Cluster Comput (2019) 22:S13027–S13039
https://doi.org/10.1007/s10586-017-1187-7

Enhanced intrusion detection and prevention system on cloud environment using hybrid classification and OTS generation

V. Balamurugan[1] · **R. Saravanan**[2]

Received: 28 June 2017 / Revised: 30 August 2017 / Accepted: 11 September 2017 / Published online: 21 September 2017
© Springer Science+Business Media, LLC 2017

Abstract Cloud environment is an assembly of resources for furnishing on-demand services to cloud customers. Here access to cloud environment is via internet services in which data stored on cloud environment are easier to both internal and external intruders. To detect intruders, various intrusion detection systems and authentication systems was proposed in earlier researches which are primarily ineffective. Many existing researchers were concentrated on machine learning approaches for detecting intrusions using fuzzy clustering, artificial neural network, support vector machine, fuzzy with neural network and etc., which are not furnishing predominant results based on detection rate and false negative rates. Our proposed system directed on intrusion detection system and it uses cloudlet controller, trust authority and virtual machine management in cloud environment. We propose two novel algorithms such as (i) *packet scrutinization algorithm* which examines the packets from the users and (ii) hybrid classification model called "NK-RNN" which is a combination of *normalized K-means* clustering algorithm with *recurrent neural network*. For preventing the user from intruders, we propose a *one time signature* for cloud user in order to access the data on cloud environment. Our proposed classifier effectively detects the intruders which are experimentally proved by comparing with existing classification models. Thus our proposed results are expressed by packet loss ratio, average packet delay, throughput, detection rate, false positive rate and false negative rate.

Keywords Cloud computing · Cloudlets · Queue modeling · IDS · RNN classifier · Flood attacks · DDOS · U2R attacks · Zero day attacks and R2L attacks

1 Introduction

Nowadays, information on computing is one of the assets for all organizations by utilizing local network to present available internet services with distributed storage that makes simple tasks for accessing. Introduction of cloud computing involves easy maintenance of information based on offering an open architecture by molding more attention to several intruders or attackers. An intrusion outlines the attempt for compromising the Confidentiality, Integrity and Availability (CIA) of a computer or network or the larger environment like cloud. IDS is composed of various elements which are used for identification and detection of the malicious activity. IDSs are categorized into two types: signature based and anomaly based. Anomaly based IDS method detects the new types of intrusions whereas signature based method detect attacks and compare the capture patterns with original patterns [1]. This cloud environment has different service models such as SaaS, PaaS and IaaS with four kinds of deployment models such as Public cloud, Private cloud, Community cloud and Hybrid cloud [2]. Many corporations have eagerly begun to upload their huge important information into public cloud [3], which is more sensitive to many vulnerable security risks. Secure cloud storage permits preventing the data from malicious intruders and their advancements [2] on distributed cloud environment with secure manner. For this anti-malware [4]

✉ V. Balamurugan
vbalamuruganmsec@gmail.com

R. Saravanan
saravanandeepha@gmail.com

[1] Department of Computer Science and Engineering, Mohammed Sathak Engineering College, Kilakarai, Ramanathapuram, Tamilnadu 623 503, India

[2] Department of Computer Science and Engineering, RVS Educational Trust Group of Institution, RVS Nagar, Dindigul, Tamilnadu, India

Table 1 Attackers and their descriptions

S.no.	Attacks	Description
1	DDOS	This attack forges a few resource overloaded and declines for handling actual user requests
2	Probing	It analyses the network of computer in order to collect vulnerability information for misuse
3	U2R	This attack initially access the cloud resources as normal access and it expands its vulnerability to the root access of the system
4	R2L	This initially sends packet to a machine over the network and then captures the weakness of machines for obtaining illegitimate gaining of user access
5	Zero day attacks	This attack works as a normal cloud user and affects the whole computer programs, data and additional computers on the network.
6	Distributed attacks	This attack sends malicious emails, or spam or it can performs DDoS attacks
7	Vulnerability report	Misconfiguration and interlinked documents accessed through the Internet
8	Covert channel attacks	Storage channel attacks and timing channel attacks allows to transfer information to unauthorized person

software was proposed for detecting infectious node in cloud. This uses the virtualization technology which enables virtual machines to resettle from one physical sever to virtual server. Despite of many cloud service, intruders from various sources gain access and followed by misusing the resources and services which are furnished by Cloud Service Provider (CSP). The intruders (anomalies) may attack the end users' confidential data, utilization of CPU, bandwidth, storage and energy for processing the cloud system. In order to save user's data and cloud resource from malpractices, researchers concentrated on IDS [5–9] and firewall are the best solution for attack detections. Here firewall doesn't have capacity to detect the inside intruders and complex attacks. Cloud computing environment faces more complex and vulnerable attacks such as IP spoofing, DDOS, Port Scanning attacks, virtualization attacks, probe attacks, R2L attacks and U2R attacks [1,5,10]. Defeating the DDOS attacks in cloud environment based on analyzing the software requirement and its management was focused in software security engineering [11] and attacker evidences [12] are collected on cloud environment which involves different scenarios for efficacious identification of attackers on the cloud environment. We furnish description for the vulnerable attacks in Table 1.

Cloudlets can avoid certain unwanted inter-domain traffic and data ownership problems. Cloudlets build better resources from cloud data centers [13]. Detecting intrusions on cloud data centers [14] includes two types of techniques such as (i) rule based IDS and (ii) anomaly or behavior based IDS. Rule based detection approaches uses a built-in signatures for detecting intrusions and it may be represented as signature based IDS whereas anomaly based IDS uses the detection approaches based on comparing their traffic patterns and resource utilizations [15], there are various detection techniques that discussed in latter section. Here anomaly based detection approach is more critical due to analyzing the behavior of systems that changes take place from time to time. Anomaly based system has a major drawback which results in higher false positive rates and false negative rates. To solve these issues on anomaly based intrusion detection system, Machine Learning Algorithms (MLA) was preferred which includes classification algorithms, clustering algorithms were discussed in [5,10,16] and solves the problem of increasing false positive rates and false negative rates for detecting attacker. Authors from [5], proposed an anomaly detection system on cloud environment with combination of clustering approach and classification mechanism. This paper focuses on high frequent attacks (such as DOS attacks & flooding attacks) and low frequent attacks (such as U2R attacks and R2L attacks). Here the combination of Fuzzy C-Means (FCM) clustering and ANN was proposed for detection the accuracy and followed by higher detection rate and lower false negative rate on cloud. Thus FCM-ANN works on the basis of divide and conquer strategy.

In our proposed system, we design a novel intrusion detection system architecture with cloud environment for combating DDOS, U2R, R2L, probing and zero day attacks. Many traditional approaches involve either intrusion detection system or intrusion prevention system but our proposed system involves both intrusion detection and prevention systems with several novel algorithms. Our proposed system uses two algorithms such as PSA and Hybrid NK-RNN classification algorithm. For preventing the cloud data from intruders we allow a novel one time signature algorithm which is different from one time password systems.

We majorly contribute our proposed work as follows:

- We design our cloud computing environment with multiple cloudlets, CC, TA and VMM. First, we allow several users from an organization or elsewhere and they can move everywhere.
- Second, cloudlets are used as components that are permitted to gather packets from different users via routers

and here our CC monitors the packets from different cloudlets. Here a novel Packet Scrutinization Algorithm is used for analyzing the packets based on packet arrival time, flows, confidence levels and packet counts according to its header.
- Third, VMM has the novel Hybrid NK-RNN classification algorithm that detects several attacks on the cloud environment and it results the attacks packets and normal packets.
- Fourth, a queue modeling "M/M/C: ?/FIFO" is proposed and placed on VMM, which used for allocating the packets on VM with packet priorities.
- Fifth, we propose one time signature (OTS) generation in TA for cloud users that support prevention mechanism on cloud from intruders.
- Our proposed system works effectively by packet loss ratio, average packet delay, throughput, detection rate, false positive rate and false negative rate that are measured experimentally.

Our paper is organized with different sections: Sect. 2 illustrates preliminary models of intrusion detection system and we also discuss previous works in IDS and their concepts in Sect. 3. Section 4 deals with problems on previous works, then Sect. 5 describes the overall proposed system and its experimental analysis is concentrated in Sect. 6. At last, we conclude our proposed work in Sect. 7 and then we furnish reference papers in References section.

2 Knowledge of IDS

Securing confidential and private data is an important part of cloud computing from its birth because of its distributed nature, for this IDS is introduced and can be defined as, "A software entity which runs on server and monitors the activity of users and programs on this server and monitors traffic on networks where it is connected" [17,18]. IDS may be classified based on its behavior for detection, monitoring scope and detection techniques. Here the behavior models are based on application model that are chose from cloud [1] We specify the characteristics of IDS in Table 2 which are used in cloud scenario.

Table 2 IDS models

IDS [1]	Models
Detection method	Specification models [7]
	Anomaly detection [5]
Monitoring method	Network IDS [6]
	Host IDS [8]
Behavior pattern	Passive and active IDS [9]

The above table illustrates several types of detection techniques in cloud. Cloud based Intrusion Detection system is divided into four types [1,18] they are, (I) network based IDS (NIDS), (II) host based IDS (HIDS), (III) VMM (or) hypervisor based IDs and (IV) distributed IDS (DIDS).

2.1 Host based IDS

HIDS collects information from specific hosts and it analyzes for identifying the intrusive events [1]. Here the analysis is based on host-bounded information such as operating system, users and applications. The efficacious of the HIDS are improved based on illustrating the features which are used for detecting intruders.

2.2 Network IDS

NIDS seizes traffics of entire network which inspects possible intrusions like DOS attacks, port scanning, etc., by utilizing IP and transport layer header of captured network packets [16,19]. This system uses anomaly based and signature based detection methods for identifying intrusions. Many hosts are deployed in network that can be secured from intruders based on utilizing proper NIDS.

2.3 Distributed IDS

DIDS is a combination of multiple IDS such as HIDS and NIDS for monitoring traffic from larger network and also avoiding intruders. DIDS has mainly two components [20] such as (i) detection component is used to monitor the system or subnet and (ii) correlation manager gathers information from multiple IDS is used to generate higher level alerts for intruder awareness.

2.4 VMM (or) hypervisor based IDS

This furnishes the platform for communication among multiple VMs which is based on hypervisor layer [20]. This Hypervisor based IDS supports analyzing available information for detecting intruder activities based on communication between VM and Hypervisor, multiple VMs within virtual network.

The most common challenges of traditional intrusion detection and prevention systems (IDPSs) are [21]:

- IDPS generate false alarm rate
- It do not deals with cloud requirements and also do not satisfy the high-speed networks constraints
- Identify internal intrusion attacks is very difficult
- They do not use proper standard or parameter to evaluate IDPS. This can lead to the misuse problem

- Networks do not audit data continuously which changes the system very in fast

3 Related work

Most researchers have developed intrusion detection system on cloud in order to detect intruders based on enlisting machine learning models such as clustering, classification algorithms [5,10,16,20]. These IDS were used for detecting intruders based on tracing attack packets which is a tedious approach. So that many research works [5,10,20] used machine learning approaches in order to detect intruders. Different types of intruders such as Flood attacks, DDOS, U2R attacks and R2L attacks were listed on [22]. For detecting the attacks on cloud, Pandeeswari and Kumar [5] proposed an anomaly detection approach in cloud environment based on fuzzy clustering models with the combination of ANN (FCM-ANN) which supports detecting both inside intruders and outside intruders. Here a hypervisor layer was preferred for monitoring the multiple operating systems in order to improve accuracy of the detection system. This system results in limitation that, FCM fails when huge request arises from user on cloud environment. Another machine learning approach called hybrid system was used for intrusion detection which is based on fuzzy systems with four different phases. This also includes a modified k-means clustering algorithm based on Miskowski distance in order to obtain clusters. These clusters were taken to type-2 fuzzy logic based genetic algorithm [10] which was utilized for rule based optimization. This system has higher execution time on clustering the non-linear data based on priori specification of different clusters.

Rule based NIDS system was proposed to detect DDOS and port scanning intruders [15] which supports preserving the network from unauthorized access and its imparts. This detection process gathers packets from networks and inspects them. If any changes were identified, then it makes an alert signal for possible attacks. Intrusion detection system, network security and secure cloud [2] have the favor of both NIDS and HIDS and there is an alternative approach in [12], authors presented an evidence collection on cloud environment by utilizing the attacker scenarios. These evidences are targeted as long as detecting the potential intruders that cannot involve other traditional security policies and in [2], a security architecture called "MetaCloudDataStorage" was proposed for protecting the Bigdata against intruders. Various researchers concentrated on DDOS attacks mitigation and that are illustrated in [23]. DDOS attacks occur in two types [24] in cloud environment that are (i) application-bug level and (2) infrastructural level. A resilience of DDOS in cloud environment was proposed to conceptual cloud environment [25], also presents an overview of DDOS attacks and a cloud security deployment policy based on CIA model. Here the author focuses for detecting DDOS attacks on the cloud and it offers a new dimension based on its architectures and features. To mitigate the vulnerabilities on cloud environment, a novel security framework was focused with optimizing the cost and coverage optimization based on Cuckoo search algorithm with levy flights [26] whereas in [24], a peer-to-peer based clustering was proposed for SNMP data for detecting the network attacks which is based on unsupervised decentralized data mining algorithms. Back off [19] counting mechanism was used for detecting DDOS attacks in distributed NIDS. Context aware anomaly detection [27] was focused on detecting the zero day attacks that allows a one-class support vector machine with deep packet inspection.

Performance and security of cloud data centers are analyzed in [14] by using Bro-IDS. Here Bro was a useful approach for maintaining all network connections and responds performance of network patterns and it includes some major components such as packet capture and filter, event engine and policy script interpreter. Here embedded Markov chain model was promoted due to inspecting packets and for analyzing the lower level packets, a Libpcap tool was preferred. This model has lower performance like higher service time in cloud data centers because FIFO queue model was used as processing the packets. Intrusion prevention methods [28] were illustrated on cloud for protecting user data that uses one time key generation [29] and trusted authority [30,31].

In [32] fusion of multi-agent functionalities scheme was proposed to detect the anomalies in the real-time datasets (SCADA, KDD). The integration of responsibilities and rules were used to find the multi-agents anomalies behavior.

4 Problem formulation

Cloud environment is utilized by every common user, so there is a higher probability for occurring intrusions. This section deals with problem definition for previous works on cloud computing and we discuss the problems that are as follows: Pandeeswari et al. [5], proposed an anomaly detection system and it supports identifying several attacks based on hybrid algorithm which was a combination of FCM clustering and ANN classification in order to improve the detection accuracy. Here the problem is that, FCM algorithms fails in furnishing accurate clusters, if large number of request raise from users, FCM does not have the capacity to cluster and its execution time is higher which leads to long time execution for overall algorithm.

A type-2 fuzzy neural network [10] was proposed based on genetic algorithm and modified k-means clustering. This system has four different operations such as cluster formation,

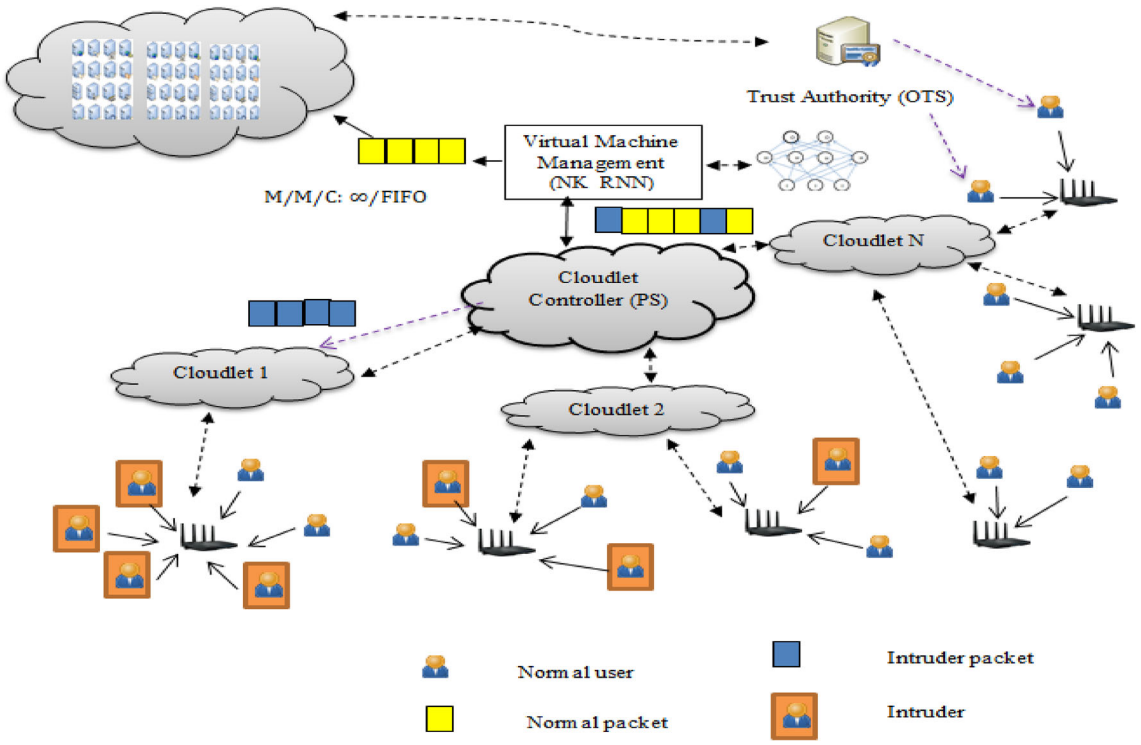

Fig. 1 Overall proposed cloud IDS architecture

extraction of initial fuzzy rules, fuzzy rule based optimization and parameter refinement. Using genetic algorithm, fuzzy rule based optimization were extracted for gaining detection rate that results in lesser speedup ratio. The speedup ratio is reduced when there is lower number of nodes and modified k-means algorithm includes a higher execution time.

In [14], analytical model called "Bro IDS" was proposed on security analysis in cloud data center by utilizing the markov chain model. This allows Libpcap to analyze the packet behavior on network which involves two servers like processing server and security server with FIFO queue modeling. Here the problem is that, FIFO queuing model has higher service time for processing packets on queue and also Libpcap is one of the system-independent interface in user-level packet capture and it is suitable for low-level network monitoring and hence it is not suitable to predicting intruders in cloud like larger environment.

For predicting DDOS attacks in cloud environment, a resource efficient network intrusion detection system [19] was proposed for securing cloud environment which includes client VM profile analysis and back off based detection of signatures. Here, three important processes were concentrated such as (i) initialization phase where many packets are allowed in cloud environment without any analysis on cloud for specific time in assumption and other flows are analyzed and updated based on initial flow, (ii) detection phase permits analysis of packets based on its rules and (iii) alert with response generation phase involves an alarm messages to cloud user. Here the problem is that, when any DDOS packets are allowed in initialization phase, then it causes involvement of attacker behavior on cloud environment. Our proposed system solves all above problems that are discussed in later sections.

5 Proposed system

In this section, we discuss our proposed system and then summarize the proposed cloud architecture which specifies the intrusion detection environment on cloud along with proposed algorithms for eradicating vulnerable attacks such as DDOS, flood attacks, U2R attacks, zero day attacks and R2L attacks. Here we illustrate intrusion detection and intrusion prevention in two folds: this first fold has our proposed detection process whereas in second fold, we concentrate on prevention mechanism. Figure 1 describes the overall proposed cloud IDS architecture.

5.1 System overview

Cloud computing is exposed to various threads and vulnerabilities that are discussed already on Sect. 2.2. Our work is concentrated on intrusion detection and prevention mechanisms and it has cloud controller (CC), trust authority

(TA) and virtual machine management (VMM). In detection mechanism, we initially collect the packets from cloud users who are located at different locations. Their packets are collected by cloudlets via routers. Our CC monitors all packets on cloudlets from users. We furnish a threshold value to every cloudlet owing to balance the packets traffic from routers. When a heavy traffic arises on single cloudlet, then, CC migrate those packets to idle cloudlets. Here we examine the packet based on packet scrutinization (PS) algorithm that classifying arrival time, flows, confidence levels and packet counts according to its header. Then packets are moved to VMM which classifies the intruder packets and normal packets using a NK-RNN classifier model. After deriving normal packets, we allocate to virtual machines using proposed packet prioritized queue modeling called M/M/C: ?/FIFO. Thus we detect the intruder packets and we discard it. In second fold, we prevent the cloud users from intruders based on furnishing OTS in our proposed system where TA allocates OTS to users for safe accessing of data from cloud. In Fig. 1, we outline our overall proposed intrusion detection and prevention architecture different users and intruders. The different types of attackers are R2L, DoS, U2R, etc.

5.2 Intrusion detection

In the first fold, we involve intrusion detection system on CC and VMM. We broadly discuss about the proposed novel algorithms in later subsections.

5.2.1 Cloudlet controller

We initially discuss about the packet examination from various users. According to our proposed system, users can move to various locations in the world, so user can send packets from wherever to cloudlets via routers. Then cloudlet collect user's packet via routers, so all users packets are collected via cloudlets. Here a complication arises like packet traffic on every cloudlet. For solving this complication, our CC furnishes a threshold value to assemble the packets from users. When packet arrival is above the threshold value, then CC migrate other packets to idle cloudlets. Then we concentrate on our proposed novel packet scrutinization (PS) algorithm. Figure 2 depicts the proposed work of cloud controller with PS algorithm.

In PS algorithm, we involve analysis of every packet based on arrival time of packets, packet flows which illustrates the sequence of packets arises from source, packet count according to header and checking confidence level. Here confidence is defined as the frequency of appearances of attributes in the packet flows or it can be called as trust value and packet counting is based on its header.

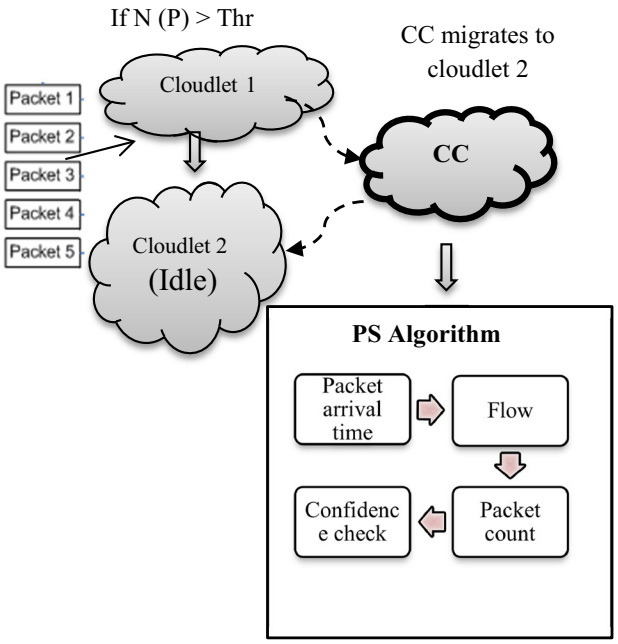

Fig. 2 Proposed work of CC with PS algorithm

The confidence level [33] is calculated based on single attribute and pair of attributes.

(i) Confidence for single attributes

$$\mathrm{C}(A_i = a_{i,j}) = \frac{N(A_i = a_{i,j})}{N_n} \tag{1}$$

where i = 1, 2, 3 . . . n and j = 1, 2, 3 . . . $\mathrm{m_i}$.

(ii) Then confidence for attribute pairs

$$\mathrm{C}(A_{i_1} = a_{i_1,j_1}, A_{i_2} = a_{i_2,j_2}) = \frac{N(A_{i_1} = a_{i_1,j_1}, A_{i_2} = a_{i_2,j_2})}{N_n} \tag{2}$$

where $i_1 = 1, 2, 3 \ldots n, i_2 = 1, 2, 3 \ldots n, j_1 = 1, 2, 3 \ldots \mathrm{m}_1$ and $j_2 = 1, 2, 3 \ldots \mathrm{m}_2$.

where N depicts the number of attributes that are considered for our proposed system overcoming the flooding attacks and DDOS attacks. A_i illustrates the ith attribute in packet and M_i is the values that A_i has, and $\mathrm{a_{i,j}}$ is the jth value of attribute and $\mathrm{N_n}$ indicates total number of packets on packet flow in one time interval (t), $N(A_i = a_{i,j})$ specifies attributes $\mathrm{A_i}$ has the value $\mathrm{a_{i,j}}$ in packet flow in one time interval (t) and $N(A_{i_1} = a_{i_1,j_1}, A_{i_2} = a_{i_2,j_2})$ denotes number of packets whose attributes A_{i_1} has the value a_{i_1,j_1} and A_{i_2} has the values a_{i_2,j_2} in packet flow in one time interval (t). Using these equations, we calculate the confidence levels of every

packet; if confidence level of packet is lower, and then corresponding packet will be discarded otherwise the packet will be accepted. We furnish the following steps that explain the processing of PS algorithm.

Steps for ***Packet Scrutinization (PS) Algorithm***

Step 1: Start
Step 2: Examine the arrival time of every packet from all Cloudlets
Step 3: Classify the packets based on arrival time and its Flows
Step 4: Check packets according to its header
Step 5: Count the packets according to its header
Step 6: Check confidence level using (1) and (2)
If (packet > threshold level)
Accept packet
else
Discard packet
Step 7: End

Here the algorithm explains that after checking arrival time, we classify the flows of packet by considering the arrival time and we also calculate the packet count according to its header like TCP, UDP, HTTP and etc. Then finally we check confidence level for every packet and then we accept the packet. Thus using this algorithm, we can detect and remove the initial flooding attack and port scanning attack.

5.2.2 Virtual machine manager

This subsection involves our proposed hybrid classifier for classifying the intruders and it is followed by queue modeling which allocates packets to VMs with prioritization.

5.2.2.1 Hybrid classifier After analyzing the packets, CC allows the packets to VMM which involves the novel hybrid classifier named "NK-RNN" that involves two phases such as (1) normalized K-means (NK) clustering algorithm and (2) recurrent neural network (RNN). In first phase, we initially permit usual k-means clustering algorithm. Then we normalize the values of clusters that support removing non-reliable data based on calculating the maximum value and minimum value. Compute Normalized values (V'') described in below [30],

$$V'' = \frac{v - min(e)}{max\,(e) - \min(e)} \tag{3}$$

where e denotes the corresponding attributes whereas min(e) and max(e) represents minimum value and maximum value for attribute. We calculate the centroid points (nearest points) based on sorting operations for clusters. Thus in first phase, we obtain clusters with based on considering their attributes. In second phase, the result of NK is clustering of packets that maintain consistency within the cluster. Here the resulting clusters are undertaken by various RNN [34,35] as input. We train the input clusters based on back propagation method since, total size is reduced and efficacy of the RNN will be improved. The major difference between Artificial Neural Network and RNN is Computation process. RNN is computationally expensive and it process with a given time t. ANN is building manual features to feature learning whereas RNN learn dependencies between observations i.e. features related to the dynamic. Feedforward neural network is one of the first artificial neural networks which accommodate input layer, hidden layer, output layer and connections between different layers. When the Feedforward network is a directed cycle, so-called as RNN and its theme of RNN is unfolding a recurrent computation of cyclic Feedforward network and this permits deep learning patterns in sequences. RNN is based on weights that are specified on connections between each layer, there are three kinds of weights such as,

- *I2H weight* a weight from input layer to hidden layer
- *H2O weight* a weight from hidden layer to output layer
- *H2H weight* a weight from hidden layer to next time step hidden layer

Then RNN trains the clusters as $[x_t, y_t]$ and uses the forward propagation,

$$x_{t+1} = x_t - (f'(x))^{-1} f'' = x_t - (H(f)(x_t))^{-1} f'' \tag{4}$$

where H is the hessian matrix which is also called as curvature matrix f with its second derivatives, a non-linearity based activation function (f and g) are preferred such as sigmoid, hyperbolic tangent on neural network,

$$h_t = f(W_{I2H} x_t + W_{H2H} h_{t-1} + b_h) \tag{5}$$

$$\bar{y}_t = g(W_{H2O} h_t + b_y) \tag{6}$$

After training the clusters, we predict $\bar{y}_t$ using Eq. (6). Here x_t, h_t and y_t denotes the input vector, hidden state and output vector respectively where t illustrates the time sequence. $\bar{y}_t$ represents the estimated output vector by RNN. W_{I2H}, W_{H2H} and W_{H2O} are the weights of different layers, b_h and b_y are the bias values of hidden state and output vector respectively, f denotes the hidden non-linearity and g depicts the output non-linearity. Thus we obtain $\bar{y}_t$ from every cluster and merge all the results obtained and we again perform RNN for merged result. Thus we obtain the intruder packets and normal packet according to its intruder's attributes. We also furnish steps for NK-RNN classifier model as follows:

Steps for ***NK-RNN Classifier Model***

NK- Clustering

Step 1: Start

Step 2: We collect packets from CC

Step 3: we execute K-means clustering algorithm by following steps:

(1) choose randomly k of our packets for partition centers

(2) estimate distance between data point on set where centers store information

(3) Assign each point to nearer cluster center based on minimum distance (Euclidean distance) based on,

$$D\ (x, y) = \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2} \quad (7)$$

(4) Update cluster center using,

$$C_i = \frac{1}{|k_i|} \sum_{x_j \in k}^{k} x_j \quad (8)$$

(5) If (cluster center changes)

Go to (2).

Else

Go to *Step 4*.

Step 4: Normalize k-clusters using equation (3).

Step 5: Sort the packets on clusters

Step 6: Calculate the centroid points using equation (7)

Step 7: Re-cluster according to centroid points using (8)

Step 8: End

RNN classifier

Step 9: Start

Step 10: train clusters using back propagation algorithm with equation (4)

Step 11: use activation functions (5) & (6) for every cluster

Step 12: aggregate all results from equation (6)

Step 13: repeat *step 9*

Step 14: perform equation (5) and (6) to predict intruders and normal packets

Step 15: End

5.2.2.2 Queue modeling After classifying the intruder packets and normal packets, we discard intruder packets from VMM whereas the normal packets are passed for processing on virtual machines. In order to furnish efficacious servicing, we introduce a queue modeling that involves prioritizing the packets. Usually queuing system is characterized with four basic components such as (1) *Queue Discipline*, (2) *Arrival rate*, (3) *Service Channels* and (4) *Service Rate*. Our proposed queuing model has FIFO queuing model, arrival rate is estimated based on packet entering on environment, service channels are specified with multiple VMs can estimate different packets and service rates are defined as that multiple packets are executed with different VM at a time. We prioritize the packets based on types of rules which are depicted with arrival time and processing time. Herein, number of rules to be checked each time a packet arrives. For example, if a TCP packet is to be analyzed, it does not sense to apply UDP signature rules to the packet. In this way, intruders were find in the real-time scenarios. Our proposed queue model has multi-user packets (∞) and multi-server (C) "M/M/C : ∞/FIFO" and we propose four priorities such as A, B, C and D which is depicted as follows:

- *A* When a packet has short waiting time and its request type is urgency then packet get first priority on queue for processing
- *B* A packet with long waiting time and has urgency request then we furnish second priority for the packet
- *C* A packet with short waiting time and has no urgency gets third priority for processing.
- *D* A packet with long waiting time and has no-urgency for processing, then we furnish fourth priority for the packet

Based on these priorities we process the packets and we allocate the packets to execute on virtual machines and it improves QoS on our proposed system. Our proposed queue model is explained with several steps:

Steps for ***Queue Modeling***

Step 1: Start
Step 2: VMM → P
Step 3: if (P → RT: Urgency && WT: Short)
PT: A
End if
Step 4: if (P → RT: Urgency && WT: Long)
PT: B
End if
Step 5: if (P → RT: No Urgency && WT: Short)
PT: C
End if
Step 6: if (P → RT: No Urgency && WT: Long)
PT: D
End if
Step 7: P → Q
Step 8: Q → VM
Step 9: End

In above steps, P is the packet, Q specifies FIFO queues, RT represents request type, WT illustrates waiting time and PT denotes priority type (A, B, C and D) of packets. Thus, our proposed intrusion detection furnishes efficacious result in terms of detection accuracy, false alarm rate, F-score, packet loss ratio and throughput.

5.3 Intrusion prevention

In second fold, we discuss our proposed system with intrusion prevention mechanism by preferring TA in our cloud.

5.3.1 Trust authority After identifying intruders on cloud environment, we furnish a novel prevention mechanism for preserving user's data and secure access. Our TA involves the secure access of data for cloud users and preventing data from intruders based on promoting OTS generation algorithm for users. Data on cloud environment are stored based on elliptical curve cryptographic method [36,37]. Using this cryptographic method, every user has a pair of public key and private key. Our novel approach is that, we generate the private keys randomly and it is used by the cloud users only once in a time. In order to access the data, every user initiate a generation of signature based on considering user id and randomly generated private key. After accessing data, signature is changed and a new private key is initiated at the trust authority for every user and it prevents user's data from several vulnerable attacks.

6 Experimental validation

In this section, we discuss our proposed outcome with experimental evaluation. This section is encompassed with performance metrics and comparative analysis with graphical plots. With this result, we demonstrate our work which furnishes efficacious results. Our experimental evaluation furnishes effective results which are compared with several previous works based on considering performance metrics. Our proposed Intrusion Detection and Intrusion Prevention System is proved based on analyzing our proposed algorithms with metrics such as, packet loss ratio, throughput, detection rate, speedup ratio, F-score and false alarm rate. We discuss and prove our efficacious results that are described on latter section and we learn about the problems of previous works in detailed manner.

Packet loss ratio is defined as the number of packets which are not properly sent to the receiver.

Packet Loss Ratio = NPS/NPR*R, where NPS is the number of data packets sent by sender, NPR is the number of packets which are received by the receivers and R is the number of receivers

Throughput is defined as the minimum data reception rate overall multicast receivers.

Detection rate is a ratio of the number of correct detection to the total number of attacks and False Alarm rate is a ratio of the number of misclassification

Table 3 Proposed system results

Parameter	Normal	DDOS	Probe	R2L	U2R
F-score	99	99	90	89	85
False alarm rate	0	0	0	2	2
Detection rate	100	100	100	99	97

$$\text{Detection rate} = \frac{TP}{TP + FN}$$

$$\text{False alarm rate} = \frac{FP}{TN + FP}$$

Comparative result with graphical plots

This section depicts the efficacy of our proposed system which is compared with previous works based on furnishing graphical plots. Here our metrics are evaluated and examined against previous works that we considered are Anomaly detection system [5], intrusion detection and prevention system [14], Fuzzy based hybrid system [10] and context aware anomaly detection [27] (Table 3).

6.1 Effectiveness of F-score against various vulnerable attacks

In previous works, the attacks like probe, DDOS, R2L and U2R attacks are identified using Fuzzy-ANN methodology [5] whereas we solve these attacks based on Hybrid classifier. F-score or F-measure is defined as the measuring the accuracy of the system and it is calculated based on considering the precision, recall which involves the true positive rate and true negative rate. Thus we calculate them by,

$$\text{Precision} = \frac{TP}{TP + FP}$$

$$\text{Recall} = \frac{TP}{TP + FN}$$

$$\text{F} - \text{score} = \frac{(1 + \beta^2) * recall * precision}{\beta^2 * (recall + precision)}$$

where TP denotes number of true positive, FP specifies number of false positive and FN illustrates number of false negative and β represents the relative importance of precision vs. recall such that $\beta = 1$. We plot our graphical charts with several attacks packets and normal packets against F-score.

In above Fig. 3, we can see comparison result in F-score which are respected to precision and recall values according to proposed result and previous work result. In this result, we can see the higher scoring of our proposed hybrid classifier when compared to FCM-ANN classifier and it furnishes poor result on intruders such as U2R and R2L due to failing in accurate clusters. From this result, we have seen that performance of our hybrid classifier furnishes efficacious results

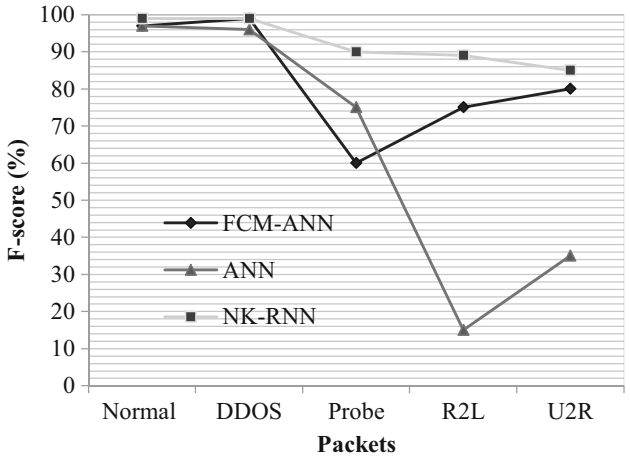

Fig. 3 Evaluating F-score values against packets with attacks

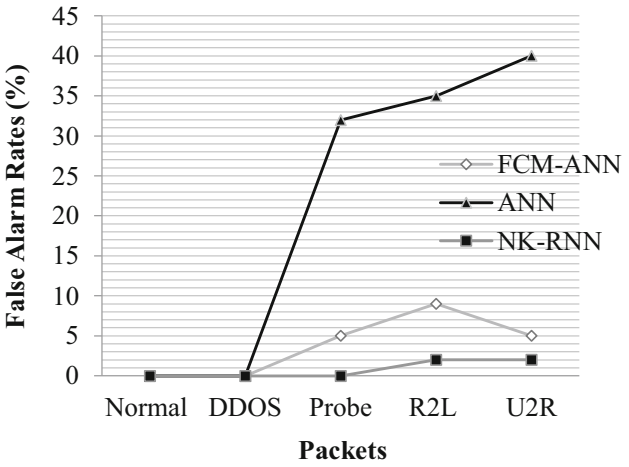

Fig. 4 Graphical plot for False alarm rates values against packets with attacks

on both high frequent attacks and low frequent attacks that can surely identify any attacks on the cloud environment and hence cloud can be freed from intruders.

6.2 Effectiveness of false alarm rate (false negatives) against attacks

This section describes the false alarm rate against several attack types and also specifies the accurate prediction of packets on our proposed cloud. We furnish the graphical plot for the false alarm rate by comparing with FCM-ANN classifier [5] which shows efficacious results. This Fig. 4 describes the performance of proposed system under several attack packets and it produces lower false alarms when compared with FCM-ANN and ANN. FCM-ANN results false alarm rates above 5% whereas ANN classifiers goes upto rates of above 30% for probe attacks and lower frequent attacks such as R2L and U2R. Thus our NK-RNN is best classifier for identifying intruders under lower frequent, higher frequent attacks and probe attacks because it has less false alarm rates i.e. 4 % for lower frequent attacks.

6.3 Effectiveness of detection rate against attacks

In proposed work, we detect the intruders like DDOS, Probe, R2L, U2R and zero day attacks based on NK-RNN classifier. We compare our detection results by comparing with our previous works Anomaly detection system [5] and Context aware anomaly detection [27]. This graphical plot describes the detection rate of attacker packets under several types of attacker packets.

In Fig. 5a, we have shown the performance of detection rate under different intruder packets with previous work [5]. Here our proposed result furnished higher detection rates which are above 98 % whereas the FCM-ANN has higher detection rates i.e., 100 % for normal packets, probe pack-

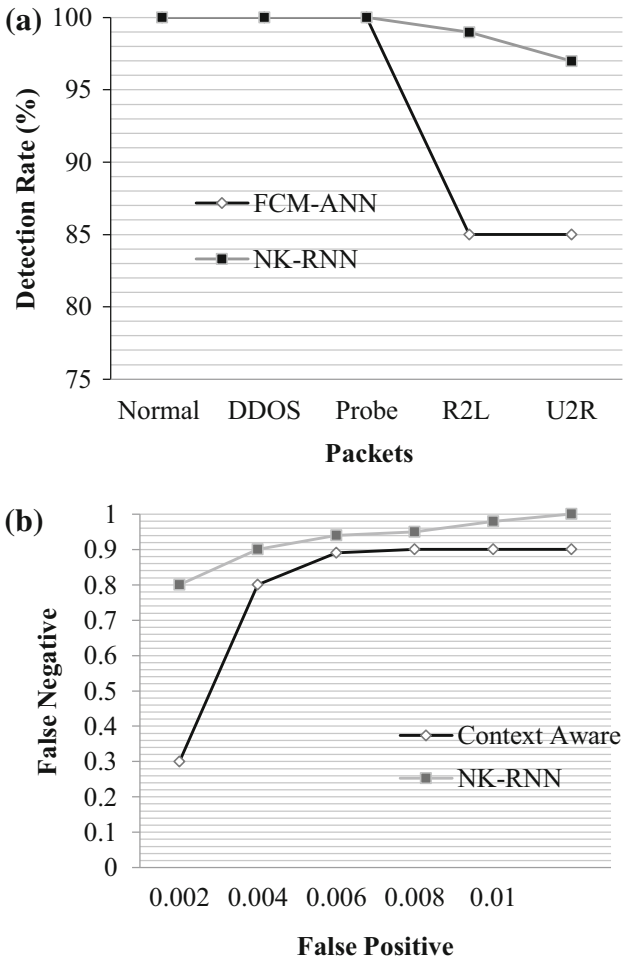

Fig. 5 **a** Detecting rate for packets and **b** comparison result for detection attacks against context aware anomaly detection [27]

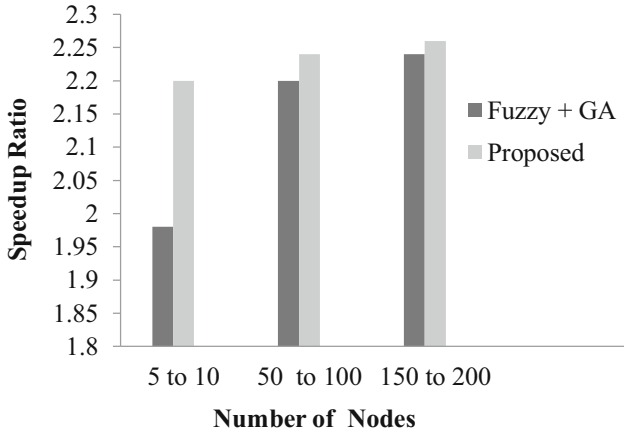

Fig. 6 Graphical plot for speedup ratio against number of nodes

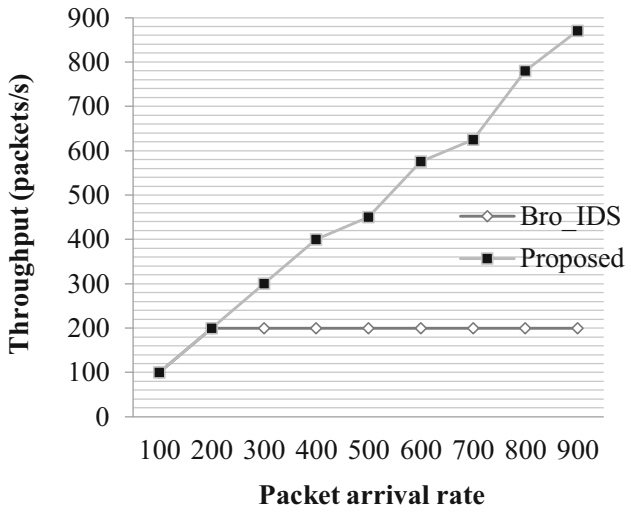

Fig. 7 Graphical plot for throughput against packet arrival rate

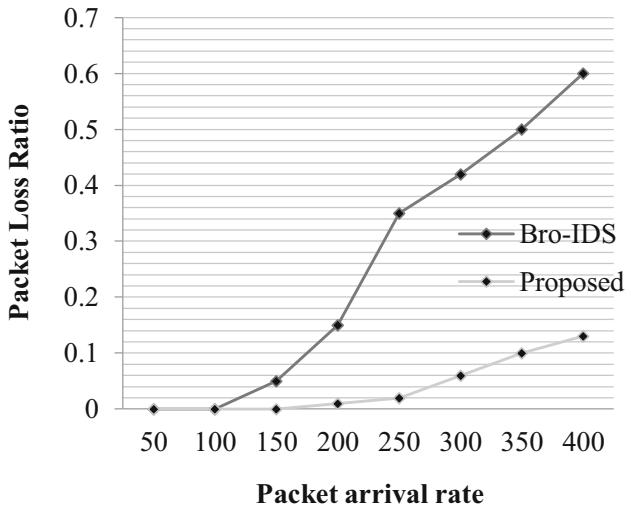

Fig. 8 Performance of packet loss ratio against packet arrival rate

ets and DDOS attacks and it reduces its detection rate upto 85 % for U2R and R2L attacks. In Fig. 5b, the performance of detection rates are specified under false negative and false positive probabilities. Here the previous work [27] represents their detection rate while increase on both false positive values and false negative values whereas our proposed system furnishes higher detection rate which maintains the steady state i.e., false negative values while at lower false positive values. Thus, Fig. 5a, b shows efficacious detection rate of attacks on proposed NK-RNN classifier model.

6.4 Effectiveness of speedup ratio

This section describes the overall speed up which involves user's packets on cloud. Here this metric considers average execution time during training the data. The speed up ratio is defined as that supports increasing the performance between two nodes which processing the same packet. We depict the speedup ratio in graphical plot against number of nodes on the recurrent neural network.

Figure 6 illustrates the graphical plot for performance of Nodes which specifies the scaling tendency for the cloud environment and incorporating the intrusion detection of cloud. Here the number of packets is directly proposed to size of cloud which doubles the size of nodes according packets arrival. Here the previous work [10] faces the issue like lower speedup ratio for small number of nodes, whereas our proposed system solves the problem and it works in efficient manner when there are smaller nodes available on cloud.

6.5 Effectiveness of throughput

In this section, we describe the performance of our queuing model in order to analyze the throughput of proposed environment. Throughput is defined as the rate that packet finishes successful processing of packets and the graphical plot for both previous systems and proposed system are shown as follows:

In Fig 7, we have seen that throughput obtained for both proposed system and Bro-IDS [14]. Here we specify the mean service time 5 micro seconds for both results. The previous work shows result that, it maintains the throughput at 200 packets/second on higher packet arrival rate whereas our proposed system increases the throughput of system which is equal to packet arrival rate. According to [14], the protection is based on rules of analytical model; hence the protection for cloud environment increases whereas the throughput decreases. But here we focused OTS for preventing data. This shows the best performance of proposed system than previous work, where we maintain both performance metrics and security of cloud at a steady state.

6.6 Effectiveness of packet loss ratio

In this section, we depict the performance of our queuing model in order to analyze the packet loss ratio of proposed environment. Here we specify the mean arrival rate at 0.5 micro seconds for the packets on the queues.

In Fig. 8, we illustrate the outcome of packet loss ratio for both proposed system and Bro-IDS [14]. Here we have seen that our proposed system has lesser loss ratio i.e., upto 300 packet arrival rate, our loss ratio is below 0.1 and after that we face a slight increase, whereas the existing system has 0 ratio upto 100 packets arrival and after above 100 there is a rapid increase of loss ratio thus, it specifies when number of packet increases then it suffers from higher loss ratio.

7 Conclusion

In our proposed system, we have directed our research on intrusion detection system on cloud. In this system, we point out the complications of vulnerable intruders and we also furnished efficacious solutions in order to solve problem of intruders such as DDOS, probe, U2R, R2L and zero day. Here we proposed a novel intrusion detection and intrusion prevention environment for cloud with three components like TA, VMM and CC. A PS algorithm is proposed on CC for analyzing the flooding attacks and port scanning attacks, a novel hybrid classifier is proposed for detecting the intruder packets on cloud which uses the combination of NK and RNN that differentiates the normal packets and intruder packets, a queue modeling is proposed for allocating the packets to VM for execution and finally a novel OTS is preferred for secure access of data for the cloud users. Thus, our proposed system presents efficient results based on verifying and analyzing the performance metrics with graphical results and it is proved that our system can be implemented in real time for detecting intruders in cloud, so as a future work, we directed our research to implement our proposed system in real time.

References

1. Mehmood, Y., Shibli, M.A., Habiba, U., Masood, R.: Intrusion detection system in cloud computing: challenges and opportunities. In: IEEE 2nd National Conference on Information Assurance (NCIA), pp. 59–66 (2013)
2. Manogarana, G., Thotab, C., Vijay Kumar, M.: MetaCloudDataStorage architecture for big data security in cloud computing. In: 4th International Conference on Recent Trends in Computer Science & Engineering, Elsevier, pp. 128–133 (2016)
3. Jin, H., Xiang, G., Zou, D., Wu, S., Zhao, F., Li, M., Zhengm, W.: A VMM-based intrusion prevention system in cloud computing environment. J. Supercomput. **66**, 1133–1151 (2011)
4. Abazari, F., Analoui, M., Takabi, H.: Effect of anti-malware software on infectious nodes in cloud environment. Comput. Security **58**, 139–148 (2015)
5. Pandeeswari, N., Kumar, G.: Anomaly detection system in cloud environment using fuzzy clustering based ANN. Mobile Netw. Appl. **21**(3), 494–505 (2015)
6. Xing, T., Xiong, Z., Huang, D., Medhi, D.: SDNIPS: enabling software-defined networking based intrusion prevention system in clouds. In: CNSM Short Paper and Workshop, pp. 308–311 (2014)
7. Le, A., Loo, J., Chai, K.K., Mahdi, A.: A specification-based IDS for detecting attacks on RPL-based network topology. MDPI J. **7**(25), 1–19 (2016)
8. Deshpande, P., Sharma, S.C., Peddoju, S.K., Junaid, S.: HIDS: a host based intrusion detection system for cloud computing environment. Int. J. Syst. Assur. Eng. Manag. doi:10.1007/s13198-014-0277-7 (2014)
9. Tolupa, S., Nischenko, V.: Analysis of intrusion detection systems TAXONOMY in the CONTExt of current development level of information systems. Exclus. J. **2**, 1–6 (2015)
10. Raja, S., Ramaiah, S.: An efficient fuzzy-based hybrid system to cloud intrusion detection. Int. J. Fuzzy Syst. **19**(1), 62–77 (2016)
11. Ramachandran, M.: Software security requirements management as an emerging cloud computing service. Int. J. Inf. Manag. **36**, 580–590 (2016)
12. Pasquale, L., Hanvey, S., Mcgloin, M., Nuseibeh, B.: Adaptive evidence collection in the cloud using attack scenarios. Comput. Soc. **59**(C), 236–256 (2016)
13. Chen, Y., Member, Y.C., Cao, Q., Yang, X.: PacketCloud: a cloudlet-based open platform for in-network services. IEEE Trans. Parallel Distrib. Syst. **27**(4). doi:10.1109/TPDS.2015.2424222 (2015)
14. El Mir, I., Haqiq, A., Kim, D.S.: Performance analysis and security based on intrusion detection and prevention systems in cloud data centers. Adv. Intell. Syst. Comput. **552**, 456–465 (2016)
15. Patel, S.K., Sonker, A.: Rule-based network intrusion detection system for port scanning with efficient port scan detection rules using snort. Int. J. Future Gen. Commun. Netw. **9**(6), 339–350 (2016)
16. Keegan, N., Ji, S.-Y., Chaudhary, A., Concolato, C., Yu, B., Jeong, D.H.: A survey of cloud-based network intrusion detection analysis. Hum. Centr. Comput. Inf. Sci. **6**, 19 (2016)
17. Labib, K.: Computer security and intrusion detection. The ACM Student Magazine (2004)
18. Deshpande, P., Sharma, S.C., Sateeshkumar, P.: Security threats in cloud computing. In: IEEE International Conference on Computing, Communication and Automation, pp. 632–636 (2015)
19. Gupta, S., Kumar, P.: Profile and back off based distributed NIDS in cloud. Wireless Pers. Commun. **94**(4), 2879–2900 (2016)
20. Patel, A., Taghavi, M., Bakhtiyari, K., Junior, J.C.: An intrusion detection and prevention system in cloud computing: a systematic review. J. Netw. Comput. Appl. **36**(1), 25–41 (2013)
21. Carlin, A., Hammoudeh, M., Aldabbas, O.: Intrusion detection and countermeasure of virtual cloud systems—state of the art and current challenges. Int. J. Adv. Comput. Sci. Appl. **6**(6) (2015). doi:10.14569/IJACSA.2015.060601
22. Kumar, U., Gohil, B.N.: A survey on intrusion detection systems for cloud computing environment. Int. J. Comput. Appl. **109**(1), 6–15 (2015)
23. Zargar, S.T., Joshi, J., Tipper, D.: A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. IEEE Commun. Surv. Tutorials **15**(4), 2046–2069 (2013)
24. Cerroni, W., Moro, G., Pasolini, R., Ramilli, M.: Decentralized detection of network attacks through P2P data clustering of SNMP data. Comput. Security **52**, 1–16 (2015)
25. Osanaiye, O., Kim-Kwang, R.C., Dlodlo, M.: Distributed denial of service (DDoS) resilience in cloud: review and conceptual cloud

DDoS mitigation framework. J. Netw. Comput. Appl. **67**, 147–165 (2016)
26. Zineddine, M.: Vulnerabilities and mitigation techniques toning in the cloud: a cost and vulnerabilities coverage optimization approach using Cuckoo search algorithm with Lévy flights. Comput. Security **48**, 1–8 (2015)
27. Duessel, P., Gehl, C., Flegel, U., Dietrich, S., Meier, M.: Detecting zero-day attacks using context-aware anomaly detection at the application-layer. J. Netw. Comput. Appl. **16**(5), 475–490 (2016)
28. Alshehry, B., Allen, W.: Proactive approach for the prevention of DDoS attacks in cloud computing environments. In: Applied Computing and Information Technology. Springer, Cham, pp. 119–133 (2016)
29. Ranjan, N., Ekhlasur Rahman, Md., Uddin, M.S.: Generation and verification of digital signature with two factor authentication. In: IEEE International Workshop on Computational Intelligence, pp. 131–135 (2016)
30. Yu, Z., Zhang, W., Dai, A.: A trusted architecture for virtual machines on cloud servers with trusted platform module and certificate authority. J. Signal Process. Syst. **86**(2—-3), 327–336 (2017)
31. Dawoud, M.M., Ebrahim, G.A., Youssef, S.A.: A cloud computing security framework based on cloud security trusted authority, pp. 133–138. In: Proceedings of the 10th International Conference on Informatics and Systems. ACM Digital Library (2016)
32. Sadhasivan, D.K., Balasubramanian, K.: A fusion of multiagent functionalities for effective intrusion detection system. Security Commun. Netw. **2017**. doi:10.1155/2017/6216078 (2017)
33. Negi, P., Mishra, A., Gupta, B.B.: Enhanced CBF packet filtering method to detect DDoS attack in cloud computing environment. Cryptography and Security, Cornell University Library, pp. 1– 5 (2013)
34. Kim, J., Kim, H.: Applying recurrent neural network to intrusion detection with hessian free optimization. In: International Workshop on Information Security Applications, pp. 357–369. Springer, Cham (2016)
35. Javed, A., Larijani, H., Ahmadinia, A., Emmanuel, R.: Comparison of the robustness of RNN, MPC, and ANN controller for residential heating system. In: Fourth International Conference on Big Data and Cloud Computing (IEEE), pp. 604–612 (2014)
36. Hong, M., Zhao, W., Wang, P.: Homomorphic encryption scheme based on elliptic curve cryptography for privacy protection of cloud computing. In: 2nd International Conference on Big Data Security on Cloud (IEEE), pp. 152–157 (2016)
37. Chintawar, N.N., Gajare, S.J., Fatak, S.V., Shinde, S.S., Virkar, G.: Enhancing cloud data security using elliptical curve cryptography. Int. J. Adv. Res. Comput. Commun. Eng. **5**(3), 1–4 (2016)

V. Balamurugan received his M.Sc degree in computer Science from Yadava College, Madurai Kamaraj University in 2000 and received his M.E. degree in Computer Science and Engineering from Mohamed Sathak Engineering College, Anna University, India, in 2008. Currently, he is working as a Assistant Professor, CSE department in Mohamed Sathak Engineering, Kilakarai, Tamil Nadu, India from 2008 to till date. His research interest includes Information Security, Distributed Computing and Fault Tolerance. He has total 11 years of experience in Academic.

R. Saravanan received his B.E. degree in Electrical and Electronics Engineering from Thiagarajar College of Engineering, India, in 1994, M.E. in Computer Science and Engineering from Madurai Kamaraj University, India, in 2000, and Ph.D. in Distributed Computing from Anna University Chennai, in 2010. Currently, he was Director/Principal in RVS Educational Trust's Group of Institutions, Dindigul, Tamil Nadu, India from 2013 to 2017. Currently he is working as a Principal in RVS College of Engineering Dindigul from 28.08.2017 onwards. His research interest includes Distributed Computing, Information Security, and Mobile Computing. He has published more the 35 papers in reputed International journals and 25 International conferences. He has total 20 years of experience in Academic and industry. Previously he was working as Head, Department of Computer Science and Engineering for more than 10 years in PSNA college of Engineering and Technology, Dindigul. He was the motivational force for the students to do real time projects and it was well appreciated by media and press.