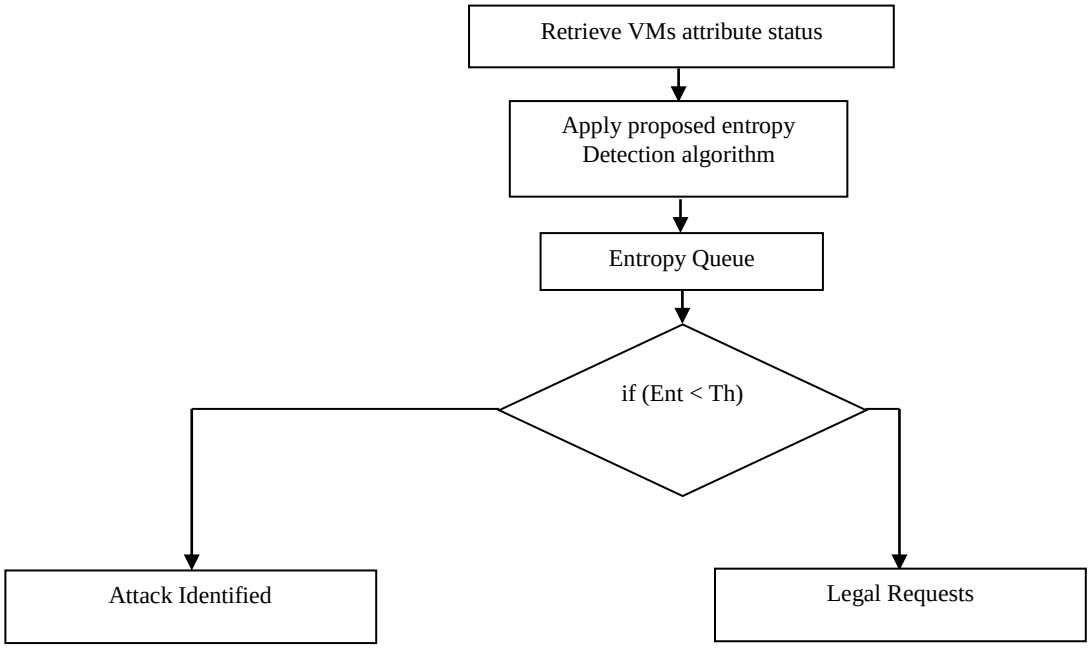


Figure 3 Attack detection module

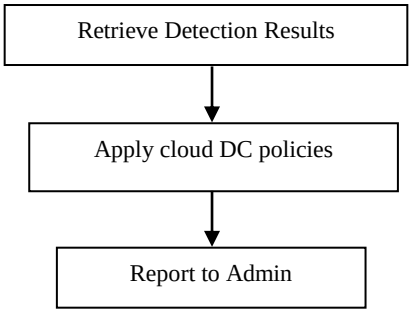


Figure 4 Cloud control module