10.48047/jocaaa.2025.34.12.12

PaaS Platform Security Enhancement and DOS Attack Detection In Cloud Computing and its Prevention

Sreedevi Vallabapurapu [1], Ramdas Vankdothu[2]

[1] School of Computing, University of South Africa, Johannesburg, South Africa

Abstract Assault identification systems encounter a confusing problem landscape because of the nonlinear nature of interference attempts, the unpredictable nature of framework traffic, and the vast number of attributes in the issue space. Based on a combination of the recurrent neural network (OCSA+RNN) and the oppositional crow search algorithm, this study suggests an efficient DOS assault detection solution. bolster the PaaS network platform's defenses. The method suggested in this paper incorporates lightweight attribute-based encryption (LW-ABE). RNN is employed for the detection and classification of DOS attacks, whereas OCSA is used for the selection of feature data. First, the OCSA approach is applied to choose the most crucial characteristics. After selection, the RNN classifier receives the features. The testing process involves classifying the input data using an RNN classifier. Finally, while the attack data is erased, the regular data is stored in the cloud. Normal data moves to the last step of the procedure, security enhancement, once the assaults have been eliminated. Security is maintained through the use of a lightweight attribute-based encryption technique. Because of their scalable infrastructures, open APIs, and multi-tenancy, PaaS platforms are extremely susceptible to DoS assaults. Resilience is greatly increased by combining intelligent resource management, container hardening, robust identity and access security, and AI-driven anomaly detection. The most reliable security is provided by a hybrid system that combines behavior analysis, machine learning, and proactive mitigation. This solution guarantees high availability, cost effectiveness, and continuity for cloud-based services.

Keywords Cloud computing, DOS attack, recurrent neural network, Crow search algorithm, Security, Oppositional based learning.

1. INTRODUCTION

Cloud computing has transformed the way IT services are delivered by providing scalable, on-demand resources through Platform-as-a-Service (PaaS), Software-as-a-Service (SaaS), and Infrastructure-as-a-Service (IaaS). Among these, PaaS offers developers a controlled environment for creating, deploying, and scaling applications without requiring them to manage the underlying infrastructure. Nevertheless, this ease of use brings with it serious security risks, particularly DoS and DDoS attacks, which have the potential to seriously impair platform availability.

DoS attacks deplete PaaS resources, including memory, computation, networks, and APIs, leading to either sluggish performance or no service at all. Attackers take use of multi-tenant vulnerabilities, PaaS middleware, auto-scaling features, and API gateways. Therefore, maintaining service integrity, availability, and trust requires improving PaaS platform security and creating clever DoS detection techniques.

But there are also significant security risks associated with this convenience. Malicious actors find PaaS systems to be appealing targets because they frequently house numerous apps and tenants on shared infrastructure. Insecure APIs, incorrectly designed services, or insufficient tenant separation can all lead to security flaws. The Denial-of-Service (DoS) attack is one of the most persistent and destructive of these threats, wherein attackers try to overload system resources, interfere with regular processes, and prevent authorized users from accessing cloud-hosted apps. By utilizing numerous hacked devices, Distributed Denial-of-Service (DDoS) attacks can increase the impact when carried out on a wider scale, causing significant downtime, monetary losses, and harm to the reputation of both consumers and service providers.

Because traditional security techniques were created primarily for isolated and static systems, they frequently fail in dynamic cloud environments. Real-time monitoring, anomaly detection, and adaptive defense mechanisms that can scale with changing workloads are necessary for the detection and prevention of DoS/DDoS assaults in PaaS platforms. Promising strategies to improve resilience against such assaults include machine learning, deep learning, and trust-based security frameworks, which reduce false positives and allow for proactive detection of malicious traffic.
By incorporating strong detection systems for DoS and DDoS assaults, this research aims to improve the security of PaaS platforms. The objective is to provide a clever architecture that protects application availability, boosts confidence in cloud services, and guarantees continuous service delivery. The suggested solution will help create cloud environments that are safer, more dependable, and more effective for both enterprises and end users by tackling security issues at the platform level.

With applications worldwide, distributed computing is now one of the fastest expanding areas in the IT industry [6]. Conveyed registering aims to provide convenient, on-demand access to a standard collection of configurable figuring assets

10.48047/jocaaa.2025.34.12.12

(for example, structures, workers, data, applications, and associations) that can be provisioned and delivered quickly using immaterial association exertion or cloud association collaborations. Platform as a Service (PaaS), Software as a Service (SaaS), and Infrastructure as a Service (IaaS) are all advantages of the cloud (IaaS). As a result of the numerous hurdles involved with it, they may attract gatecrashers [7]. As distributed computing enables on-demand, flexible, and open registration administrations, a growing number of organizations are beginning to recognize this shift in viewpoint by shifting their databases and applications to the cloud [8]. Phishing, deceit, Denial of Service (DoS), identifying holes, and record catching are all unmistakable ambush tactics for stealing someone's capabilities. If an assailant has access to someone's affirmations on the cloud, the individual can listen in on a customer's exercises, trades, and change data invisibly [9]. A Denial of Service (DoS) attack is a circular, encouraging ambush on the openness of a host worker (application worker, stockpile, database Server, or DNS worker) or framework resource, pushed through a network of infected systems indirectly [10]. The characteristics of DoS ambush, such as having a distinct appearance in various situations, make it difficult to detect [11].

PaaS stands for Platform as a Service, and it is a platform to which outside designers can upload their applications. As applications share assets, PaaS security becomes more important. Step-by-step procedures for verifying and separating assets become a primary focus [12]. To give cloud customers the ability to assess their security needs to identify key areas in PaaS cloud structures where security solutions offered by CSPs might be compared. The investigation uses a quantitative approach to deal with offers numeric information that reveals basic models inside the PaaS condition where security can be analysed and security controls inspected to satisfy these security requirements, using a flexible security planning network. The framework can be customized for different PaaS cloud models based on unique security requirements

and administrative level destinations recognised by PaaS cloud users [13]. Improve security requirement decisions by allowing clients to specify and convey their security requirements using a flexible and easy framework. These methodologies are validated using two use case scenarios and a model based on real-world CSP secSLA data gathered from the Cloud Security Alliance's Security, Trust, and Assurance Registry [14], in addition to providing guidelines on the independent and aggregate use of QPT and QHP. The executives use Security Manager (SM) to store metadata such as square marks, scrambled keys, and procedure characters. While SM verifies and confirms the right character, the CCAF security maintains concurrent encryption as the third layer of security [15].

1.1. Contribution and Organization of the paper:

This study's primary contribution is the usage of OCSA and LW-ABE to detect DOS assaults and enhance cloud PaaS platform security. The two stages of the suggested endeavor are security bolstering and DOS assault detection. When OCSA selects the feature data in the best possible way and advances them all to the next step of attack detection, each phase comprises of a few stages of the working process. RNN makes a distinction between data that has been compromised and data that has not. After the compromised data is removed, only the regular data is sent to the following security improvement phase.

.

The rest of the paper organized as follows; The remainder of the paper is structured as follows: The proposed DOS attack detection and security enhancement of the PaaS network platform is discussed in section 3. Section 2 includes a review of similar works, and section 3 explains the proposed DOS attack detection and security enhancement of the PaaS network platform. In section 4, the experimental results are analyzed, and in section 5, the conclusion is offered.

2. LITERATURE SURVEY

Kubernetes/OpenShift/Cloud Foundry) so developers ship apps while the platform handles build, deploy, autoscaling, and service discovery. This flattening of control planes (API server, etcd, admission webhooks), data planes (CNI, ingress/gateway, service mesh), and shared add-ons (registries, CI/CD, logging) introduces distinct DoS/DDoS surfaces: API saturation, ingress/gateway floods, CoreDNS exhaustion, pod churn from bursty scaling, node-local resource starvation, and cost-amplifying “Economic DoS” (EDoS). Industry studies since 2023–2025 highlight cloud-native security gaps (visibility, misconfig, runtime controls) that intersect with DoS exposure and incident impact, especially in K8s-based PaaS.

Anteneh Girma et al. [16] have demonstrated the use of advanced machine learning to distinguish DoS ambushes on distributed computing utilising entropy and bunching development. They were continuing their investigation to implement such compelling DDoS combination discovery frameworks. They planned to do even more in-depth reverse testing to finish that exhaustive technique on both sides of the distributed computing situation (the framework and host level). Those recommended systems may be the perfect choice suffering response for distributed computing organisations openness, based on their fundamental engaging and promising exploratory outcomes and the up and coming extra execution testing stages they intend.

Amandeep Singh Sohal et al. [17] have presented a framework for digital security. Their structure has been completely revealed to detect the malignant edge gadgets in the haze figuring scenario. Their system employs a two-phase Markov model for early detection of potentially dangerous edge devices and legitimate edge devices. The results of their tests demonstrate the usefulness and sufficiency of their framework, which is backed up by test results. One of the main

10.48047/jocaaa.2025.34.12.12

motivations for their framework was to recover the valid edge contraption from the VHD, which could have occurred inadvertently.

Qiao Yan et al. [18] have dissected the new patterns and properties of DDoS assaults in distributed computing. They show in their analysis that SDN gives us a new way to cope with DDoS attacks under proper figuring settings and that SDN has fantastic features for countering DDoS ambushes. By that time, they were mostly talking about DDoS ambushes on SDN and how to defend against DDoS attacks in SDN. They also mentioned several issues that need to be addressed to make DDoS in SDN more manageable with adequate processing. The true purpose of this technology was to detect DDoS ambushes in the cloud employing SDNs.

Alex Akinbi et al. [19] intends to enable cloud users to evaluate their security requirements in order to pinpoint important areas inside PaaS cloud architectures where security products from CSPs can be contrasted. Thanks to a flexible security planning grid, it employs a quantitative technique to uncover numerical data that illustrates fundamental designs within the PaaS scenario where security may be analyzed and security controls looked at to meet these security needs. Depending on the particular security needs and administrative level objectives that PaaS cloud customers have established, the framework can be tailored for different PaaS cloud models.

Debiao He et al [20], using a personality-based mark conspiracy, create a new PAA plot for MCC administrations. According to a security investigation, the proposed PAA scheme can address the true security difficulties in Tsai and Lo's plan and meet the security requirements for MCC administrations. The proposed PAA plot has lower calculation and correspondence costs than Tsai and Lo's PAA plot, according to the presentation evaluation. This investigation reveals that Tsai and Lo's PAA scheme is impotent in the face of a real attack and is unable to maintain client anonymity. Another PAA conspire for MCC administrations is presented in paper [12] to understand such genuine flaws. Tsai and Lo's PAA plot has a security issue, which can be addressed by examining the security of the newly introduced PAA plan. Furthermore, according to the presentation investigation, our proposed PAA plot has preferred execution over their PAA plot.

Kyriakos Kritikos et al. [21] tackles both security issues by presenting a new model-driven approach and engineering that guarantees multiple cloud phases, gives clients their own private area, and guarantees that application configurations are created in compliance with and uphold a particular client-required security level. This answer leverages innovations in safe model administration, security programming, and state-of-the-art security standards. Additionally, it offers a range of access control situations, including online, external, and automated client validation.

3. PROPOSED METHODOLOGY

The cloud environment is a gathering of states to provide on-demand organizations to cloud customers. Access to the cloud is provided via the web, making data stored on the cloud more accessible to internal and external intruders. Because every regular customer uses cloud conditions, there's a good chance that may occur. Different discovery frameworks are presented to identify attack information. Regardless, those procedures do not produce unearthly results that are susceptible to detection and false negative rates. An efficient DOS attack detection system employing a combination of oppositional crow search algorithm and recurrent neural network (OCSA+RNN) was developed to address the above issue. Improve the security of the PaaS network platform even more. This study proposes a technique that includes low weight attribute-based encryption (LW-ABE). OCSA was used to select feature data, and the RNN classifier was used to classify it. The important features are first picked using the OCSA method. The RNN classifier is then given the selected features. The incoming data is categorised using an RNN classifier throughout the testing process. Finally, the attack data is deleted and the normal data is preserved in the cloud. After the attacks have been removed, the normal data is moved to the final stage of the process: security enhancement. A lightweight attribute-based encryption mechanism is utilized to ensure security.

10.48047/jocaaa.2025.34.12.12

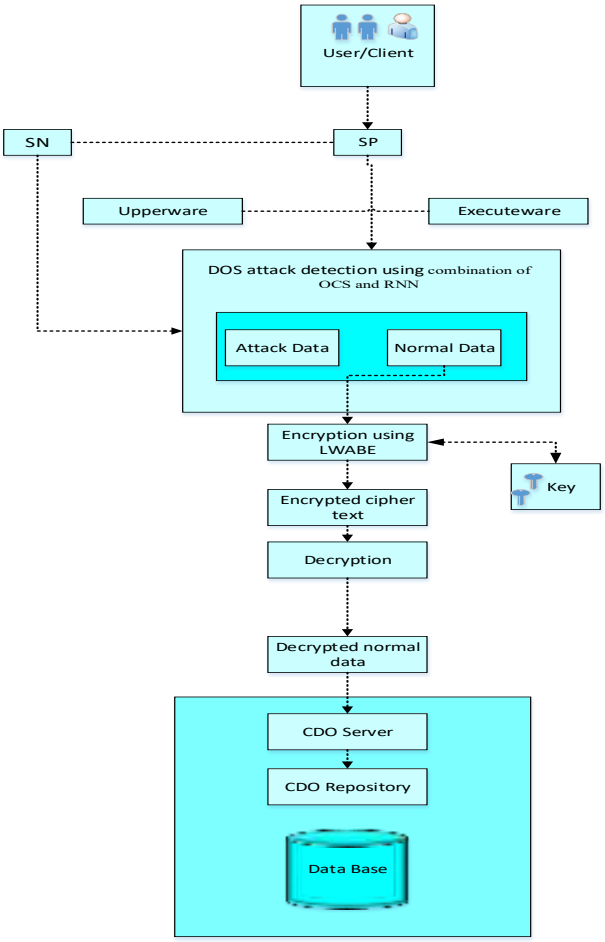

Figure 1: Overall system architecture for PaaS security enhancement

As shown in Figure 1, the PaaS has two main route focuses to enable users to benefit from its features. The Service Point (SP) is a RESTful service that provides clients with platform services that enable them to handle the whole diverse application provisioning process or stand-alone lifecycle tasks. The core stage modules and components of the provisioning process are now orchestrated by SP. Although this service is suitable for automatic associations, it is not meant for direct use. The next entry point enhances the SP to give platform consumers a more interesting experience. This is acknowledged by the Social Network (SN). Other kinds of external user interfaces or IDEs, on the other hand, may be used for comparison or, in any event, to offer the user more value (e.g., billing, examination, or model modifying services). Along with standard social network features, the SN enables users to read program execution narratives, start application deployment work procedures, and track the progress of deployment assignments. Additionally, it makes it possible to share information about application models, metric specifications, adaptation rule models, and encouraging deployment practices for applications that are similar or identical. In a recent study, security enhancement and the PaaS domain based on three five modules were improved by employing Upperware, Executeware, Access control with fuzzy, and Security with Trust base signature. This is explained in further depth in [22].

In addition to detecting DOS assaults, further increase the security of its PaaS platform. The oppositional crow search algorithm and recurrent neural network (OCSA+RNN) are combined in this study. Fuzzy provided user/client access controls in earlier work. The PaaS platform provides the access control user with the necessary data. Following that, TBS is used to safeguard the user-accessed data. The user-accessed data is pre-processed in our work so that OCSA can choose the feature data in the best possible way. All of these data then proceed to the next phase of attack detection. RNN distinguishes between normal and attacked data. At last, only the regular data is moved to the next stage of security upgrading, while the attacked data is eliminated. The idea, which combines the recurrent neural network (RNN) with the antagonistic crow search method, is explained in full below.

3.1. Pre-processing

The data accessed by the user/client is pre-processed in this step. The data values are in many formats, including nominal, binary, and numeric. Detection and classification processes are problematic when dealing with multiple formats of data. As a result, we pre-process the supplied dataset. Redundancy data and null values are removed during pre-processing, and category data is turned into numerical data. The output data is supplied to further processing after pre-processing.

3.2. Combination of oppositional crow search algorithm and recurrent neural network (OCSA+RNN)

10.48047/jocaaa.2025.34.12.12

After the pre-processing, we select the main features using the oppositional crow search algorithm (OCSA). OCSA is a combination of the crow search algorithm (CSA) and opposition-based learning (OBL). We used an OBL approach in conjunction with CSA to enhance its searching capabilities [23]. Crow intelligence and characteristics serve as the foundation for the CSA. A detailed explanation of the recommended feature selection process can be found below.

Step 1: Initialization

The initialization stage of the optimization problem is crucial. Initially, we select data and attributes at random from the original number of user/client data at this step. The length of the crow is N if the total amount of user data is N. The letter crow symbolises the solution. The crows are written in the manner described in equation 1, and the solution is depicted in picture 3.

$$C_i = \begin{bmatrix} A_{11} & A_{12} \ldots\ldots A_{1D} \\ A_{21} & A_{22} \ldots\ldots A_{2D} \\ A_{n1} & A_{n2} \ldots\ldots A_{nD} \end{bmatrix} \quad (1)$$

	D1	D2	D3	D4		D4
C1	1	0	1	0	·····	1
C2	0	0	1	1	·····	0
⋮	⋮	⋮	⋮	⋮	⋮	⋮
Cn	1	0	1	0	·····	1

Figure 2: Solution representation for CSA based feature data selection

The sample solution encoding process is given in figure 3. In this work N=41 (i.e., number of attributes available in dataset is 41). The crows are randomly initialized to either 0 or 1. Here, if the i^{th} position of a crow is 0 then it represents that i^{th} user data does not select for classification process. Else if it is 1 then the i^{th} user data is selected for classification process.

Step 2: Opposite solution generation

For every solution C_i has a unique opposite solution OC_i. The opposite solution $OC(A_1', A_2', \ldots, A_n')$ is calculated given as follow;

$$A_i' = a_i + b_i - A_i \; i \in 1,2,\ldots,n \quad (2)$$

$$OP_i = \begin{bmatrix} A_{11}' & A_{12}' \ldots\ldots A_{1D}' \\ A_{21}' & A_{22}' \ldots\ldots A_{2D}' \\ A_{n1}' & A_{n2}' \ldots\ldots A_{nD}' \end{bmatrix} \quad (3)$$

Step 3: Fitness calculation

Following the solution initialization, we determine the fitness of the initial and opposite solutions. Every crow location is evaluated using a fitness function at each iteration. In CSA, the fitness computation is critical. It is used to assess the ability (quality) of candidate solutions. The accuracy measure is used to determine the fitness function in this research. Each crow's fitness is calculated separately. The fitness is calculated for each iteration using equation (14),

$$\text{Fitness} = \frac{\text{TP}}{\text{TP} + \text{FP})} \quad (4)$$

Where, TP → True positive, FP → False positive.

Step 4: Updation base on CSA

The updating of crow positions using CSA is shown in equation after fitness calculations (5).

$$B_j(k) = \sum_{i=1}^{n} \beta_{ij} H_i(k), \qquad j = 1,\ldots\ldots\ldots n \quad (5)$$

10.48047/jocaaa.2025.34.12.12

$$S_m^{t+1} = \begin{cases} if\ \ R_n \geq P_n^t & update\ \ position\ \ by\ \ u\sin g\ \ equation\ (1) \\ else & update to\ \ random\ \ position \end{cases}$$

Step 5: Termination criteria

The optimization process is completed when the maximum number of emphases is reached or the best solution is found. This work employs a wide range of emphases. The pseudo code for the OCSA algorithm-based feature data selection is shown in Table 1.

Start
Define population size (N), the extreme quantity iteration (K), Flight length (FL) and awareness probability P_n .
Randomly initialize the positions of the flock of crows (refer figure 2)
Calculate the opposite location of the flock of crows (refer Eq. (2))
Initialize and record the crow's memories.
Set the iteration count k=1
While (the termination criterion is not satisfied)
For i=1…N
Arbitrarily select one of the crows to follow (nth crow)
Create R_n
If $R_n \geq P_n^t$
Update solution using

$$B_j(k) = \sum_{i=1}^{n} \beta_{ij} H_i(k), \qquad j = 1,.....n$$

Else
Update random position
End if
End for i
Calculate the latest location of the crows
Update the memories of crow individuals
End while
Select the best position and visualize the results
End

Table 1: Proposed OCSA-based feature data selection pseudocode

After feature data selection, all the user/client data are move to the RNN. RNN detect DOS attack and classifies attacked data as well as the normal data. The whole concept are explained in detailed as the following section.

3.3. Attack detection using recurrent neural network (RNN):

After the feature data selection process, we employ a recurrent neural network to determine whether the packet is normal or intruded [24]. RNNs are specialized neural networks that are used to classify, predict, and recognize objects. The RNN's input is provided with the selected data features. Here, the input layers to hidden layer weights are specified as $(w_{11}, w_{12}, ..., w_{1n})$ and $(w_{21}, w_{22}, ...w_{2n})$. The random weights of the recurrent layer and the output layer neuron are generated in the specified interval $[w_{\min}, w_{\max}]$. The weight of the input layer neurons is set to unity. The back propagation through time delay (BPTT) technique with Bayesian regulation is used to train the RNN. The backward and forward passes are essential to the RNN technique. The following is a step-by-step guide to the procedure:

Step 1: Initially, we give the weights to the chosen attributes Ai and start them in the input layer.

Step 2: Typically, an RNN can be expressed using the equations (6) and (7) below.

10.48047/jocaaa.2025.34.12.12

$$x_i(t) = \sum_j y_j(t) w_{ij}(t) \quad (6)$$

$$y_i(t) = f_i(x_i(t)) \quad (7)$$

Where, y_i and w_{ij} specifies the neuron's activation state i at a time t and optimize weights value. The activation function f_i is based on the inputs of the network and context layer inputs.

Step 3: The decision vector (8) is obtained by passing the hidden node activation function through the sigmoid function, which is given as an equation.

$$f_i = \frac{1}{1+e^{(-x_i)}} \quad (8)$$

Where $i = 1,2$ and the RNN output is $Y^{act} = W_{2i} f_i$ for a single output system output weight matrix.

Step 4: In the forward technique of backpropagation, the function (9) is used to determine the output of each neuron (10),

$$y_i(t) = f_i(x_i(t), C_i(t)) \quad (9)$$

$$x_i(t) = \sum_{j \in H} y_j(t) w_{ij} + \sum_{j \in I} x_j(t) w_{ij} + \sum_{j \in C} y_j(t - \tau_{ij}) wij \quad (10)$$

Where, f, H, I and C represents the activation function of a neuron, hidden layer values, input neurons values, the values of the neuron which store in data on the last network stage. Then x_j is j^{th} input neuron and τ_{ij} is an integer value referring the displacement in recurrent connection through the times.

Step 5: The backpropagation error is found from the equation (11),

$$E_m = Y^{tar} - Y^{act} \quad (11)$$

The Bayesian Regularization method can be used to reduce the error.

Step 6: The bias values and weight are updated in this function (12).

$$E_d = \frac{1}{N} \sum_{i=1}^{N} \left((E_m)^2 \right) \quad (12)$$

Step 7: For updating the weights, this equation is expanded in the equation (13),

$$B_r = \beta E_d + \alpha E_w \quad (13)$$

Here the total of squares of the network weights is E_w. Then α and β are the parameters that is to be optimized in the Bayesian framework. Until BP error gets minimized to the lowest value, If not, the procedure is performed again. The well trained networks are attained from the neural network process's output. After detection and classification, attacked data are removed, and the normal data are transferred to the next phase of security enhancement. The whole concepts are explained in detailed as followings section;

3.4. PaaS platform security enhancement based on lightweight-attribute based encryption (LW-ABE):

ABE is one of the open key cryptographic frameworks that consistently conveys information sharing between numerous users, which can accomplish both protection and access control. In this, encryption and decryption utilizing qualities like user/client information just as user's secret keys, which are connected with an access policy. When the client accreditations fulfill the access policy, only the user decrypts the encrypted data. In this, the encryption depends on set of characteristics. There are three entertainers for the encryption and decryption process: the data owner and the data user. In this, Authority which produces a public key, additionally creates a master secret key. In the wake of producing a public key it will send it to the data owner for encryption process. As indicated by the attributes, authority produces secret user keys with the master secret key. In view of the public key data, the owner encrypt the information alongside the attributes after finishing its encryption procedure the encoded information is put away into the cloud stage just as dependent on the lightweight cryptography the public keys likewise encoded.

At this time, the combined LW-ABE procedure happens [25]. The necessary information's are decoded and the data users get the private key from the authority. The information disentangling is possible exactly when in any event, d component of the qualities in the encoded information are arranged with attribute authority in the secret key in any event. In case any user needs to incorporate the framework, the approved user that is authorized user will reclassify as make the keys again. The accompanying figure speaks to the ABE procedure;

10.48047/jocaaa.2025.34.12.12

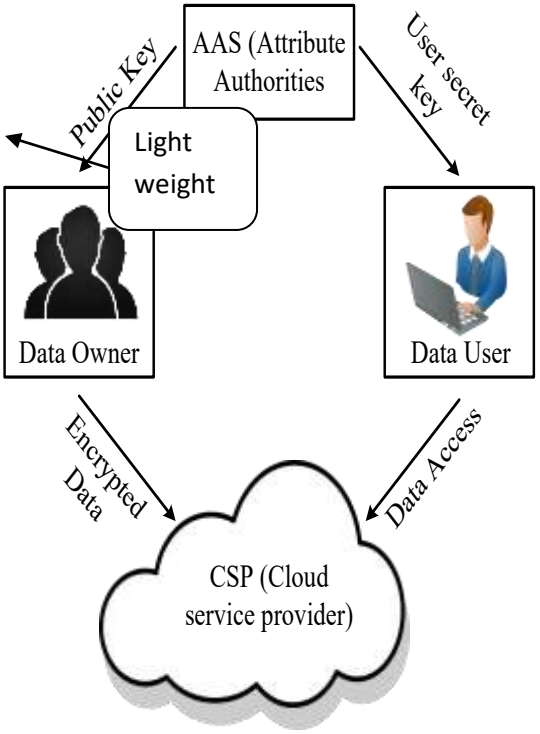

Figure 2: Overview of LW-ABE

3.4.1 Attribute Authorities:

Every AA is a self-contained attribute authority in charge of handling customer attributes. The proportional AA's can entitle, discredit, and update customer's qualities in its region based on the customer's lead spot in any instance personality. In this case, attributes are linked to a single AA; however, each AA can control an arbitrary number of attributes. Each AA distributes its public key, just as each attribute distributes hidden keys to customers that reflect their qualities.

3.4.2 Cloud Service Providers:

Cloud service providers provide data storage services to data owners and data access services for clients. It also serves as a source of computer power. When an attribute is revoked or a policy is updated, CSP assists DOs in re-encrypting and updating their cypher text. The cloud service provider is semi-trusted because it is interested in the data messages it receives. However, it will truly carry out the responsibilities assigned to it by authentic parties in the framework.

3.4.3 Data Owner (DO):

Before moving information files to the Cloud Service Provider, DO characterizes the access policy over attributes from that point. Forward the information could be encoded under access policy. DO doesn't relies upon the Cloud Service Provider to do information get to control. Customers with different characteristics gain distinctive interpreting benefits, and thus the access control happens inside the cryptography.

3.4.4 User:

Every client is distributed with complete independence just as described with part of properties. In this, the clients will request their attributes with important secret keys from comparable characteristic specialists. Cipher text is downloaded from the cloud specialist co-op, and chooses whether to redistribute decoding. Just the clients whose attributes satisfy the access policy can decrypt the encrypted information using their secret keys.

In this plan, there are four procedures to be executed which are named as; Setup, KeyGen, Encrypt, as well as Decrypt. Let A1 and A2 be two bilinear associations of prime order 'PO', let 'g' be a generator of A1. Furthermore, let e: A1×A1 →A2 signify the bilinear map, let 'TV' be a threshold value.

3.5. Lightweight Attribute based Encryption Algorithm Scheme:

3.5.1 Set up (TV):

In this, the attribute authority equivalently as well as randomly selects $u_1 \dots u_n$, x from Z_q and issues public key as PBK = $G_1 = g^{u1} \dots, G_n = g^{un}, X = E(e,e)^x$). the master key is represented as, MRK=$(u_1 \dots u_n, x)$.

3.5.2 Key Gen (AAU, PRK, MRK):

In this the attribute authority produces and executes the private key (PRK) for the data user DU. Also encrypt the public keys based on lightweight cryptography. Here, randomly selects TV – 1 degree polynomial D_{pq} such that $D_{pq}(0)$ = x. the private key of the data user N is represented as, $\left\{N_j = g^{\frac{TV(j)}{u_j}}\right\} \forall i \in AAU$.

10.48047/jocaaa.2025.34.12.12

3.5.3 Encryption (A_{ED}, PBK, MES):
In this, they DO encrypt the message, which is represented as $MES \in A2$ with a set of attributesA_{ED}. Selects a random number$H \in Z_Q$, as well as the encrypted data is distributed as $ED = (A_{ED}, V = HX^H = E(e,e)^{xH}, \{V_j = g^{u_j H}\} \forall j \in AAU)$.

3.5.4 Decryption(ED, PBK, N):
In this, the encrypted data ED with the private key N is decrypted by the data user. Selects the TV attributes from $j \in AAU \cap A_{ED}$ to calculate $e(V_j, N_j) = E(e,e)^{q(j)H}$ if $|AU \cap A_{ED}| \geq TV$.
Then calculate $R^H = E(e,e)^{q(0)H} = E(e,e)^{RH}$ through the LaGrange co-efficient as well as finally obtained the message is $= {}^{V}/_{R}{}^{H}$.
After decryption, the decrypted normal data are moved to the CDO server, and different processes are explained in the research paper [22].

4.RESULTS AND DISCUSSION

The suggested DOS attack detection and PaaS platform security upgrade in cloud computing using the OCSA and LW-ABE procedures in this section. We tested our suggested DOS attack detection and security upgrade using Java(jdk 1.6) and cloud Sim devices on a PC running Windows 7 @ 2 GHz dual-centre PC with 4 GB RAM running a 64-bit version of Windows 2007.

4.2. Evaluation Metrics:

A set of performance indicators is used to evaluate the suggested strategy's efficacy.
.
Accuracy: The sensitivity and specificity metrics are used to calculate accuracy. It's written as follows:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \times 100 \tag{14}$$

False Positive Rate (FPR): The FPR is calculated by dividing the total number of negative predictions by the number of incorrect positive predictions. It can alternatively be calculated as 1-specificity.

$$FPR = \frac{FP}{FP + TN} \tag{14}$$

4.3. Comparative Analysis:

Our suggested methodology's primary focus is on detecting DOS attacks and improving PaaS platform security using OCSA and LW-ABE. Existing Decision-Tree, SVM, MSVM, CAMEL, and ECCTS results are contrasted with the suggested outcome. The performance of the suggested method with this configuration is displayed in the accompanying figure.

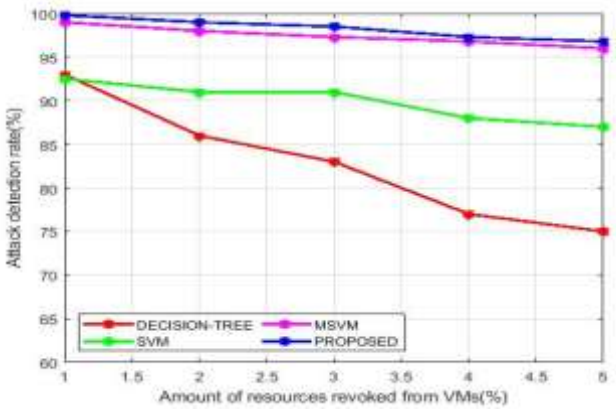

Figure 3: Performance analysis of attack detection rate

10.48047/jocaaa.2025.34.12.12

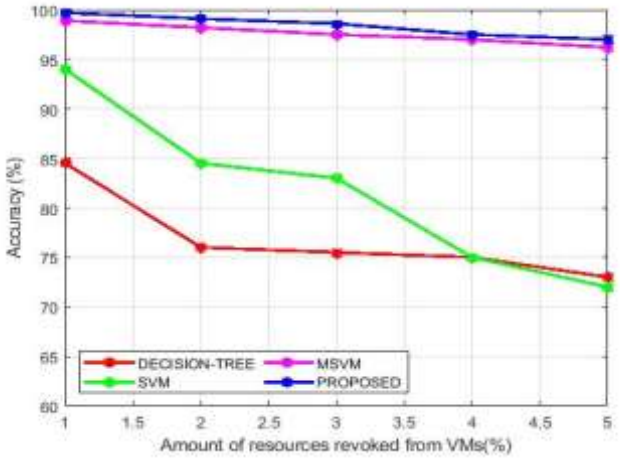

Figure 4: Performance analysis of accuracy

Figures 3 and 4 show that the suggested model's average accuracy and attack detection rates at various percentages of revoked resources are 99.02 and 99.4 percent, respectively. The accuracy and attack detection rates of a proposed method are contrasted with those of the current Decision-Tree, SVM, and MSVM methodologies in the graph above. The suggested approach produces the greatest results in terms of accuracy and attack detection rate when looking at figures 3 and 4. In terms of outcomes, our suggested approach performs better than other current alternatives.

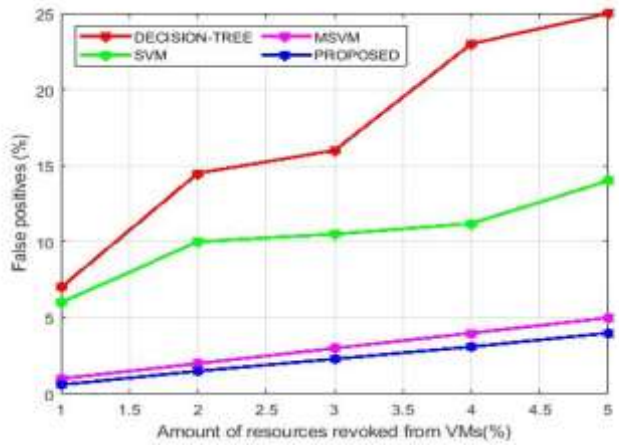

Figure 5: Performance analysis of false positive rate

The aforementioned graph contrasts the false positive rate of a proposed method with that of the current decision-tree, SVM, and MSVM techniques. In terms of outcomes, our suggested approach performs better than other current alternatives.

.

10.48047/jocaaa.2025.34.12.12

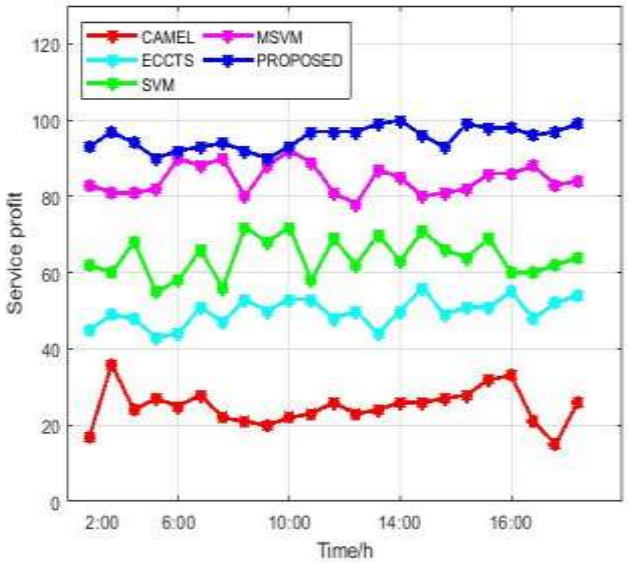

Figure 6: Analysis of service profit comparisons for Monday through Friday 1

Figure 6 compares our suggested methods with CAMEL, ECCTS, SVM, and MSVM. Our suggested methodology produces high-quality results when compared to the aforementioned existing methodologies. The aforementioned statistic details the service profitability for Monday through Friday1. The service profit in OCSA and LW-ABE comes before the service profit in CAMEL, ECCTS, SVM, and MSVM since the system in the suggested method uses the same infrastructure and the service in OCSA and LW-ABE is smoother than that in CAMEL, ECCTS, SVM, and MSVM. Because a telecommunications service is busier during the week, we find that service profit during the vacation season is larger than on Mondays and Fridays.

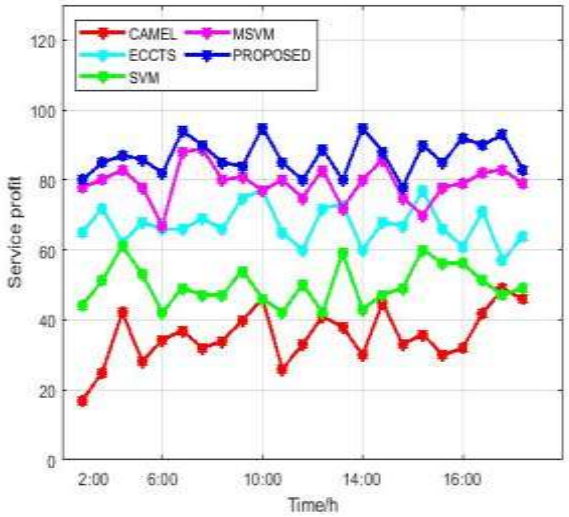

Figure 7: Comparative evaluation of Monday through Friday consumer satisfaction

Figure 7 compares our suggested methods with CAMEL, ECCTS, SVM, and MSVM. Our suggested methodology produces high-quality results when compared to the aforementioned existing methodologies. The accompanying graphic details a comparative analysis of user satisfaction from Monday through Friday. Additionally, Fig. 7 shows that user satisfaction in OCSA and LW-ABE is higher than that in CAMEL, ECCTS, SVM, and MSVM. The reason for this is that CAMEL, ECCTS, SVM, and MSVM have busier application services than OCSA and LW-ABE. Furthermore, weekdays and weekends see a higher usage of the telecommunications service than weekends and holidays. Because of this, users are happier on holidays than they are throughout the workday.

10.48047/jocaaa.2025.34.12.12

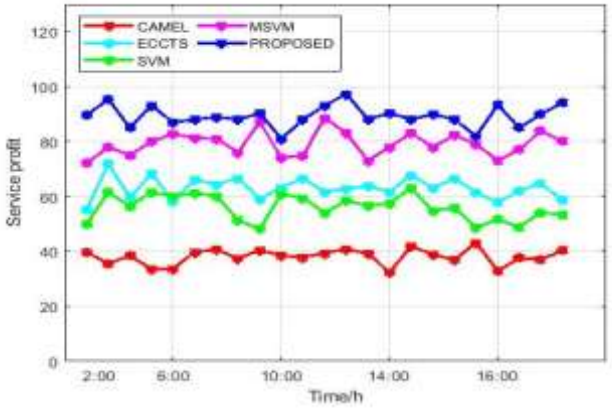

Figure 8: Comparative analysis of service utility in Monday to Friday 3

From Fig. 8, The service utility in proposed comes before the service utility in CAMEL, ECCTS, SVM, and MSVM, as we can also prove. Additionally, we can observe that the line is more relaxed in OCSA and LW-ABE. Therefore, the special security model works better than a standard telecommunications service. The effectiveness and safety of a telecommunications service can be guaranteed by the novel security mechanism, per the preliminary security and benefits analysis. Figure 8 illustrates how our suggested procedure produces high-quality results.

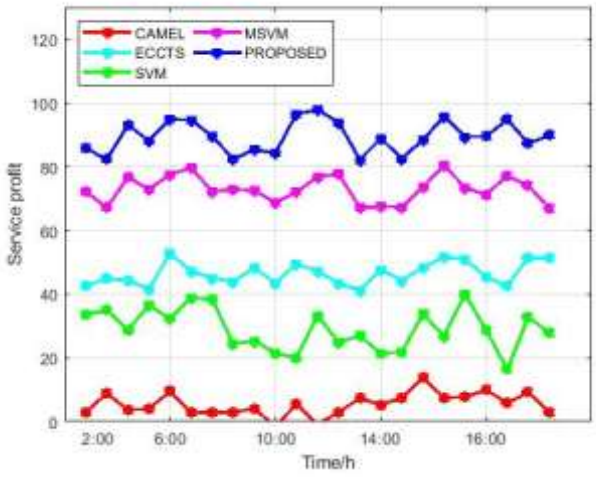

Figure 9: Service profit comparison from Saturday to Sunday 1

Because the system and the suggested methodology share the same infrastructure, and because the service in OCSA & LW-ABE is smoother than that in existing approaches, we can see from Fig. 9 that the service profit in the proposed methodology comes before the service profit in CAMEL, ECCTS, SVM, and MSVM. In the meantime, we find that because a telecommunications service is busier throughout the week, service profit is higher during the holiday season than it is on Saturday and Sunday. Figure 9 illustrates how our suggested procedure yields a high-quality outcome.

10.48047/jocaaa.2025.34.12.12

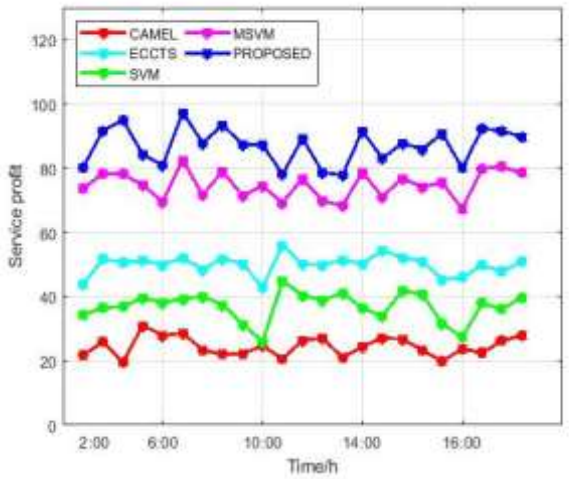

Figure 10: A comparison of Saturday and Sunday 2 consumer satisfaction

Figure 10 compares our suggested methods with CAMEL, ECCTS, SVM, and MSVM. Our methodology produces high-quality results when compared to the aforementioned existing methodologies. The above graphic details a comparative examination of user satisfaction from Saturday to Sunday 2. Additionally, Fig. 10 shows that user satisfaction in OCSA and LW-ABE is higher than that in CAMEL, ECCTS, SVM, and MSVM. This is due to the fact that the applied service of the current approach is busier than that of OCSA and LW-ABE. Additionally, the number of people using the telecommunications service is higher on Saturdays and Sundays than on weekends and holidays. Because of this, users are happier on holidays than they are throughout the workday.

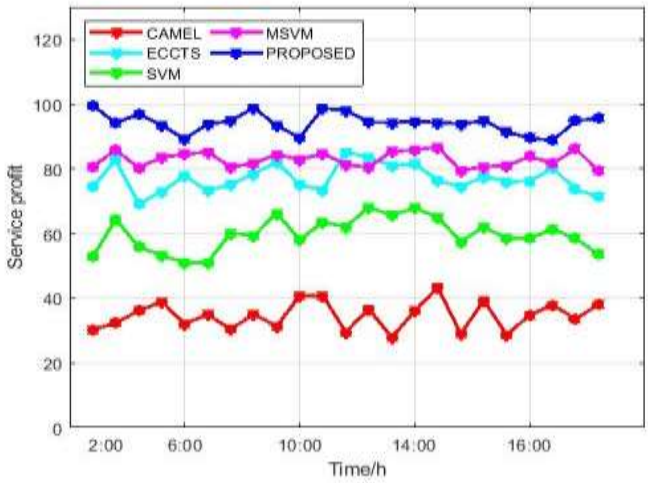

Figure 11: Service utility comparison from Saturday to Sunday 3

According to Fig. 11, the service utility in OCSA & LW-ABE is in front of the service utility in CAMEL, ECCTS, SVM, and MSVM. Additionally, we can observe that the line is more relaxed in OCSA and LW-ABE. Consequently, the new security model performs better than conventional telecommunications services. The effectiveness and safety of a communications service can be guaranteed by the new security mechanism, based on the security above and the benefit analysis. Figure 10 analysis indicates that our suggested process yields a high-quality outcome.

.

10.48047/jocaaa.2025.34.12.12

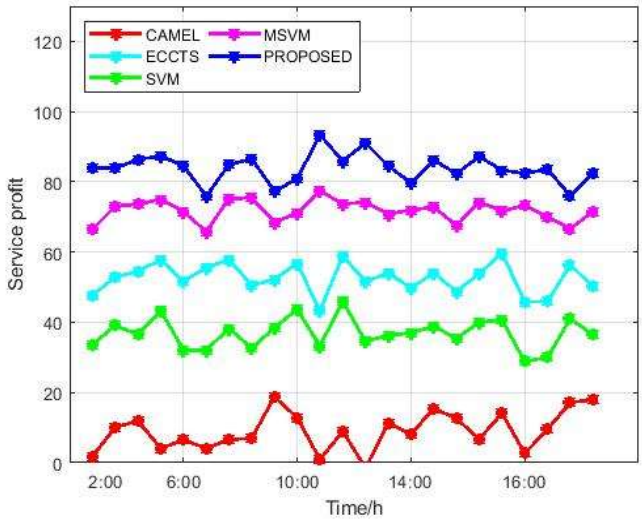

Figure 12: Comparative evaluation of holiday 1's service profit

Because the system in the suggested technique uses the same infrastructure and the service in OCSA & LW-ABE is smoother than that in CAMEL, ECCTS, SVM, and MSVM, we can see from Fig. 12 that the service profit in OCSA & LW-ABE comes before the service profit in CAMEL, ECCTS, SVM, and MSVM. Our suggested methodology produces a high-quality result based on an analysis of Figure 8.

.

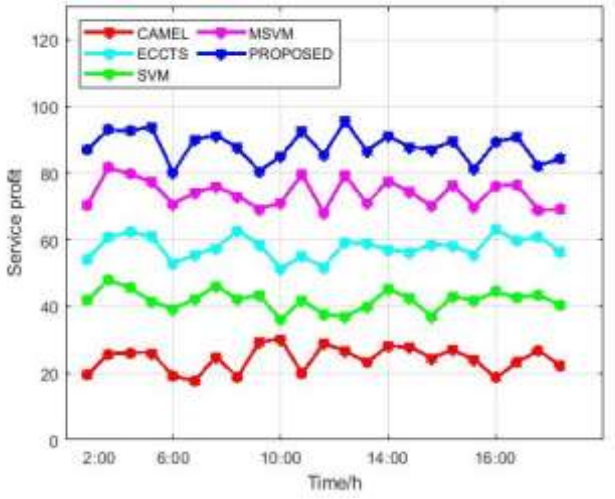

Figure 13: Comparative analysis of consumer satisfaction during holiday two

Figure 13 compares our suggested methods with CAMEL, ECCTS, SVM, and MSVM. Our suggested methodology produces high-quality results when compared to the aforementioned existing methodologies. The graphic above details comparative evaluations of customer satisfaction during holiday 2. According to Fig. 13, user satisfaction in OCSA & LW-ABE is higher than that in CAMEL, ECCTS, SVM, and MSVM. This is because OCSA and LW-ABE have busier application services than CAMEL, ECCTS, SVM, and MSVM.

10.48047/jocaaa.2025.34.12.12

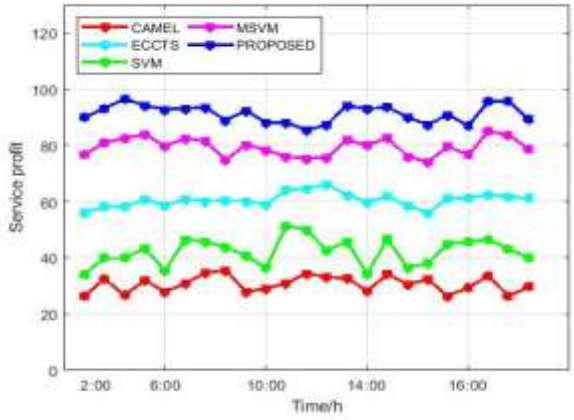

Figure 14: Comparative evaluation of Holiday 3's service utility

We can discover that our suggested service utility comes before that of CAMEL, ECCTS, SVM, and MSVM. Additionally, we observe that the line in LW-ABE and OCSA is calmer. Consequently, the new security model performs better than conventional telecommunications services. Our suggested methodology produces excellent results based on our analysis of Figure 14.

5.CONCLUSION

System security is becoming one of the most important topics due to the numerous attacks and vulnerabilities on the internet. Detecting DOS attacks is therefore an essential part of system security. In this research, we propose a PaaS security enhancement method and a cloud-based DOS attack detection system that integrates OCSA and RNN. One metaheuristic algorithm for selecting feature data is the OCSA. The OBL and CSA algorithms are combined in the OCSA algorithm. The provided user/client data properties are classified using the RNN classifier. The suggested outcome is contrasted with a number of approaches and some earlier research. The results of our suggested methodology are superior to those of earlier studies.

Platform-as-a-Service (PaaS) has become an essential cloud delivery model, providing developers with a scalable, adaptable, and economical environment for application deployment. The shared and multi-tenant characteristics of PaaS create distinct vulnerabilities, especially to Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, which jeopardize service availability and economic viability. Literature indicates that classic perimeter-based defenses offer limited security and are inadequate for contemporary cloud-native platforms characterized by intricate APIs, service meshes, and dynamic autoscaling methods.

Improving security in PaaS platforms necessitates a multi-tiered defense strategy. Provider-level safeguards, like Web Application Firewalls (WAFs) and CDN-based scrubbing, must be augmented with in-cluster strategies, such as ingress rate limitation, service mesh resilience capabilities, and kernel-level packet filtering utilizing technologies like eBPF/XDP. Simultaneously, machine learning and deep learning models have demonstrated efficacy in identifying abnormalities and distinguishing between malicious floods and legitimate high-traffic workloads; nonetheless, issues such as dataset quality, concept drift, and adversarial evasion persist.

Equally crucial is the necessity for cost-conscious defenses against Economic Denial of Sustainability (EDoS), wherein adversaries leverage cloud flexibility to escalate operational costs. Incorporating anomaly detection into autoscaling policies, implementing surge limits, and employing challenge-response mechanisms (such as proof-of-work and CAPTCHAs) are essential measures in combating this emerging threat.

Research and industry findings consistently indicate that PaaS security augmentation must be comprehensive, encompassing the network, application, and control planes, while maintaining a balance among availability, performance, and cost. Future endeavors should concentrate on creating authentic cloud-native datasets, adaptive machine learning-driven detection algorithms, and enhancing alignment between cloud providers and tenants on shared accountability. PaaS platforms can successfully combat DoS/EDoS threats and offer secure, reliable cloud services through the integration of proactive monitoring, intelligent detection, and resilient architecture.

10.48047/jocaaa.2025.34.12.12

DECLARATION OF STATEMENT

This work is partially supported by Our BRICS and NRF grants

REFERENCES

[1] J. Hwang, Toward beneficial transformation of enterprise workloads to hybrid clouds, IEEE Transactions on Network & Service Management, 2016.
[2] Somani, Gaurav, Manoj Singh Gaur, Dheeraj Sanghi, Mauro Conti, and RajkumarBuyya. "DDoS attacks in cloud computing: Issues, taxonomy, and future directions." Computer Communications, Vol. 107, pp. 30-48, 2017.
[3] García-Valls, M., Cucinotta, T., & Lu, C. "Challenges in real-time virtualization and predictable cloud computing", Journal of Systems Architecture, 2014.
[4] Vaezi, M., & Zhang, Y, "Virtualization and Cloud Computing", In Cloud Mobile Networks (pp. 11-31). Springer International Publishing, 2017.
[5] Mohamaddiah, M. H., Abdullah, A., Subramanian, S., &Hussein, M. (2014). A survey on resource allocation and monitoring in cloud computing. International Journal of Machine Learning and Computing, 4(1), 31.
[6] Subashini, Subashini, and VeerarunaKavitha, "A survey on security issues in service delivery models of cloud computing," Journal of network and computer applications, Vol. 34, No. 1, pp.1-11, 2011.
[7] Modi, Chirag, Dhiren Patel, BhaveshBorisaniya, Hiren Patel, Avi Patel, and MuttukrishnanRajarajan, "A survey of intrusion detection techniques in the cloud," Journal of network and computer applications, Vol. 36, No. 1, pp.42-57, 2013.
[8] Wang, Bing, Yao Zheng, Wenjing Lou, and Y. Thomas Hou, "DDoS attack protection in the era of cloud computing and software-defined networking," Computer Networks, Vol. 81, pp.308-319, 2015.
[9] Modi, Chirag, Dhiren Patel, BhaveshBorisaniya, Avi Patel, and MuttukrishnanRajarajan, "A survey on security issues and solutions at different layers of Cloud computing." The Journal of Supercomputing, Vol. 63, No. 2, pp.561-592., 2013.
[10] Girma, Anteneh, Moses Garuba, Jiang Li, and Chunmei Liu, "Analysis of DDoS attacks and an introduction of a hybrid statistical model to detect DDoS attacks on cloud computing environment." In Information Technology-New Generations (ITNG), in process of 12th International Conference, pp. 212-217, 2015.
[11] Yu, Shui, YonghongTian, Song Guo, and Dapeng Oliver Wu, "Can we beat DDoS attacks in clouds," IEEE Transactions on Parallel and Distributed Systems, Vol. 25, No. 9, pp. 2245-2254, 2014.
[12] N. P. C. Priya, "Security Management in Inter-Cloud," Int. J. Emerg. Trending Trends TechinologyComput. Sci., 2012. [13]D., Zissis, D., Lekkas, "Addressing cloud computing security issues". Future Generation Computer Systems, 2012.
[14] Jesus Luna, Ahmed Taha, "Quantitative Reasoning About Cloud Security Using Service Level Agreements", IEEE Transactions on Cloud Computing, 2014.
[15] Victor Chang, Muthu Ramachandran, "Towards achieving Data Security with the Cloud Computing Adoption Framework", IEEE Transactions on Services Computing, 2015.
[16] Sohal, Amandeep Singh, Rajinder Sandhu, Sandeep K. Sood, and Victor Chang, "A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments." Computers & Security, Vol. 74, pp.340-354, 2018.
[17] Girma, Anteneh, Mosses Garuba, and RajiniGoel, "Advanced machine language approach to detect DDoS attack using DBSCAN clustering technology with entropy," In Information Technology-New Generations, pp. 125-131, Cham, 2018.
[18] Yan, Qiao, and F. Richard Yu, "Distributed denial of service attacks in software-defined networking with cloud computing," IEEE Communications Magazine, Vol. 53, no. 4, pp.52-59, 2015.
[19] Alex Akinbi; Ella Pereira, "Mapping Security Requirements to Identify Critical Security Areas of Focus in PaaS Cloud Models", Computing and Communications,2015.
[20] Debian He, Neeraj Kumar, "Efficient Privacy-Aware Authentication Scheme for Mobile Cloud Computing Services", IEEE Systems Journal, Volume: 12, Issue: 2, June 2018.
[21] Kyriakos Kritikos, Tom Kirkham, "Towards a Security-Enhanced PaaS Platform for Multi-Cloud Applications", Future Generation Computer Systems, 6 October 2016.
[22] Kyriakos Kritikos, Tom Kirkham, "Towards a Security-Enhanced PaaS Platform for Multi-Cloud Applications", Future Generation Computer Systems, August 10, 2016.
[23] Wim De Mulder, Steven Bethard and Marie-Francine Moens, "A survey on the application of recurrent neural networks to statistical language modeling", Journal of Computer Speech and Language, 2014.
[24]Almoataz Y. Abdelaziz and Ahmed Fathy, "A novel approach based on crow search algorithm for optimal selection of conductor size in radial distribution networks", Engineering Science and Technology, an International Journal, 2017.
[25] Sana Belguith, Abderrazak Jemai,"Enhancing Data Security in Cloud Computing Using a Lightweight Cryptographic Algorithm", Autonomic and Autonomous Systems, May 2015.
[23] Ramdas Vankdothu,Dr.Mohd Abdul Hameed, Husnah Fatima" A Brain Tumor Identification and Classification Using Deep Learning based on CNN-LSTM Method" Computers and Electrical Engineering , 101 (2022) 107960
[24] Ramdas Vankdothu,.Mohd Abdul Hameed "Adaptive features selection and EDNN based brain image recognition on the internet of medical things", Computers and Electrical Engineering , 103 (2022) 108338.
[25] Ramdas Vankdothu,.Mohd Abdul Hameed,Ayesha Ameen,Raheem,Unnisa " Brain image identification and classification on Internet of Medical Things in healthcare system using support value based deep neural network" Computers and Electrical Engineering,102(2022) 108196.
[26] Ramdas Vankdothu,.Mohd Abdul Hameed" Brain tumor segmentation of MR images using SVM and fuzzy classifier in machine learning" Measurement: Sensors Journal,Volume 24, 2022, 100440 .
[27] Ramdas Vankdothu,.Mohd Abdul Hameed" Brain tumor MRI images identification and classification based on the recurrent convolutional neural network" Measurement: Sensors Journal,Volume 24, 2022, 100412 .
[28] Mohd Thousif Ahemad ,Mohd Abdul Hameed, Ramdas Vankdothu" COVID-19 detection and classification for machine learning methods using human genomic data" Measurement: Sensors Journal,Volume 24, 2022, 100537