Buletin Ilmiah Sarjana Teknik Elektro
Vol. 8, No. 1, February 2026, pp. 208-221
ISSN: 2685-9572, DOI: 10.12928/biste.v8i1.15187

Mitigating Economic Denial of Sustainability (EDoS) Attacks in Cloud Computing Using an AI-Driven Cost-Aware Defense System

Zubaidi Maytham Sahar Saeed [1], Anazida Binti Zainal [1], Fuad A. Ghaleb [2]
[1] Faculty of Computing, University of Technology Malaysia, Johor Baharu, Malaysia
[2] College of Computing, Faculty of Computing, Engineering and the Built Environment, Birmingham City University, Birmingham, United Kingdom

ARTICLE INFORMATION

Article History:

Received 03 November 2025
Revised 30 December 2025
Accepted 08 February 2026

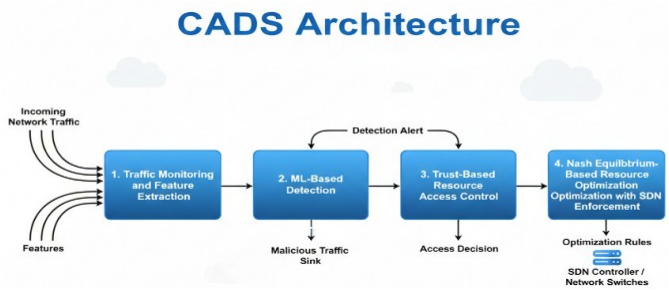
Keywords:

Economic Denial of Sustainability;
Cloud Security;
Cost-Aware Defense;
Deep Learning;
Trust-Based Access Control;
SDN

Corresponding Author:

Zubaidi Maytham Sahar Saeed, Faculty of Computing, University of Technology Malaysia, Johor Baharu, Malaysia.
Email: sahar20@graduate.utm.my

ABSTRACT



The pay-per-use billing model of cloud computing makes cloud infrastructures highly vulnerable to Economic Denial of Sustainability (EDoS) attacks, where adversaries exploit auto-scaling mechanisms to trigger excessive resource consumption and inflated operational costs. Existing mitigation approaches, such as rate limiting and conventional anomaly detection, struggle to accurately distinguish legitimate traffic from attack-traffic requests, often leading to false negative alarm and unnecessary financial overhead. This paper proposes a Cost-Aware Adaptive Defense System (CADS), a novel artificial intelligence-driven (AI-driven) defense system that integrates deep learning-based (DL-based) traffic classification, Trust-based resource access control, and Software-Defined Networking-based (SDN-based) traffic filtering to mitigate EDoS attacks while preserving economic sustainability. The Trust-based access control mechanism dynamically assigns trust scores to incoming requests and restricts suspicious entities from triggering auto-scaling, thereby preventing fraudulent resource allocation. The proposed defense system introduces a lightweight computational overhead of approximately 85 ms for detection and 210 ms for mitigation response, ensuring real-time protection with minimal performance impact. Experimental evaluation was conducted in an OpenStack-based simulated cloud environment, modeling multiple EDoS attack strategies, including HTTP flood, ICMP-based, and workload-based attacks. Results demonstrate that CADS achieves a detection performance such as 97.1% for (F1-score), 97.5% for Recall and 96.8 for Precision, indicates significantly reducing missed attacks and false alarm. More importantly, CADS reduces overall cloud billing costs by approximately 25% compared to state-of-the-art EDoS mitigation mechanisms, such as Advanced EDoS Attack Defense Shell (EDoS-ADS) and Multi-head Attention Network (MAN-EDoS). The results highlight the practical effectiveness of CADS in enhancing cloud security resilience while substantially lowering operational expenses for cloud service providers. Although CADS has not been tested in real-world environments, it demonstrates strong performance under simulated conditions. Future work will focus on large-scale real-world deployments and the integration of reinforcement learning techniques to adapt to evolving attack patterns.

Document Citation:

Z. M. S. Saeed, A. B. Zainal, and F. A. Ghaleb, "Mitigating Economic Denial of Sustainability (EDoS) Attacks in Cloud Computing Using an AI-Driven Cost-Aware Defense System" *Buletin Ilmiah Sarjana Teknik Elektro*, vol. 8, no. 1, pp. 208-221, 2026, DOI: 10.12928/biste.v8i1.15187.

1. INTRODUCTION

Cloud computing has become a fundamental paradigm for delivering scalable and on-demand computing resources, enabling organizations to deploy applications without the burden of owning and maintaining physical infrastructure [1]-[3]. However, the widespread adoption of pay-per-use billing models has introduced new security and economic vulnerabilities, most notably EDoS attacks [1],[4]-[11]. An EDoS attack aims not to disrupt service availability directly, but to exhaust a cloud tenant's financial resources by deliberately triggering excessive resource scaling and inflated operational costs.

Unlike traditional Distributed Denial of Service (DDoS) attacks, EDoS attacks exploit cloud elasticity mechanisms by generating traffic patterns that appear legitimate [7],[12]-[15]. For example, attackers may mimic flash crowd behavior, where sudden but seemingly valid surges in user requests activate auto-scaling policies. As a result, cloud systems allocate additional virtual machines and bandwidth, leading to substantial and sustained operational costs even when service availability remains intact [16]-[18]. This characteristic makes EDoS attacks particularly difficult to detect using static thresholds or signature-based defense mechanisms.

Existing EDoS mitigation techniques primarily rely on rate limiting, rule-based filtering, or conventional anomaly detection approaches. While these methods can reduce malicious traffic, they often struggle to distinguish between legitimate workload spikes and attack-driven traffic, resulting in high false positive rates or delayed response. More recent Artificial Intelligence (AI) and Deep Learning (DL)-based methods have shown promise due to their ability to learn complex and previously unseen traffic patterns, enabling more accurate detection of sophisticated and evolving EDoS strategies. However, many of these approaches focus solely on detection accuracy and overlook the economic implications of cloud auto-scaling decisions [19]-[21].

In cloud environments, adaptive scaling refers to the dynamic adjustment of computing resources in response to workload changes, including both scaling up during high demand and scaling down when traffic is identified as suspicious or malicious. Most existing EDoS defenses treat all malicious traffic equally, without considering the financial impact of allowing high-cost requests to trigger scaling actions. As a result, even accurate detection systems may still permit economically damaging traffic flows before mitigation occurs [22].

This paper addresses this gap by introducing a cost-aware perspective to EDoS mitigation. Unlike approaches that focus only on minimizing false negatives, the proposed defense system explicitly considers the economic cost associated with different traffic classes and scaling actions. High-cost traffic that disproportionately contributes to resource consumption is prioritized for restriction, ensuring that mitigation decisions directly align with financial sustainability objectives rather than purely statistical accuracy.

Recent studies have explored advanced defenses using (SDN), game-theoretic models, and ML techniques. While some recent works employ Transformer-based architectures or Deep Reinforcement Learning (DRL) for adaptive security control, these solutions often incur high computational complexity, lack explicit cost-awareness, or assume idealized threat models that limit their practical deployment in real-world cloud environments [3],[6],[23]. Consequently, there remains a need for a lightweight, economically grounded defense system that balances detection accuracy, response speed, and operational cost efficiency.

To address these challenges, this paper proposes a Cost-Aware Adaptive Defense System (CADS) that integrates DL-based traffic detection, Trust-based resource access control, and SDN-enabled traffic filtering. The defense system is designed to prevent malicious entities from triggering unnecessary auto-scaling while preserving service quality for legitimate users. Experimental evaluation demonstrates that the proposed system significantly reduces cloud billing costs while maintaining high detection accuracy and system resilience.

The research contributions of this paper are summarized as follows:

1. Problem Definition: This study formally addresses the problem of EDoS attacks as both a security and economic threat in elastic cloud environments, highlighting limitations of secutity-oriented mitigation strategies which neglected the economic side of the problem.
2. Novel Cost-Aware defense system: A novel AI-driven, cost-aware defense system is proposed that integrates DL detection with Trust-based access control to prevent financially damaging scaling actions.
3. Economic-Oriented Mitigation Strategy: Unlike conventional approaches, the proposed defense system prioritizes mitigation decisions based on traffic-induced operational cost rather than solely minimizing false alarms.
4. Comprehensive Evaluation: The effectiveness of the proposed defense system is validated through extensive experiments in a simulated cloud environment, demonstrating improved detection accuracy, reduced false alarms, and significant billing cost savings compared to existing EDoS defenses.

The remainder of this paper is organized as follows: Section 2 reviews related work on EDoS mitigation techniques. Section 3 presents the architecture and methodology of the proposed CADS defense system.

Section 4 describes the experimental setup and evaluation metrics, and discusses the results and comparative analysis, and Section 5 concludes the paper with future research directions.

2. LITERATURE REVIEW

EDoS attacks specifically target cloud computing systems by manipulating operation services to create escalating expenses for service providers. Research investigations continue into detection and mitigation strategies due to the evolving nature of these attacks.

Studies in [24]-[28] conducted primary surveys of EDoS attacks countermeasure strategies which were documented the essential requirements for addressing EDoS attacks. Research by [4] presented controlled resource access as an effective solution to stop these attacks. [29] carried out a study of ICMP-based EDoS attacks against cloud infrastructures to show performance decline and higher service expenses.

Current advancements in AI systems enabled researchers to build machine learning (ML)-based detection tools for EDoS vulnerabilities. The research in [1] utilized AI-based IDS that include multiple ML and DL algorithms to identify EDoS attacks and other attacks in cloud computing environment. [3],[6] developed dynamic detection approaches using SDN-based cloud and Recurrent Neural Networks RNN with stochastic features. The article demonstrates ML algorithms can detect EDoS attacks more effectively according to [30]. The research of [16] developed a ML framework which detected DoS attacks in cloud environments to boost security options.

Research studies have shown game theoretic models as effective solutions for addressing EDoS attacks. The researchers in [21] created EDoS Eye as a game-theoretic method for dynamic EDoS attacks analysis and defense. The research study by [31] utilized game theory to develop a model of EDoS attacks while investigating possible mitigation plans. The researchers in [22] proposed Attack Defense Shell-Pay As You Go (ADS-PAYG) as a trust-based mechanism to fight malicious operations through trust factors in cloud storage systems.

Various protection methods have emerged to address the vulnerabilities which EDoS presents. The research in [32] implemented a specific detection and mitigation solution for cloud computing infrastructure, the method combined entropy-based anomaly detection with adaptive thresholding system. Advanced EDoS Attack Defense Shell (EDoS-ADS) features serve as an innovative resilience improvement method which developed in study of [33].

While the research in [34] proposed their resource management framework as being designed to preserve cloud performance in conditions of DDoS and EDoS attacks. The study of [35] delivered a thorough review on DDoS attack tools and their defense strategies within private cloud environments. The authors in [36] created a defensive solution involving fog computing to reduce cloud network vulnerability to EDoS attacks through a lightweight system. The newly developed Multi-head Attention Network (MAN-EDoS), as introduced by [18] has enhanced the efficiency of malicious detection for EDoS attacks.

Recent innovations have not eliminated the strict challenges that persist during EDoS detection and mitigation processes. According to [37] the identification of EDoS attacks presents significant issues relative to workload and system instantiation in upcoming 5G telecommunications systems. Researchers from [38][39] employed Genetic Algorithms (GA) and Artificial Neural Networks (ANN) to study EDoS prevention alongside performing a mitigation approach evaluation.

As per [40] engineering applications with self-adaptability features on SDN infrastructure systems presents a potential solution approach for cloud security systems. The ongoing evolution of EDoS attacks requires businesses to sustain their innovation in detection along with their development of mitigation strategies. Future investigative approaches should develop a strong defense mechanism against evolving cyber threats through the integration of AI-driven models and game-theoretic approaches and trust-based mechanisms.

To better highlight the gaps in existing research, Table 1 presents a comparative analysis of key studies, their methods, strengths, and limitations. This comparison clarifies how our proposed CADS advances the state of the art by integrating AI-driven traffic classification with adaptive scaling while explicitly addressing financial sustainability.

Identified gap is that existing studies primarily focus on detection accuracy or network resilience, but few integrate adaptive scaling with financial cost-awareness. This current research proposed CADS defense system which fills this gap by combining AI-driven anomaly detection, trust-based control, and cost-aware scaling to reduce both attack impact and economic loss.

Table 1. Comparative Analysis of EDoS Mitigation Approaches

Study	Approach	Key Strengths	Limitations	Research Gap
[4]	Controlled access to cloud resources	Reduced attack impact	Limited scalability	No integration with cost models
[16]	ML-based traffic classification	Improved detection	Not evaluated for resource cost	Financial optimization missing
[22]	Trust-based ADS-PAYG	Trust-enhanced access control	Lacks adaptive response	Cost efficiency not addressed
[23]	SDN with RNN-based detection	High detection accuracy	Expensive computational overhead	No explicit cost-awareness
[24]	Survey of EDoS mitigation techniques	Early categorization of mitigation strategies	Lacked practical implementation	Need for operational frameworks
[33]	EDoS-ADS mitigation system	Enhanced resilience	High resource usage	Financial impact not optimized
[18]	Multi-head attention network	Robust anomaly detection	Focus only on detection	No integrated resource scaling

3. METHOD

This section presents the methodological design of the proposed Cost-Aware Adaptive Defense System (CADS), including threat modeling, attack simulation, system architecture, ML detection, game-theoretic optimization, trust-based access control, and system implementation. Figure 1 provides an overview of EDoS ataack simulation process, it is illustrating the life cycle of an EDoS attack in a cloud environment, from initial exploitation to eventual mitigation. The attacker first generates a surge of malicious requests, causing the cloud platform to detect a traffic spike and automatically scale out resources, which in turn inflates the victim's cloud bill. If the attack remains undetected, the autoscaling mechanism continues to allocate additional capacity and costs escalate further; once the attack is correctly identified, the defense system is activated, the malicious traffic is neutralized, and resource usage and therefore cost gradually returns toward normal levels. Figure 2 illustrates the interaction between detection, Trust evaluation, and SDN-based mitigation. This Figure 2 shows how ligetimate flow are dynamically scaled up or down, and optimized resource allocation were done by SDN controller, while detected malicious flows redirected and mitigation strategy was activated.

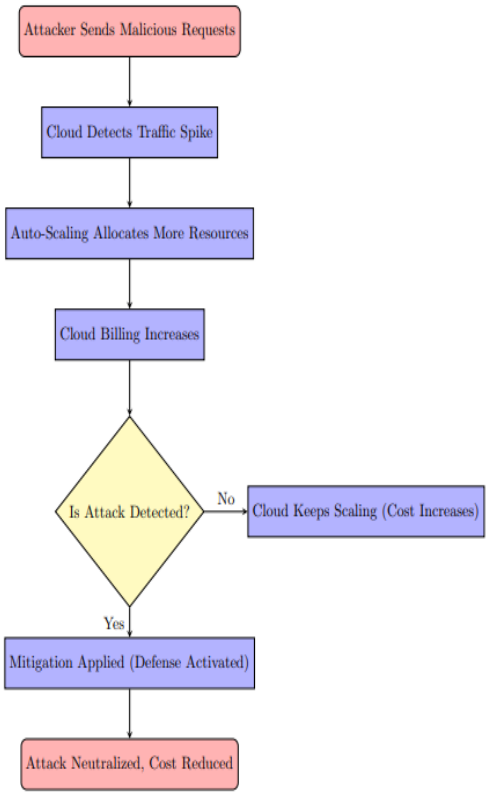


Figure 1. EDoS Attack Simulation Process

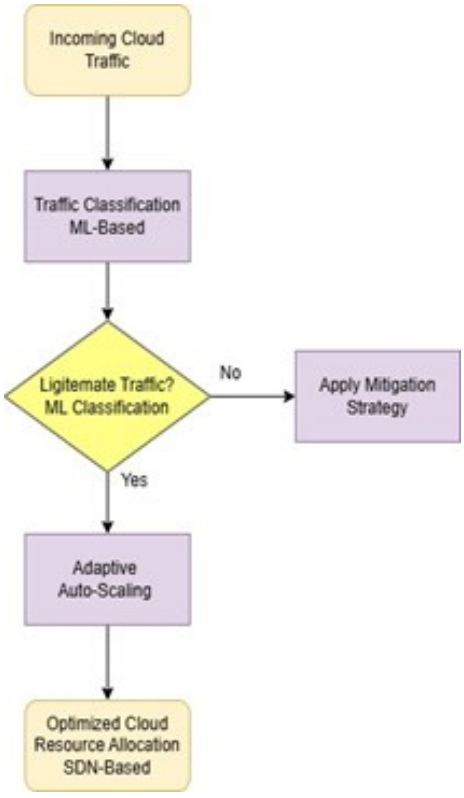


Figure 2. Flowchart of the Proposed CADS Defense System

To provide a clear and intuitive overview of the research workflow, Figure 3 presents the proposed research methodology in a step-by-step flowchart. The Figure 3 summarizes the complete methodological pipeline, starting from EDoS threat modeling and attack simulation, followed by dataset generation and feature extraction, ML model training, trust evaluation, and game-theoretic optimization. The methodology concludes with SDN-based enforcement and comprehensive performance evaluation. This flowchart visually clarifies the interaction between the proposed components and highlights how detection, economic decision-making, and mitigation are systematically integrated within the CADS defense system.

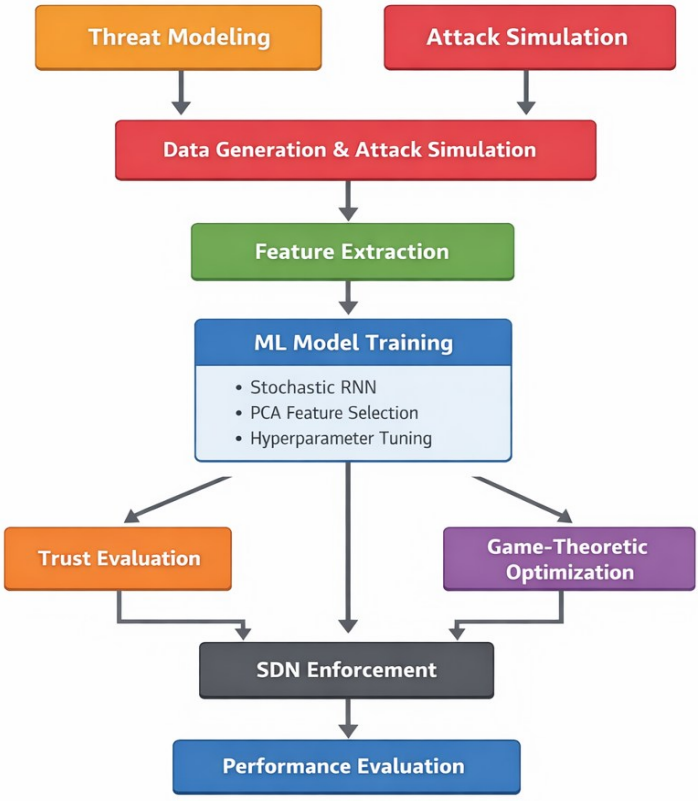


Figure 3. Research Methodology Flowchart

3.1. Threat Model and Attack Simulation

This section outlines how the EDoS attack is modeled, the strategies used to trigger costly resource consumption, and the controlled simulations employed to reproduce these behaviors in a cloud environment.

3.1.1. EDoS Threat Model

The considered threat model assumes adversaries aim to exploit cloud auto-scaling mechanisms by generating traffic patterns that remain protocol-compliant while inducing sustained resource scaling and increased billing costs. Unlike volumetric DDoS attacks, the objective is economic exhaustion rather than service unavailability. Attackers are assumed to have moderate capabilities, including the ability to distribute requests across multiple sources and adjust request rates dynamically to evade static thresholds. The cloud infrastructure follows a pay-per-use model with elastic scaling enabled.

3.1.2. Attack Strategies

The simulated attack strategies include:

- Low-rate HTTP flood attacks,
- Workload-aware request flooding targeting auto-scaling thresholds,
- Hybrid attack patterns that combine benign-looking traffic bursts with sustained background requests.

These strategies are designed to closely resemble legitimate traffic surges such as flash crowds, making detection challenging for conventional systems.

3.1.3. Attack Simulation

The attack simulation phase is used exclusively for modeling and dataset generation, not for performance evaluation. Synthetic EDoS traffic is generated using controlled traffic generation tools within the cloud environment, allowing precise control over request rates, burst intervals, and attack duration. This simulated traffic forms the labeled dataset used to train and validate the ML component. The same cloud environment is later reused in Section 4 for experimental evaluation, ensuring consistency between modeling and implementation while maintaining a clear separation between training data preparation and performance testing.

3.2. CADS Architecture

The CADS defense system consists of four tightly integrated modules:

1. Traffic Monitoring and Feature Extraction
2. ML-Based Detection
3. Trust-Based Resource Access Control
4. Nash Equilibrium-Based Resource Optimization with SDN Enforcement

Figure 4 explicitly illustrates this modular interaction and data flow.

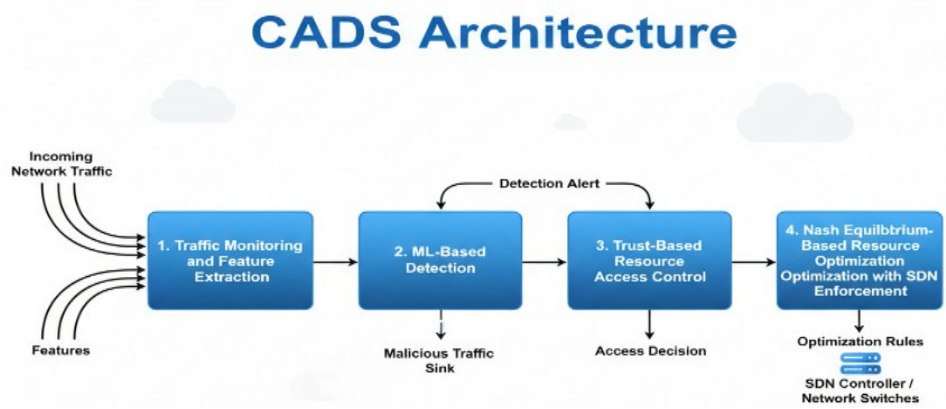


Figure 4. CADS Architecture

3.3. Machine Learning-Based Detection Module

A Stochastic Recurrent Neural Network (SRNN) is employed for traffic classification due to its ability to model temporal dependencies and stochastic variations in cloud traffic patterns. Unlike static classifiers (e.g., SVM or Random Forest), the SRNN captures sequential request behavior, which is critical for distinguishing sustained EDoS attacks from transient workload spikes.

Feature Selection, the model is trained using time-series traffic features, including:

- Request arrival rate,
- Session duration,
- Resource consumption per request,
- Scaling trigger frequency,
- Historical trust score trends.

Dimensionality reduction is applied using Principal Component Analysis (PCA) to eliminate redundancy and improve training efficiency. Hyperparameters Key SRNN hyperparameters include:

- Hidden layers: 2
- Neurons per layer: 64
- Learning rate: 0.001
- Optimizer: Adam
- Training epochs: 100

These values were empirically selected after series of experiments to balance detection accuracy and computational overhead.

3.4. Trust-Based Resource Access Control

CADS provides trust-based access control by basing access to the system on dynamic trust scores T_i on each traffic source i to measure the degree to which that source has acted reliably in the past. This score is

updated with a continuous and up-to-date behavioral evidence as opposed to fixed identities hence allowing CADS to reward consistently benign tenants and penalizing suspicious ones gradually. On an individual basis, CADS keeps the following trust factors on each source:

Trust factors include:

- Behavioral consistency B_i: The extent to which the pattern of requests remains constant through time (e.g. the variability in request rate, inter-arrival times and requested resources) relative to a historical baseline of of the entity and to the anticipated profile of the service. Fully bursty or discontinuously cost-amplifying patterns cause a decrease in B_i.
- Resource efficiency R_i: Measures the efficiency of the source using cloud resources, e.g. the ratio of successful usages to the cost incurred or the proportion of the requests served, which do not result in throttling, time out, or error responses. Such EDoS-like behavior which increases cost with minimal useful work results in reduced R_i.
- Classification Confidence C_i: The confidence that the recent traffic of source (i) is benign determined by the detection probabilities, or the ML detector using a confidence threshold calibration scheme (e.g., $C_i = 1 - P_i^{attack}$ or a confidence threshold calibration scheme). Streams marked many times as high probability of attack will receive a low C_i, although they may have been good before.

The trust score T_i for entity (i) is computed as:

$$T_i = \alpha B_i + \beta R_i + \gamma C_i \quad (1)$$

where B_i represents behavioral consistency, R_i denotes resource efficiency, C_i reflects classification confidence, and:

$$\alpha + \beta + \gamma = 1 \quad (2)$$

α controls the impact of long-term behavioral consistency on trust (e.g., higher in environments where stable usage patterns are critical). β emphasizes resource efficiency, which is particularly relevant for EDoS mitigation because it directly reflects cost-aware behavior. γ tunes the influence of the ML detector's classification confidence, allowing CADS to react quickly when the detector predicts attacks with high probability. Each factor is normalized to [0,1], where values closer to 1 indicate more trustworthy behavior on that dimension. Entities with low trust scores are prevented from triggering auto-scaling events, thereby reducing unnecessary resource allocation.

3.5. Nash Equilibrium–Based Resource Optimization

The Nash Equilibrium-based algorithm operates as a decision layer between ML detection and SDN enforcement. As a game theoritic concept the cloud provider and potential attackers are modeled as players with conflicting objectives: cost minimization versus resource exploitation.

The equilibrium solution determines the optimal mitigation strategy by balancing:

- Detection confidence from the SRNN,
- Trust scores from the access control module,
- Expected operational cost of scaling actions.

The algorithm ensures that mitigation decisions stabilize at a point where no player can reduce cost unilaterally, thereby preventing oscillatory scaling behavior.

3.6. Cost Modeling

To rigorously assess the economic impact of EDoS attacks and their mitigation, CADS adopts a holistic cloud cost model that accounts for both normal service operation and the additional defense overhead. The total operational cost "C_{total}" over a given evaluation window is defined as:

$$C_{total} = C_{compute} + C_{storage} + C_{network} + C_{defense} \quad (3)$$

- C_{compute} is the Cost of virtual machines, containers, or serverless invocations consumed while serving both benign and malicious traffic. This component reflects the core processing work driven up by EDoS attacks.

- C_{storage} is the Cost of persisting data such as logs, session state, and application data, including any additional storage incurred by attack traffic (e.g., inflated logging volume).
- C_{network} is the Cost of bandwidth and data transfer (ingress/egress and inter-zone traffic), which can grow significantly under volumetric or sustained low-rate EDoS patterns.
- C_{defense} is the Cost associated with running CADS itself, including ML inference, feature extraction, trust computation, and SDN control actions, as well as any extra logging or control-plane traffic they generate.

Modeling C_{defense} is necessary since lots of mitigation strategies seem desirable when reported is the avoidance attack cost, and maintaining the defense system operative active is not counted. CADS considers the net effect of C_{defense} incidence of C_{total} in calculating the net economic benefit by considering whether the decrease of $C_{compute} + C_{storage} + C_{network}$ used when assessing the cost of defense position, is additional to the defense cost overhead value.

3.7. System Implementation

The CADS defense system is implemented in an OpenStack-based cloud testbed that closely resembles a modern multi-tenant IaaS deployment, with software-defined networking enabled through an OpenFlow-compatible controller to support fine-grained traffic steering and mitigation actions. Within this environment, EDoS attack scenarios are driven by scripted workload generators that emulate realistic tenant behaviors and adversarial patterns, rather than relying solely on static or outdated benchmark datasets, which are known to misrepresent contemporary cloud workloads. This design choice allows the evaluation to capture current traffic dynamics, autoscaling reactions, and billing effects more faithfully, thereby providing more credible evidence for the practical effectiveness of CADS.

3.8. Methodological Assumptions and Limitations

The proposed methodology in this paper is based on a series of methodological assumptions in order to render the assessment of CADS manageable and reproducible in a controlled cloud testbed. The simulated environment is set up to mimic a representative traffic behavior and attacker strategies, but is not able to fully model the heterogeneity, burstiness and strategy-adaptation seen in large-scale clouds of production. In turn, the described findings can be interpreted in the context of the potential effectiveness of CADS under conditions that are well characterized, considering that practical deployments can bring a number of other sources of variability, such as dissimilar loads between tenants, unexpected attack patterns, and operational limitations, that can be explored systematically in future research.

4. RESULTS AND DISCUSSION

This section presents a comprehensive evaluation of the proposed Defense System (CADS) and compares its performance against two representative and recent EDoS mitigation approaches, namely EDoS-ADS and MAN-EDoS, which are widely cited in the EDoS defense literature. The comparison focuses on detection accuracy, false positive behavior, resource consumption, financial cost impact, and latency under realistic EDoS attack scenarios.

4.1. Detection Performance and Dataset Composition

The experimental evaluation was conducted using a test dataset composed of 55% legitimate cloud workload traffic and 45% EDoS attack traffic. The attack traffic includes both continuous low-rate flooding attacks and sophisticated pulsing EDoS attacks that intentionally mimic legitimate workload fluctuations to evade detection mechanisms. Table 2 summarizes the detection performance of CADS compared to EDoS-ADS and MAN-EDoS, with metrics including Precision, Recall, and F1-Score. As shown in Table 2, CADS achieves the highest metrics such as F1-Score, Recall and Precision. This improvement is critical in cloud environments, as incorrectly blocking legitimate traffic can directly translate into lost revenue and degraded service quality.

Table 2. Attack Detection Performance of CADS

Metric	CADS (Proposed)	EDoS-ADS [33]	MAN-EDoS [18]
Precision	96.8%	91.2%	88.9%
Recall	97.5%	89.4%	87.3%
F1-Score	97.1%	90.3%	88.1%

Higher F1, Recall, and Precision indicate that the defense system can identify a larger proportion of EDoS attacks while keeping both missed attacks and false alarms low, which is critical in highly imbalanced cloud traffic where malicious flows are rare compared to legitimate ones. This balance means the system is more reliable than state-of-the-art baselines for sustaining accurate EDoS detection over time, preventing unnecessary auto-scaling costs without disrupting normal user activity.

4.2. Resource Consumption Analysis

The impact of EDoS mitigation on cloud resource consumption is analyzed in terms of CPU utilization, memory usage, and network bandwidth. Figure 5 illustrates the comparative resource usage of CADS, EDoS-ADS, and MAN-EDoS under identical attack conditions. As shown in Figure 5, CADS consistently consumes fewer computing resources across all metrics. This improvement is directly attributable to two core mechanisms:

1) early-stage filtering of malicious traffic via the ML detection module, and
2) trust-based access control that prevents low-trust entities from triggering auto-scaling events.

By blocking economically harmful traffic before scaling decisions are executed, CADS avoids unnecessary allocation of virtual machines and bandwidth. In contrast, EDoS-ADS and MAN-EDoS rely on delayed mitigation, allowing short-lived but costly scaling actions to occur before traffic is filtered.

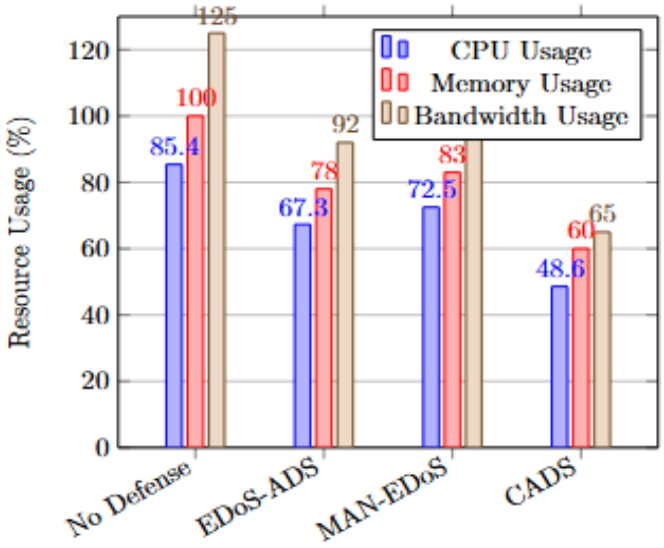


Figure 5. Cloud Resource Consumption Analysis

4.3. Financial Cost Analysis

To translate resource consumption into monetary cost, a pay-per-use cloud pricing model was assumed, consistent with common Infrastructure-as-a-Service (IaaS) billing practices. Costs were calculated based on:

- CPU usage per hour,
- Memory allocation duration,
- Network bandwidth consumption,
- Storage overhead.

The resulting resource consumption is presented in Table 3. CADS achieves a substantial reduction in total operational consumption compared to both EDoS-ADS and MAN-EDoS. This consumed resource reduction is primarily driven by the system's ability to prevent malicious traffic from activating scaling policies rather than merely reacting after resource allocation has already occurred.

Table 3. Cloud Resource Consumption Under EDoS Attacks

Defense Strategy	CPU Usage (%)	Memory Usage (MB)	Bandwidth (MB/s)
No Defense	85.4%	2,410 MB	125 MB/s
EDoS-ADS[33]	67.3%	1,890 MB	92 MB/s
MAN-EDoS[18]	72.5%	2,010 MB	105 MB/s
CADS (Proposed)	48.6%	1,430 MB	65 MB/s

4.4. Latency and System Overhead

System latency is a critical performance indicator for real-time cloud defense mechanisms. Live attack mitigation depends heavily on systems achieving quick response times. An evaluation of detection time and response time occurred through multiple defense strategies. Table 4 compares the end-to-end mitigation latency of the three systems.

Table 4. Latency and Response Time Analysis

Defense Strategy	Detection Time (ms)	Mitigation Response Time (ms)
EDoS-ADS[33]	120 ms	300 ms
MAN-EDoS[18]	135 ms	320 ms
CADS (Proposed)	85 ms	210 ms

The detection along with response time remains lowest in CADS.The system operates with a quick response time of 210 ms to enable real-time protection of legitimate cloud services. As shown in Table 4, CADS demonstrates lower response latency compared to EDoS-ADS and MAN-EDoS. This improvement is primarily due to:

- The programmability of SDN, which enables rapid flow rule enforcement.
- The lightweight inference process of the Stochastic RNN, which avoids computationally expensive feature recomputation.

While CADS introduces a modest computational overhead for ML inference and SDN controller decision-making, this overhead is significantly outweighed by the reduction in unnecessary scaling actions and prolonged attack-induced resource usage. The primary function of CADS is to cut down on cloud prices resulting from EDoS attacks. The analysis in this study determined monthly cloud service expenditures (expressed in USD) through different conditions by using 5 major EDoS attacks per month as the basis, (See Table 5).

Table 5. Monthly Financial Cost Analysis (Cloud Service Charges in USD)

Defense Strategy	Computing Cost	Storage Cost	Network Cost	Total Monthly Cost
No Defense	$4,520	$980	$1,340	$6,840
EDoS-ADS[33]	$3,120	$820	$1,010	$4,950
MAN-EDoS[18]	$3,430	$890	$1,110	$5,430
CADS (Proposed)	$2,210	$730	$780	$3,720

The lack of defense protection leads to EDoS attacks raising cloud expenses up to $6,840 per month from spending on unwanted resources. The Cloud Attack Defense System cuts cloud expenses by 45.6% better than having no protection and delivers up to 25% lower expenses than current existing EDoS defense solutions, (See Figure 6). Cost efficiencies mainly stem from proper computing resource optimization methods paired with automatic scaling features. The monthly costs for cloud services become evident from Figure 6 through different EDoS mitigation strategies. The operational costs of CADS show lower values than traditional defense systems which proves its financial sustainability for cloud service companies.

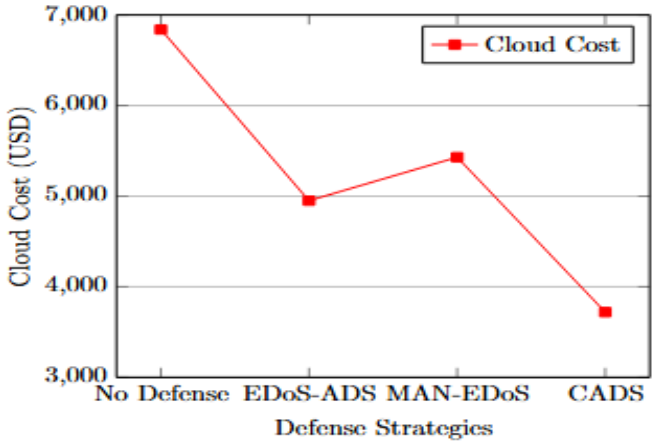


Figure 6. Cost Reduction Analysis

4.5. Discussion

The results demonstrate that CADS effectively mitigates EDoS attacks while maintaining high detection accuracy, low false positive rates, reduced resource consumption, and significant financial cost savings. Compared to EDoS-ADS and MAN-EDoS, CADS uniquely integrates economic awareness into mitigation decisions, rather than focusing solely on traffic classification. This explains its superior performance in reducing both operational cost and scaling-related inefficiencies. The findings confirm that addressing EDoS attacks as an economic optimization problem, rather than only a security challenge, yields more sustainable cloud defense outcomes. The ability of CADS to mitigate pulsing attacks further highlights its robustness against advanced adversarial strategies. The primary strength of CADS lies in its integrated design combining ML detection, trust-based control, and game-theoretic optimization. However, the evaluation is conducted in a simulated cloud environment, and real-world deployments may introduce additional variability. Future work will explore large-scale deployment and adaptive learning techniques to further enhance resilience.

4.6. Summary of Results

Collectively, the results confirm that CADS directly addresses the core challenge of economic sustainability in cloud environments, as identified in the introduction. By reducing false rates, preventing unnecessary scaling, and minimizing operational costs, CADS offers a cost-aware and scalable solution for defending modern cloud infrastructures against sophisticated EDoS attacks.

5. CONCLUSIONS

This research establishes the CADS as an advanced cost-aware defense system for mitigating EDoS attacks in cloud-based systems. By integrating DL-based traffic detection, Trust-based resource access control and SDN-enabled enforcement, the proposed defense system addresses EDoS attacks as both a security and an economic challenge rather than treating it solely as a traffic classification problem.

The experimental results demonstrate that CADS consistently outperforms existing EDoS mitigation approaches across all evaluated dimensions, including detection reliability, resource utilization efficiency, financial cost control, and response latency. More importantly, these improvements collectively confirm that embedding cost-awareness into mitigation decisions is critical for maintaining economic sustainability in elastic cloud environments. Unlike conventional defenses that react after resource scaling has already occurred, CADS proactively restricts financially damaging traffic before it can trigger unnecessary auto-scaling actions.

The findings further indicate that organizations cannot rely on detection accuracy alone when defending against EDoS attacks. Instead, a proactive balance between security posture and operational expenditure is required, one that CADS effectively achieves by aligning mitigation decisions with both trust evaluation and economic impact. This capability makes the defense system suitable for cloud service providers seeking to protect availability while controlling long-term operational costs. From a theoretical perspective, this work contributes new knowledge by formalizing EDoS mitigation as an economic optimization problem, supported by a game-theoretic resource allocation strategy. The integration of Trust-based access control with Nash equilibrium-driven decision-making provides a novel mechanism for stabilizing resource usage under adversarial conditions, extending beyond detection-centric defense models commonly reported in the literature.

Despite its advantages, this study has certain limitations. The evaluation was conducted in a simulated cloud environment, and while the SDN controller demonstrated stable performance under the tested attack volumes, extremely large-scale EDoS botnets may introduce additional control-plane overhead. Future work should therefore explore distributed or hierarchical SDN controller architectures to improve scalability and resilience under massive attack scenarios. Several promising directions for future research emerge from this work. Future studies should explore blockchain-based trust systems to support immutable logging and decentralized reputation management, enhancing transparency and trust score integrity. In addition, deep reinforcement learning can be investigated to enable adaptive policy optimization in response to evolving EDoS attack strategies and dynamic cloud pricing models. Real-world deployment and long-term evaluation in production cloud environments also remain important avenues for validating the defense system's practical impact.

In summary, this study advances the state of the art in cloud security by presenting a cost-aware, intelligent defense system specifically designed to protect against EDoS attacks. By bridging the gap between security enforcement and economic efficiency, CADS offers a scalable and sustainable solution that contributes meaningfully to both academic research and practical cloud defense strategies.

DECLARATION

Supplementary Materials

No supplementary materials are available for this study.

Author Contribution
All authors contributed equally to the main contributor to this paper. All authors read and approved the final paper.

Funding
This research received no external funding.

Conflicts of Interest
The authors declare no conflict of interest.

REFERENCES
[1] T. H. Aldhyani and H. Alkahtani, "Artificial intelligence algorithm-based economic denial of sustainability attack detection systems: Cloud computing environments," *Sensors,* vol. 22, no. 13, p. 4685, 2022, https://doi.org/10.3390/s22134685.
[2] F. Briatore and M. Braggio, "Edge, Fog and Cloud Computing framework for flexible production," *Procedia Computer Science,* vol. 253, pp. 2206-2218, 2025, https://doi.org/10.1016/j.procs.2025.01.281.
[3] P. T. Dinh and M. Park, "R-EDoS: Robust Economic Denial of Sustainability Detection in an SDN-Based Cloud Through Stochastic Recurrent Neural Network," *IEEE Access,* vol. 9, pp. 35057-35074, 2021, https://doi.org/10.1109/ACCESS.2021.3061601.
[4] Z. A. Baig, S. M. Sait, and F. Binbeshr, "Controlled access to cloud resources for mitigating Economic Denial of Sustainability (EDoS) attacks," *Computer Networks,* vol. 97, pp. 31-47, 2016, https://doi.org/10.1016/j.comnet.2016.01.002.
[5] H. Abbasi, N. Ezzati-Jivan, M. Bellaiche, C. Talhi, and M. R. Dagenais, "Machine learning-based EDoS attack detection technique using execution trace analysis," *Journal of Hardware and Systems Security,* vol. 3, no. 2, pp. 164-176, 2019, https://doi.org/10.1007/s41635-018-0061-2.
[6] P. T. Dinh and M. Park, "Dynamic Economic-Denial-of-Sustainability (EDoS) Detection in SDN-based Cloud," in *2020 Fifth International Conference on Fog and Mobile Edge Computing (FMEC)*, pp. 62-69, 2020, https://doi.org/10.1109/FMEC49853.2020.9144972.
[7] A. Agarwal, A. Prasad, R. Rustogi, and S. Mishra, "Detection and mitigation of fraudulent resource consumption attacks in cloud using deep learning approach," *Journal of Information Security and Applications,* vol. 56, p. 102672, 2021, https://doi.org/10.1016/j.jisa.2020.102672.
[8] C.-N. Nhu and M. Park, "Two-Phase Deep Learning-Based EDoS Detection System," *Applied Sciences,* vol. 11, no. 21, p. 10249, 2021, https://doi.org/10.3390/app112110249.
[9] S. Ribin Jones and N. Kumar, "EDoS-BARRICADE: A Cloud-Centric Approach to Detect, Segregate and Mitigate EDoS Attacks," in *International Conference on Communication, Computing and Electronics Systems*, pp. 579-592, 2021, https://doi.org/10.1007/978-981-33-4909-4_44.
[10] K. Lalropuia, "Availability and reliability analysis of cloud computing under economic denial of sustainability (EDoS) attack: a semi-Markov approach," *Cluster Computing,* vol. 24, no. 3, pp. 2177-2191, 2021, https://doi.org/10.1007/s10586-021-03257-9.
[11] X. Xu, J. Li, H. Yu, L. Luo, X. Wei, and G. Sun, "Towards Yo-Yo attack mitigation in cloud auto-scaling mechanism," *Digital communications and networks,* vol. 6, no. 3, pp. 369-376, 2020, https://doi.org/10.1016/j.dcan.2019.07.002.
[12] H. I. H. Alsaadi, M. K. Al-Anni, and F. E. K. Al-Khuzaie, "Deep learning to mitigate economic denial of sustainability (EDoS) attacks: cloud computing," in *2023 3rd International Conference on Emerging Smart Technologies and Applications (eSmarTA)*, pp. 1-7, 2023, https://doi.org/10.1109/eSmarTA59349.2023.10293405.
[13] J. Idziorek, M. Tannian, and D. Jacobson, "Attribution of fraudulent resource consumption in the cloud," in *2012 IEEE fifth international conference on cloud computing*, pp. 99-106, 2012, https://doi.org/10.1109/CLOUD.2012.23.
[14] H. Wang, Z. Xi, F. Li, and S. Chen, "WebTrap: A dynamic defense scheme against economic denial of sustainability attacks," in *2017 IEEE Conference on Communications and Network Security (CNS)*, pp. 1-9, 2017, https://doi.org/10.1109/CNS.2017.8228640.
[15] A. Koduru, T. Neelakantam, and S. M. S. B, "Detection of Economic Denial of Sustainability Using Time Spent on a Web Page in Cloud," in *2013 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM)*, pp. 1-4, 2013, https://doi.org/10.1109/CCEM.2013.6684433.
[16] G. Capasso and A. Esposito, "Detection of DoS Attacks in Cloud Computing: A Machine Learning Approach," in *International Conference on Broadband and Wireless Computing, Communication and Applications*, pp. 275-284, 2024, https://doi.org/10.1007/978-3-031-76452-3_26.
[17] J. Britto Dennis and M. Shanmuga Priya, "Deep belief network and support vector machine fusion for distributed denial of service and economical denial of service attack detection in cloud," *Concurrency and Computation: Practice and Experience,* vol. 34, no. 1, p. e6543, 2022, https://doi.org/10.1002/cpe.6543.

[18] V. Ta and M. Park, "MAN-EDoS: A Multihead Attention Network for the Detection of Economic Denial of Sustainability Attacks," *Electronics,* vol. 10, no. 20, p. 2500, 2021, https://doi.org/10.3390/electronics10202500.
[19] F. Z. Chowdhury, L. B. M. Kiah, M. A. M. Ahsan, and M. Y. I. B. Idris, "Economic denial of sustainability (EDoS) mitigation approaches in cloud: Analysis and open challenges," in *2017 International Conference on Electrical Engineering and Computer Science (ICECOS)*, pp. 206-211, 2017, https://doi.org/10.1109/ICECOS.2017.8167135.
[20] K. Lalropuia and V. Khaitan, "Availability and reliability analysis of cloud computing under economic denial of sustainability (EDoS) attack: a semi-Markov approach," *Cluster Computing,* vol. 24, pp. 2177-2191, 2021, https://doi.org/10.1007/s10586-021-03257-9.
[21] F. Z. Chowdhury, M. Y. I. Idris, L. M. Kiah, and M. A. M. Ahsan, "EDoS eye: A game theoretic approach to mitigate economic denial of sustainability attack in cloud computing," in *2017 IEEE 8th Control and System Graduate Research Colloquium (ICSGRC)*, pp. 164-169, 2017, https://doi.org/10.1109/ICSGRC.2017.8070588.
[22] A. Karthika and N. Muthukumaran, "An ADS-PAYG approach using trust factor Against economic denial of sustainability attacks in cloud storage," *Wireless Personal Communications,* vol. 122, no. 1, pp. 69-85, 2022, https://doi.org/10.1007/s11277-021-08889-z.
[23] P. T. Dinh and M. Park, "Economic Denial of Sustainability (EDoS) Detection using GANs in SDN-based Cloud," in *2020 IEEE Eighth International Conference on Communications and Electronics (ICCE)*, pp. 135-140, 2021, https://doi.org/10.1109/ICCE48956.2021.9352082.
[24] P. Singh, S. Manickam and S. U. Rehman, "A survey of mitigation techniques against Economic Denial of Sustainability (EDoS) attack on cloud computing architecture," *Proceedings of 3rd International Conference on Reliability, Infocom Technologies and Optimization*, pp. 1-4, 2014, https://doi.org/10.1109/ICRITO.2014.7014767.
[25] Y. Alghofaili, A. Albattah, N. Alrajeh, M. A. Rassam, and B. A. S. Al-Rimy, "Secure cloud infrastructure: A survey on issues, current solutions, and open challenges," *Applied Sciences,* vol. 11, no. 19, p. 9005, 2021, https://doi.org/10.3390/app11199005.
[26] M. A. Sotelo Monge, J. Maestre Vidal, and L. J. García Villalba, "Entropy-based economic denial of sustainability detection," *Entropy,* vol. 19, no. 12, p. 649, 2017, https://doi.org/10.3390/e19120649.
[27] P. Singh, S. U. Rehman, and S. Manickam, "Comparative analysis of state-of-the-art EDoS mitigation techniques in cloud computing environment," *arXiv preprint arXiv:1905.13447,* 2019, https://doi.org/10.48550/arXiv.1905.13447.
[28] B. B. Rao, S. Bulla, K. G. Rao, and K. Chandan, "HRF (HTTP request filtering): a new detection mechanism of EDOS attack on cloud," in *2019 International Carnahan Conference on Security Technology (ICCST)*, pp. 1-7, 2019, https://doi.org/10.1109/CCST.2019.8888431.
[29] S. Q. A. Shah, F. Z. Khan, and M. Ahmad, "The impact and mitigation of ICMP based economic denial of sustainability attack in cloud computing environment using software defined network," *Computer Networks,* vol. 187, p. 107825, 2021, https://doi.org/10.1016/j.comnet.2021.107825.
[30] M. S. Hossain and M. S. Islam, "Economic Denial of Sustainability Attack Detection Using Machine Learning," in *2023 26th International Conference on Computer and Information Technology (ICCIT)*, pp. 1-6, 2023, https://doi.org/10.1109/ICCIT60459.2023.10441045.
[31] K. Lalropuia and V. Khaitan, "Game theoretic modeling of economic denial of sustainability (EDoS) attack in cloud computing," *Probability in the Engineering and Informational Sciences,* vol. 36, no. 4, pp. 1241-1265, 2022, https://doi.org/10.1017/S0269964821000334.
[32] P. S. Bawa, S. U. Rehman, and S. Manickam, "Enhanced mechanism to detect and mitigate economic denial of sustainability (EDoS) attack in cloud computing environments," *Int. J. Adv. Comput. Sci. Appl,* vol. 8, no. 9, pp. 51-58, 2017, https://doi.org/10.14569/IJACSA.2017.080907.
[33] A. Shawahna, M. Abu-Amara, A. S. H. Mahmoud, and Y. Osais, "EDoS-ADS: An Enhanced Mitigation Technique Against Economic Denial of Sustainability (EDoS) Attacks," *IEEE Transactions on Cloud Computing,* vol. 8, no. 3, pp. 790-804, 2020, https://doi.org/10.1109/TCC.2018.2805907.
[34] M. H. Khalil, M. Azab, A. Elsayed, W. Sheta, M. Gabr, and A. S. Elmaghraby, "Maintaining cloud performance under DDOS attacks," *IJCNC,* vol. 11, no. 6, pp. 1-22, 2019, https://doi.org/10.5121/ijcnc.2019.11601.
[35] R. K. Deka, D. K. Bhattacharyya, and J. K. Kalita, "Ddos attacks: Tools, mitigation approaches, and probable impact on private cloud environment," *Big Data Analytics for Internet of Things,* pp. 285-319, 2021, https://doi.org/10.1002/9781119740780.ch13.
[36] R. Priyadarshini and R. K. Barik, "A deep learning based intelligent framework to mitigate DDoS attack in fog environment," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 3, pp. 825-831, 2022, https://doi.org/10.1016/j.jksuci.2019.04.010.
[37] J. M. Vidal, M. A. S. Monge, and L. J. G. Villalba, "Detecting Workload-based and Instantiation-based Economic Denial of Sustainability on 5G environments," in *Proceedings of the 13th International Conference on Availability, Reliability and Security*, pp. 1-8, 2018, https://doi.org/10.1145/3230833.3233247.
[38] S. Nautiyal and S. Wadhwa, "A Comparative Approach to Mitigate Economic Denial of Sustainability (EDoS) in a Cloud Environment," in *2019 4th International Conference on Information Systems and Computer Networks (ISCON)*, pp. 615-619, 2019, https://doi.org/10.1109/ISCON47742.2019.9036257.
[39] S. Nautiyal, C. R. Krishna, and S. Wadhwa, "Mitigating Economic Denial of Sustainability (EDoS) in Cloud Environment using Genetic Algorithm and Artificial Neural Network," *International Journal of Innovative Technology and Exploring Engineering (IJITEE),* vol. 8, no. 10, pp. 3415-3421, 2019, https://doi.org/10.35940/ijitee.J9680.0881019.

[40] N. Beigi-Mohammadi, M. Shtern and M. Litoiu, "Adaptive Load Management of Web Applications on Software Defined Infrastructure," in *IEEE Transactions on Network and Service Management*, vol. 17, no. 1, pp. 488-502, 2020, https://doi.org/10.1109/TNSM.2019.2948969.

AUTHORS BIOGRAPHY

Zubaidi Maytham Sahar Saeed, Faculty of Computing, University of Technology Malaysia, Johor Baharu, Malaysia
Email: Sahar20@graduate.utm.my

Anazida Binti Zainal, Faculty of Computing, University of Technology Malaysia, Johor Baharu, Malaysia
Email: anazida@utm.my

Fuad A. Ghaleb,College of Computing, Faculty of Computing, Engineering and the Built Environment, Birmingham City University, Birmingham, B4 7XG, UK
Email: Fuad.Ghaleb@bcu.ac.uk