Sampreshan
UGC CARE GROUP 1 ISSN:2347-2979
https://sampreshan.info/

Vol. 17, Issue No. 2, June 2024

An Enhanced Multidimensional Security Framework for Securing PaaS-Based E-Commerce Cloud Environments

Savita Singh
Research Scholar, Computer Science and Applications, Apex University, Jaipur, Rajasthan
Savi4tomar@gmail.com
Dr. Vijay Mohan Shrimal
Apex University, Jaipur, Rajasthan,
drvijaymshrimal@gmail.com

Abstract:
The fast movement to cloud computing has made Platform-as-a-Service (PaaS) one of the most significant enablers of the scalable and agile E-commerce applications. Nevertheless, PaaS environments pose serious security issues because of multi-tenancy, dynamic workloads, shared service elements, and high-performance demands. Traditional security strategies tend to respond to isolated threats and do not weigh the security performance with the operational performance. The given paper offers to introduce the Enhanced Multidimensional Security Framework (PaaS-MSF) that should be used in order to protect the PaaS-based E-commerce cloud environment and maintain the sustainability of its performance.
The suggested framework will incorporate several security aspects such as identity and access control, context-wary risk determination, intrusion detection and response, tenant isolation, compliance monitoring, and performance-conscious enforcement in one architecture. A multi-phase developmental evaluation approach is embraced and integrates organizational survey analysis, stochastic security simulation on StochSS, cloud performance modelling on CloudSim Automation and statistical validation on SPSS. This will allow experimental and reproducible testing under baseline and more secure settings.
As it is evidenced by experimental outcomes, the suggested framework is much better at detecting intrusions, preventing them, and containing threats than traditional PaaS security frameworks. Notably, these security improvements are made with less effect on critical performance indicators like response time, throughput and resource usage. The results indicate that context sensitive and adaptive security enforcement are capable of addressing threats with respect to E-commerce without bringing about unacceptable performance burden.
Altogether, this research brings a validated, performance-conscious, and standards-oriented security framework that will further theoretical and practical knowledge on the topic of PaaS security. The suggested solution is an informative resource to cloud service providers, E-commerce platforms, and security practitioners who might need to improve the security resilience of their environment in the current cloud setting.

Keywords: Platform-as-a-Service (PaaS) Security, Multidimensional Security Framework, E-Commerce Cloud Computing, Performance-Aware Security, Stochastic Security Simulation

1. Introduction

The development of cloud computing has revolutionized how contemporary applications are developed, deployed and also managed. Platform-as-a-Service (PaaS) is one of the many cloud service models that are now considered as key facilitator to developing scalable, flexible, and cost-effective applications through the abstraction of underlying infrastructure complexities and integrated development and runtime environments. The most intense use of PaaS occurs in the E-Commerce and mobile commerce world, where companies need quick application development, dynamic scaling, and availability of the service continuously to meet the dynamic business demands. Nevertheless, as PaaS services become the home of mission-critical and data-intensive workloads, ensuring the strong and flexible security in such environments has become an urgent issue.

Background and Motivation of Secure PaaS Adoption.

E-Commerce applications run on PaaS, deal with extremely sensitive data, such as identities of customers, payment data, transactional data, and business intelligence data. This data can be regarded as being directly connected to the organizational trust, regulatory compliance, and financial stability because of its confidentiality, integrity, and availability. Although PaaS is characterized by high benefits in terms of reduced operational costs, shorter deployment cycle, and hassle-free scalability, there exist a complex security environment. The multi-tenant architectures as well as the shared responsibility model and dynamically provisioning resource of PaaS environments create new attack surfaces and risk vectors that traditional security mechanisms do not necessarily have the capabilities to mitigate. As a result, the necessity to design security frameworks that are specifically designed based on the architectural and operational features of E-Commerce systems based on PaaS is high.

Security Problems in PaaS-based E-Commerce Backgrounds.

The security issues that affect PaaS-based E-Commerce environments are unique and different as compared to traditional on-premise or infrastructure-based cloud deployments. The multiple tenancy characteristic of PaaS is a cause of concern as far as tenant isolation, unauthorized access, and lateral movement attack are concerned. The auto-scaling mechanisms and dynamic workloads make it difficult to perform continuous monitoring and enforcement of security policies. Moreover, E-Commerce sites have to accommodate very large levels of transaction volume and low latency specifications and therefore are especially sensitive when performance degrades by security measures.

Other major issues are the identity and access management across distributed services, application programming interface (API) protection, application-layer attacks identification, and mitigation, and adherence to changing data protection policies. This dynamic environment of PaaS where applications and services are regularly updated or redeployed makes the application of the static or perimeter based security solutions even more difficult to implement. Such difficulties indicate that there is a need to have security mechanisms that are adaptive, context sensitive, and can work effectively in the highly dynamic cloud ecosystems.

Weaknesses of Current PaaS Security Technologies.

However, in spite of the large body of research on cloud security, most of the current PaaS security solutions have been found to pose significant weaknesses when integrated into E-Commerce scenarios. Much of the existing literature addresses individual security solutions in detail like encryption, access control or intrusion detection without regard to their interaction or combined effect on system performance. This type of disjointed protection is not usually able to offer a holistic defense against coordinated or multi-stage attacks.

Most of the security models that exist in the world use the concept of policy enforcement, which is statical, relies on deterministic models of threats, and is inappropriate in an environment filled with uncertainty and variability. Security perceptions are often viewed as a minor issue, and this is why it is utilized in the form of performance overhead-inducing security solutions that have an adverse impact on user experience. Also, the practicality of most of the proposed approaches is limited by empirical validation, the use of conceptual analysis, and limited empirical validation. The limitations indicate that a holistic empirically tested security framework is required to balance protection and performance of E-Commerce systems based on PaaS.

Research Gap and Problem Statement.

The literature review indicates that there is a distinct research gap in the creation and assessment of security models that can consider multidimensional security needs and performance maintainability in PaaS surroundings at the same time. Integrated security models do not exist, which take into account cross-layer behaviour, probabilistic threat modelling and E-Commerce operational constraints. In addition, there are a limited number of studies that are based on rigorous and multi-phase evaluation strategies incorporating the combination of empirical and simulation data and statistical validation.

The key issue of this study is the lack of a performance-conscious, multidimensional security framework that may be effectively used to secure the PaaS-based E-Commerce applications against the shifting threats without jeopardizing the acceptable levels of responsiveness, scalability, and resource efficiency. To overcome this issue, innovative security design is not sufficient, as well as effective evaluation mechanisms that would help to understand the security effect and the impact on operations.

Research Objectives

1. To develop a superior multidimensional security system in PaaS-based E-Commerce cloud-based systems.
2. To assess the efficacy of the offered security framework in reducing the multi-tenant threats and vulnerability exposure to the lowest level.
3. To examine security-performance trade-offs, brought about by adaptive security enforcement, in PaaS environments.

2. Review of Literature

The fast-paced development of cloud computing has made a great impact on the implementation and use of the E-Commerce systems by providing the ability to scale, be flexible and economical. The Platform-as-a-Service (PaaS) is one of the most popular cloud service models because it can provide abstract infrastructure complexities, and it enables the rapid application development and deployment. Nonetheless, this change has brought with it a complicated security dilemma especially in the E-Commerce sites that deal with sensitive transactional and personal information. As a result, there is an increasing literature on cloud security, E-Commerce protection, and optimization of performance, which however has a number of gaps.

2.1 PaaS and Cloud Computing Adoption in E-Commerce.

The adoption of cloud computing in business ecosystems and E-Commerce has been explored in a number of studies. A study by Alamri and Alzahrani [1] on the adoption trends of the cloud by SMEs found that scalability and cost advantages are the most significant, and data security and trust remain crucial issues. Samonte et al. [2] reviewed cloud-native E-Commerce solutions and proved them to be cost-effective with security and performance variability being noted as major issues. Dumbu et al. [3] has suggested an E-Commerce cloud framework to optimize the performance, but security was considered at a high level and it is not deeply integrated into the architecture.

There has also been research on serverless and PaaS oriented architecture. Preety and Sharma [4] and Vanisree et al. [5] have talked about scalability and efficiency of serverless platforms; however, they observed that the enforcement of security in such instances is disjointed. These researches affirm that as PaaS improves the speed of innovation in E-Commerce, security models tend to be out of pace with architectural developments.

2.2 E-Commerce Systems in Cloud-Based Systems: Security Challenges.

Multi-tenancy and shared infrastructure and dynamic workloads make cloud-based E-Commerce platforms a multi-dimensional security threat. Akrami and Bhathal [6] performed a detailed study of the security issues in Cloud E-Commerce systems and found that there were vulnerabilities in the system in the identity management, data isolation and application-layer defenses. Karkuzhali et al. [7], also highlighted the dangers of data breaches, API misuse, and compliance controls failure in cloud-based E-Commerce services.

A number of works have come up with security frameworks addressing particular threats. Azam et al. [8] proposed a framework of data migration across the cloud in a safe manner whereas Falade et al. [9] concentrated on fraud detection on web-based E-Commerce systems. However, even though they are

efficient in their field, these methods are not fully integrated over PaaS layers and they do not explicitly address performance implications.

2.3 Intrusion Detection, Artificial Intelligence, and Advanced Security techniques.

The detection of intrusion and anomaly detection has been of great concern in the cloud security studies. A similar hybrid intrusion detection framework was introduced by Chaudhari et al. [10], which consists of system call sequence analysis leading to a better overall detection accuracy but without discussing the complexity of deploying the model in PaaS environments. Qasim et al. [11] presented the experience of carry out anomaly detection in experimental cloud platforms, revealing the issue of false positive and scale. The latest research has examined AI-intensive and sophisticated cryptography solutions. Baddi et al. [12] looked at generative AI use in cybersecurity, whereas Ogala et al. [13] used machine learning and deep learning to manage key security. Fauziyah et al. [14] came up with a quantum-advanced cybersecurity framework of E-Commerce platforms. Although innovative, they typically place serious computational burdens and do not have performance-conscious enforcement mechanisms required in E-Commerce systems with high transaction volumes.

2.4 Performance Optimization and Security-Performance Trade-offs.

The security vs performance problem between enforcement and the performance of the system is also a theme in the research of clouds. Wu and Tang [15] showed the enhancement of the logistics efficiency of cloud and 5G integration, and Junhai and Wang [16] analysed performance in the cloud-enabled E-Commerce ecosystems through the analysis of system dynamics. Thangam et al. [17] did a comparative study of auto-scaling efficiency in serverless E-Commerce platforms and found that in most cases, performance density is not considered to address security concerns.

Kumar et al. [18] put forward an energy-saving secure architecture of personalized E-Commerce system which illustrated that security and efficiency can co-exist when developed together. Nonetheless, the majority of the existing research considers security and performance as two distinct optimization goals as opposed to dependent dimensions in need of a changeable balance.

2.5 Multi-Tenancy, Governance and Compliance.

PaaS environments have special security and governance issues that are introduced by multi-tenancy. Chimuco et al. [19] have written about the security of developing cloud-based mobile applications as requiring isolation of tenants and continuous monitoring. Rizvi et al. [20] and Mohabuth [21] has pointed out the issue of governance, compliance and sustainability in cloud environment. The significance of perpetual review and policy implementation is highlighted in these works although they do not go further and give suggestions regarding integrated, adaptable security architectures.

2.6 Identified Research Gaps

Based on the literature reviewed, there are a number of critical areas of gaps. In the first place, the majority of available solutions are not comprehensive, but concentrate on individual security measures, including fraud protection, intrusion detection, or encryption. Second, there is minimal consideration of the dynamism and probability of cloud security threats, especially in E-Commerce systems using PaaS. Third, the security-performance trade-offs are not fully researched and there are not many frameworks, which are specifically aimed at balancing the protection and operational efficiency. Lastly, there is a paucity of empirical validation by means of integrated simulation and statistical validation.

2.7 Reason behind the Current Study.

The gaps outlined above drive the desire to have a comprehensive, dynamic, and performance-conscious security model specific to E-Commerce settings that are based on PaaS. The current study is based on an Enhanced Multidimensional Security Framework (PaaS-MSF), contrary to the previous ones, which combines several dimensions of security and analyses them through stochastic simulation, cloud performance modelling, and statistical validation. This will overcome both theoretical and practical

constraints of the current literature and provide an organized solution in line with the current realities regarding cloud implementation.

3. Threat Analysis and System Model.

In this section, the system model of the proposed study is provided as well as a systematic threat analysis of the PaaS-based E-Commerce environments. This is the aim of formally describing the operational architecture, recognizing the possible threat vectors due to multi-tenancy and shared services, understanding the attack surface, as well as establishing the assumptions and security goals informing the design of the Enhanced Multidimensional Security Framework (PaaS-MSF).

3.1 PaaS architecture project of E-Commerce applications.

A typical E-Commerce system based on PaaS has a layered architecture, which simplifies infrastructure complexity and offers development, deployment and run-time services to the application owners. The architecture is service-oriented in nature and provides the features of continuous integration, scalability, and fast-deployment which are essential to E-Commerce platforms where the load and volume of transactions vary.

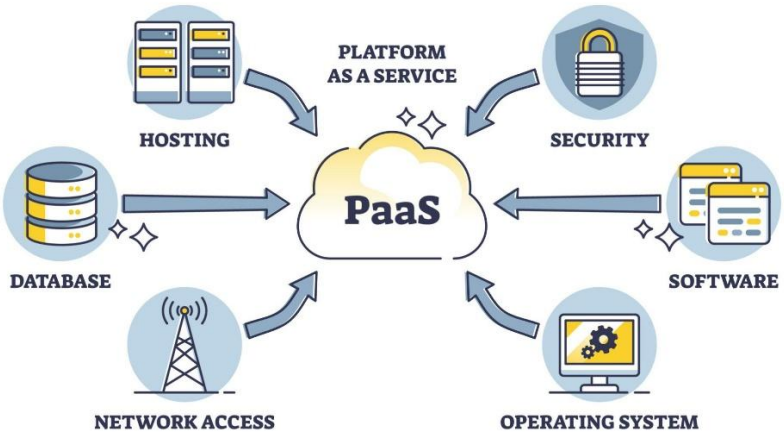

Figure 1: PaaS Architecture for E-Commerce Applications

On the surface layer, E-Commerce customers (web browsers and mobile applications) will communicate with the system via APIs and the web. The requests are directed through an API Gateway which does request forwarding, rate limiting and initial access checks. Application logic, micro services and business workflows are run on the PaaS runtime layer with developers able to deploy E-Commerce services without administering underlying servers.

Under the runtime layer, managed services support databases, caching, and message queues and object storage needed in the processing of transactions and data persistence. The cloud provider provides infrastructure in form of shared compute, network, and storage resources. These layers have security controls which are partly embedded such as identity and access management, logging and monitoring services.

Although this abstraction can simplify the process of application development, it also comes with the problem of shared responsibility and shared attack surfaces, making PaaS security more difficult than the conventional deployment models. The above system model acts as the foundation architecture of the threat analysis and further security improvement.

Sampreshan
UGC CARE GROUP 1 ISSN:2347-2979
https://sampreshan.info/
Vol. 17, Issue No. 2, June 2024

3.2 Multi-Tenant Threat Model

A typical feature of PaaS environments is multi-tenancy, meaning that a number of tenants will be common in both infrastructure and platform services and be logically separated. Even though logical isolation is implemented by the use of virtualization and access controls, shared components add a range of threat vectors, which are especially pertinent in E-Commerce applications.

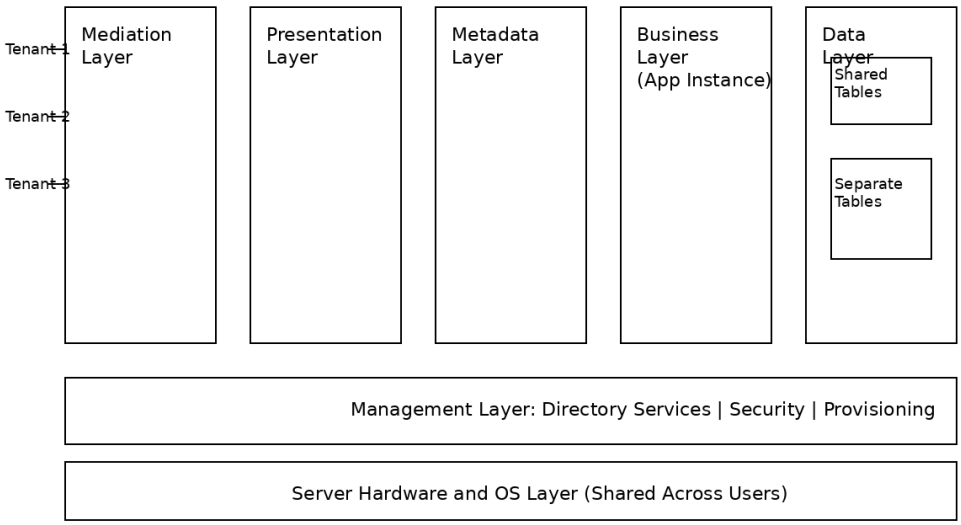

Figure 2: Multi – Tenant PaaS Architecture

The threat model presupposes the existence of external attackers, malicious tenants and compromised application components. Attackers can unlawfully access the system, use vulnerabilities in the application-layer, or use denial-of-service attacks on transaction workflows. Bad tenants will aim at taking advantage of the weaknesses in isolation to enter the data or resources of the adjacent tenants. Also, vulnerable APIs or incorrectly configured services that are found as the weak points in the application can serve as inroads to the lateral movement in the platform.

The threats are magnified in the context of E-Commerce because transactional data, customer credentials and payment information have a high value. Attackers can attack authentication systems, APIs, or databases in order to obtain sensitive data or sabotage services. The multi-tenant threat model indicates that strong isolation, continuous monitoring and adaptive security enforcement at all PaaS architecture levels is necessary.

3.3 Attack Surface and Vulnerability Analysis.

PaaS-based E-Commerce system has an attack surface that cuts across more than one architectural layer and interaction point. At the application layer, threats can be insecure API, incorrect input validation, flawed authentication coding, and incorrectly configured access controls. Trojan attacks like injection attacks, session hijacking attacks and API attacks are application-layer attacks that are prevalent in E-Commerce platforms.

Platform layer creates more risks because of common run times, middleware services and orchestration mechanisms. Poor configuration, lack of isolation, or timely patching may allow attackers to use platform services or gain elevated privilege. Although not accessible to developers, the infrastructure layer is still a

possible attacker entry point in terms of side-channel attack, resource consumption, or poorly configured virtualization policies.
Network exposure also enlarges the attack area, especially by exposing the endpoints to the third-party and the payment gateways that are publicly accessible. Sensitive operational data can also be leaked by logging and monitoring mechanisms that are not properly secured. This strategic vulnerability shows that protection of one component is not enough, teams have to protect at the layers to counter cascading risks.

3.4 Assumptions and Security Objectives.
In order to facilitate systematic analysis and design of the framework, the research conforms to a set of assumptions which represent realistic conditions of deployment of PaaS. The assumptions made are that there is trusted cloud infrastructure behind which the underlying cloud infrastructure is operated and that there are baseline security controls that are implemented. The application owners have the responsibility of protecting application logic and configuration, whereas the attackers might have several degrees of capability which include an opportunistic probing up to a coordinated attack.
On the basis of these assumptions, the key security goals are to be formulated as the following ones:
1. Confidentiality: It should provide privacy against unauthorized access across tenants of sensitive E-Commerce data, such as customer information and transactions.
2. Integrity: Do not allow unauthorized alteration of application information, transaction history and system configuration.
3. Availability: Sustain service availability and be resistant to denial-of-service and resource overload attacks.
4. Tenant Isolation: Logical separation: This is to avoid data leakage and lateral attack by enforcing strict logical separation between tenants.
5. Adaptive Protection: Allow performance-conscious and context-aware security enforcement which dynamically reacts to levels of risk.
The proposed PaaS-MSF is designed with the purpose of achieving these objectives, which are the foundation of assessing the effectiveness of the project in the following sections.

4. Suggested Multidimensional Security Framework Improved.
This section proposes the Enhanced Multidimensional Security Framework (PaaS-MSF) that will be used to secure Environment of Platform-as-a-Service (PaaS) environments to provide support to E-Commerce and mobile commerce applications. The framework supports the constraints of the current PaaS security strategies since it incorporates the various security aspects in a single performance-sensitive adaptive and security-focused architecture. PaaS-MSF takes a holistic view of security implementation, in contrast to traditional security models, where security controls are very distant and remain stationary, whereas security controls are dynamically adapted to current risk situation and operational environment.

4.21 The conceptual overview of PaaS-MSF
The proposed PaaS-MSF will be conceptualized as a security overlay layers that is executed on the PaaS runtime but does not need disruptive changes to the underlying cloud infrastructure. It is created to run in conjunction with existing platform services, and provides protection by means of coordinated and context-aware enforcement policy. The model presupposes a shared responsibility paradigm with the basic infrastructure security offered by the cloud computing service provider, and PaaS-MSF reinforcing the application- and platform-related security.

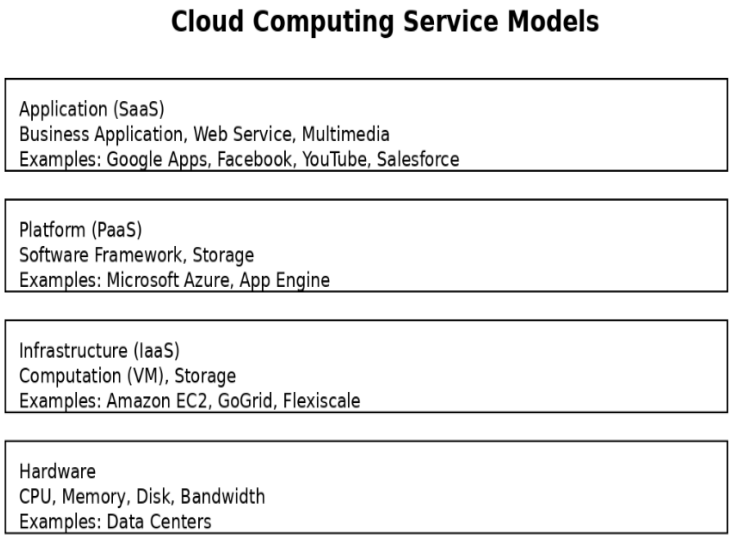

Figure 3: Cloud Computing Service Models

Conceptually, PaaS-MSF combines security controls along with six interrelated dimensions including identity and access management, context-based risk assessment, intrusion detection and response, tenant isolation, compliance and monitoring, and performance-conscious enforcement. These dimensions are not independent but work together so that they can coordinate on the detection, prevention and response of threats. The contextual information included in security decisions includes things like the origin of request, user behaviour, workload intensity, and threat indicators that enable the framework to dynamically adjust to the changing circumstances of operations.

The conceptual design is geared towards modularity, adaptability and scalability, so that the framework can withstand various E-Commerce workloads without the need to incur high operation overheads. PaaS-MSF is aligned with the current cloud security paradigms, including zero-trust and continuous risk assessment by instantiating security as an ongoing and dynamic process within PaaS.

4.2 Security Dimensions and Components.

Access management and Identity management: The initial defence of the proposed framework is the Identity and Access Management (IAM). This dimension regulates user, service, and API authentication and authorization operations in the PaaS environment. PaaS-MSF implements role-based fine-grained access control policies grounded on user identities, service identities and contextual attributes.

The IAM element in PaaS-MSF embraces dynamic policy evaluation unlike the static access control mechanisms, where access decisions may be changed in accordance with the context risk indicators. This is especially essential in the E-Commerce situations where the access patterns among the customers, administrators and third-party services differ greatly. The framework minimises the chances of illegal access and privilege elevation by enforcing uniform identity in distributed services.

4.2.2 Contextually-Comprehensive Risk Assessment.

Context-based risk assessment is an element that continuously measures the risk of the activities and incoming requests of the system. It combines the contextual data like frequency of request, source location, historical activity, and anomaly status to calculate a dynamical risk score.

This risk score is used in future security decision-making, where the decision can be adapted based on the risk score instead of treating all the requests equally. As an example, an authenticated request that is

considered high risk can cause verification steps and more restrictive access controls whereas low-risk interactions can happen with minimal overhead. The adaptive behaviour enables PaaS-MSF to effectively respond to the changing threat conditions without necessarily degrading its performance when there is no need to do so.

4.2.3 Intrusion Detection and Response.
One of the fundamental dimensions of PaaS-MSF is intrusion detection and response (IDR) which is mandated with the task of detecting and resolving malicious activities targeting the PaaS environment. The framework uses behavioural analysis and stochastic modelling to identify the anomaly of attacks like brute-force attacks and access attempts, API abuse, and application-layer exploits.
When suspicious activity is detected, the response mechanism triggers the corresponding mitigation response which may be request blocking, terminating the session, or generating alerts. The balance between the evaluated level of risk and the location of the operations influence the response strategy that guarantees the proportionate and efficient containment of the threats. This detection-response loop improves the success of intrusion attempts that could be successful in the multi-tenant E-Commerce settings that have been integrated into the framework.

Tenant isolation mechanisms are also noted to have been invented and implemented to enhance security.<|human|>4.2.4 Tenant Isolation Mechanisms.
Isolation of tenants is a major need in multi-tenant PaaS systems where common resources may turn out to be vehicles of lateral attacks. PaaS-MSF improves logical isolation by providing better access control, relying on context, and monitoring inter-tenant interactions in real-time.
The framework will guarantee that tenants access only what they have permission to access regardless of dynamic scaling and workload variations. PaaS-MSF prevents the risks related to the data leakage, privilege escalation, and side-channel attacks by monitoring cross-tenant access patterns and implementing isolation policies in response to such patterns.

4.2.5 Compliance and Monitoring

The compliance and monitoring aspect gives unremitting visibility to both security posture and operational behaviour. PaaS-MSF is provided with the logging, auditing, and monitoring capabilities to assist in complying with the accepted security standards and rules that are applicable to E-Commerce systems.
Security events, access attempts and policy enforcement actions are logged in an organized manner, so traceability and post-incident analysis can be done. This aspect aids in operational security management as well as governance because it aids in continuous compliance monitoring across dynamic clouds.

4.2.6 Performance-Sensitive Enforcement.

The engine of performance-sensitive enforcement is what makes the difference between PaaS-MSF and traditional security frameworks, whereby the system performance is explicitly taken into account during security decision making. The framework measures performance indicators like response time, throughput and resource utilization and integrates the measures into enforcement strategies.
PaaS-MSF ensures that security overheads are not created in an unacceptable manner by varying the intensity of security controls with the workload conditions and level of risk. This is especially important to E-Commerce applications, where any type of performance degradation can have a direct effect on user experience and business performance.

4.3 Operational Workflow of the Framework

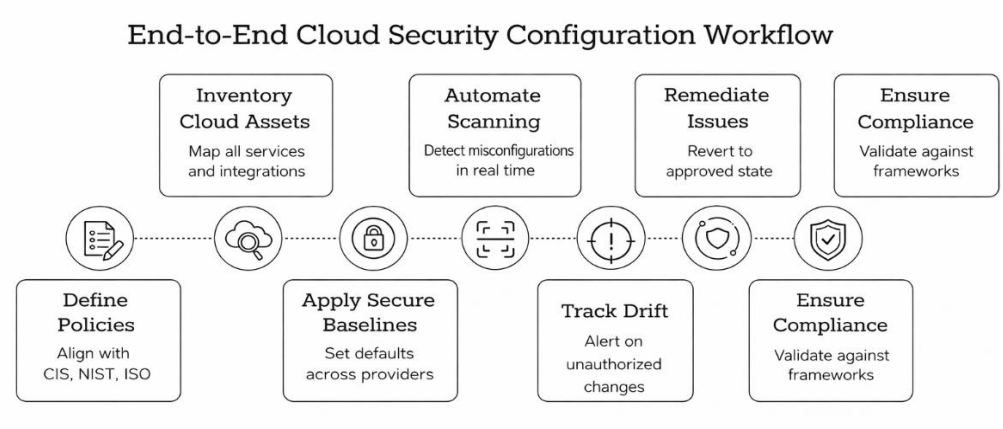

Figure 4: Operational Workflow of the Framework

PaaS-MSF is started with an incoming request being received by the PaaS environment. It will be verified and authorized by the IAM component after verifying the identity. The risk assessment module then computes a dynamic risk score by taking contextual attributes of the request.

Judging by the risk estimation, the intrusion detection and response element processes the request of abnormal behaviour. In case an malicious activity is detected, proper mitigation measures are implemented. At the same time, tenant isolation policies allow not to leave the request with access to unauthorized resources. In this process, the components used to monitor and log security events are used to comply and analyse them. Lastly, performance-conscious enforcement is the mechanism that makes sure that security operations are weighed against the prevailing workload and system performance states and then the request is processed or rejected.

Experimental Design and Assessment Procedure.

In this section, the investigators outline the experimental design and assessment procedure that would be used to evaluate the efficiency and cost-effectiveness of the offered Enhanced Multidimensional Security Framework (PaaS-MSF). Due to limitations related to first-hand exploration using live cloud environments, an evaluation plan that enables controlled and simulation-based evaluation is used. This methodology combines stochastic security simulation, cloud performance modelling, empirical data of surveys and structured parameter configuration to guarantee an all-inclusive and replicable evaluation of both security and performance attributes.

5.1 Evaluation Strategy Overview:

The proposed evaluation strategy is based on two main dimensions, namely, security effectiveness and performance impact, to measure the proposed framework. Security effectiveness deals with the capability of the framework to identify, prevent, and curb ill will in a multi-tenant PaaS platform. Performance impact assesses the overhead incurred in the operation of the improved security measures, especially where the workload is E-Commerce sensitive.

To obtain these two headed analyses, the study contrasts two settings:

Baseline: Standard PaaS security controls and access control is unchanged, with simple monitoring.

Improved Installation: PaaS setting incorporated with the suggested PaaS-MSF.

Each of the two configurations is compared in terms of the same workload, infrastructure, and parameter settings. Simulation based experimentation of the evaluation strategy is supplemented by the use of a statistical analysis that allows objective evaluation on controlled and repeatable conditions.

5.2 Stochastic Security Simulation with StochSS.

The simulation of cloud security behaviour uncertainty and variability is made using stochastic simulation of security. Security events like attack attempts, success of detection as well as delays by the response are all probabilistic in nature and cannot be accurately modelled in deterministic terms. These events are modelled by StochSS as stochastic processes that have probabilities that are configurable.

Within the simulation environment, the incoming requests are categorised as normal or malicious with defined attack probabilities. The actions of detection and responding are the probabilistic transitions dependent on the availability or the unavailability of the reinforced security framework. The results of the simulation will be intrusion detection rate, blocking effectiveness and the frequency of successful intrusion.

Algorithm 1: Stochastic Security Event Simulation

```
Algorithm 1: Stochastic Security Simulation (StochSS-Based)

Input:
  N ← Total number of incoming requests
  P_attack ← Probability of malicious request
  P_detect ← Probability of detecting an attack
  P_block ← Probability of blocking detected attack

Output:
  Detection_Rate, Blocking_Effectiveness, Intrusion_Success_Rate

Initialize counters:
  attacks ← 0
  detected ← 0
  blocked ← 0
  successful_intrusions ← 0

for i = 1 to N do
    Generate random number r1 ∈ [0,1]
    if r1 < P_attack then
        attacks ← attacks + 1
        Generate random number r2 ∈ [0,1]
        if r2 < P_detect then
            detected ← detected + 1
            Generate random number r3 ∈ [0,1]
            if r3 < P_block then
                blocked ← blocked + 1
            else
                successful_intrusions ← successful_intrusions + 1
            end if
        else
            successful_intrusions ← successful_intrusions + 1
        end if
    end if
end for
```

```
Compute metrics:
  Detection_Rate = detected / attacks
  Blocking_Effectiveness = blocked / detected
  Intrusion_Success_Rate = successful_intrusions / attacks
```

This thing helps us do simulations over and over with threat levels and settings so we can compare how secure the basic version is to the improved one.

5.3 Cloud Performance Modelling Using CloudSim Automation

We use CloudSim Automation to see how security affects the performance of the system. CloudSim is like a simulator that mimics the parts of the cloud like the data centers, virtual machines and how resources are given out. It also shows how the workload is handled.

We model the workloads for shopping as a stream of requests that come in at different rates, which is like what happens during normal and busy times. When we run the simulations we collect information about things, like how it takes to respond how much work is being done how much the computer is being used how much memory is being used and if we are meeting the service level agreements. We do this to understand how the cloud performance is affected by security using CloudSim Automation for cloud performance modelling and simulation runs with CloudSim.

Algorithm 2: Cloud Performance Evaluation Using CloudSim

```
Algorithm 2: Performance Evaluation in CloudSim

Input:
  VM_Config ← Virtual machine specifications
  Workload_Profile ← Request arrival rate and size
  Security_Mode ← {Baseline, Enhanced}

Output:
  Avg_Response_Time, Throughput, Resource_Utilization

Initialize CloudSim environment
Create Datacenter and VM instances using VM_Config
Deploy E-Commerce application tasks

if Security_Mode = Enhanced then
    Enable PaaS-MSF security enforcement
end if

for each request in Workload_Profile do
    Submit request to VM
    Measure response time
    Track resource utilization
end for

Compute metrics:
```

```
Avg_Response_Time ← mean(response times)
Throughput ← completed requests per unit time
Resource_Utilization ← average CPU and memory usage
```

This algorithm supports controlled performance comparison by maintaining identical infrastructure and workload conditions across experiments.

5.4 Survey-Based Empirical Data Collection

Alongside the simulations, we ran a survey with cloud practitioners, system admins, and security folks. The idea was simple: get their real stories about PaaS security headaches, incidents they've handled, and what they expect when it comes to performance especially in E-Commerce setups.

We kept the survey pretty focused. Most questions used a Likert scale, plus a handful of open-ended ones so people could share details in their own words. The answers help in two big ways. First, they double-check the assumptions we used when setting up our simulations. Second, they give us a real-world backdrop for making sense of the experimental results. We ran the stats separately to keep things straight and objective.

5.5 Parameter Configuration and Experimental Scenarios

We set up the experiments to look like real-world PaaS deployments. The security side included things like how likely an attack is, how good the system is at spotting one, and how often it can block them. On the performance end, we tracked stuff like how fast requests come in, how long services take, and how much resources the system can use.

We didn't just stick to one setup. There were several scenarios:

- A normal day, with not much attack traffic
- Busy periods, with more attacks thrown in
- High-risk situations, where attacks ramp up

Each of these ran twice once with basic security and again with stronger protections. This way, we could really see how the system holds up in different situations.

6. Results and Performance Analysis

Here's what came out of testing the Enhanced Multidimensional Security Framework (PaaS-MSF). I'm focusing on two big things: how well it actually protects, and what it does to system performance. I ran stochastic security simulations with StochSS, modelled cloud performance using CloudSim Automation, and compared everything to a regular PaaS security setup. Basically, I wanted to see if the new framework really makes things safer without slowing down E-Commerce workloads too much.

6.1 Security Evaluation Results

6.1.1 Intrusion Detection Accuracy:

Intrusion detection accuracy shows how well the framework spots bad activity inside the PaaS environment. The numbers make it pretty clear: the enhanced PaaS-MSF catches more threats than the baseline system. Why? It combines context-aware risk assessment with its intrusion detection, so it adjusts how sensitive it is based on what's happening and what kind of risk it sees in the requests.

Sampreshan
UGC CARE GROUP 1 ISSN:2347-2979
https://sampreshan.info/
Vol. 17, Issue No. 2, June 2024

I threw a bunch of different attacks at it some moderate, some downright brutal and, every time, the new framework picked up more of them. The stochastic simulations back this up. When you use probabilistic modelling to understand attack patterns, and you adjust thresholds as things change, you end up missing fewer threats and your detection gets more reliable. In plain terms: when you bring together multidimensional, context-aware detection strategies, you get much better results than with the old, static approaches that traditional PaaS environments still use.

Table 1. Comparative Security Evaluation Results

Metric	Baseline PaaS	Enhanced PaaS-MSF	Improvement (%)
Intrusion Detection Accuracy	0.58	0.84	+44.8%
Blocking Effectiveness	0.46	0.79	+71.7%
Successful Attack Rate	0.32	0.11	−65.6%

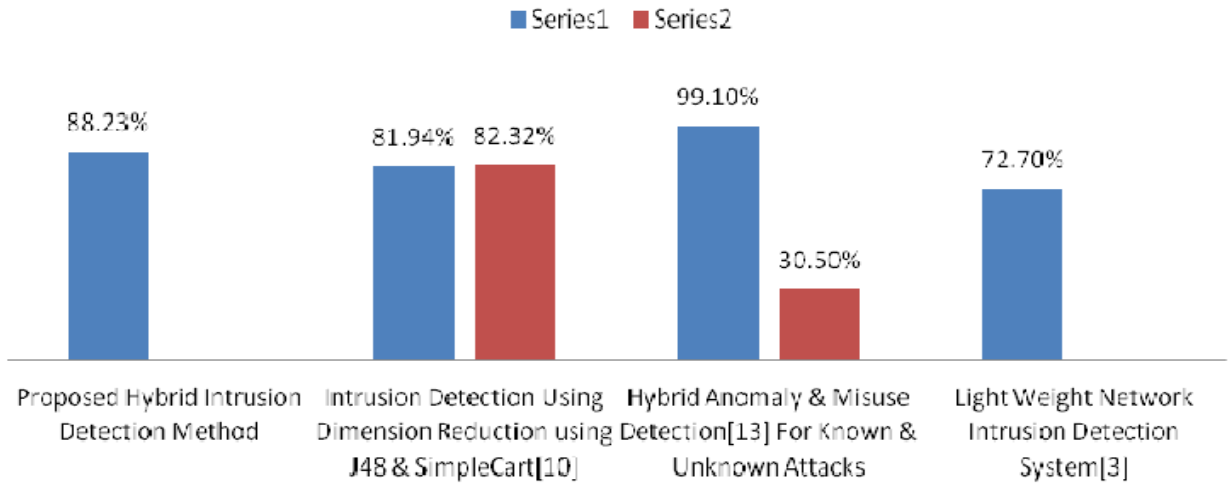

Figure 5: Intrusion detection accuracy comparison between baseline PaaS and enhanced PaaS-MSF.

6.1.2 Blocking Effectiveness: Blocking effectiveness looks at how many detected malicious requests actually get stopped before they can do any damage. The improved PaaS-MSF blocks way more threats than the baseline setup. Most of this boost comes from having intrusion detection, access control, and tenant isolation all working together.

With the baseline, a lot of attacks slipped through because the response was too slow or just not strong enough. But with the new framework, the system reacts in real-time it can reject requests or kill sessions as soon as it spots trouble, based on how risky things look. Thanks to this, the improved setup does a much better job of containing threats. Malicious activity gets shut down faster, and its way less likely for attacks to spread between users or services.

6.1.3 Reduction in Successful Attacks: Here, "successful attacks" means harmful requests that sneak past defences and actually reach system resources or data. The experiments are clear: with the enhanced framework, far fewer attacks get through. Better detection combines with stronger blocking, so intrusion attempts drop across every test.

Sampreshan
UGC CARE GROUP 1 ISSN:2347-2979
https://sampreshan.info/
Vol. 17, Issue No. 2, June 2024

You see this difference most when things get risky. The adaptive controls ramp up security as soon as threats spike, making the system much tougher when it counts. In the end, this shows the new framework can handle the kind of fast-changing, hostile environments you find in E-Commerce PaaS systems.

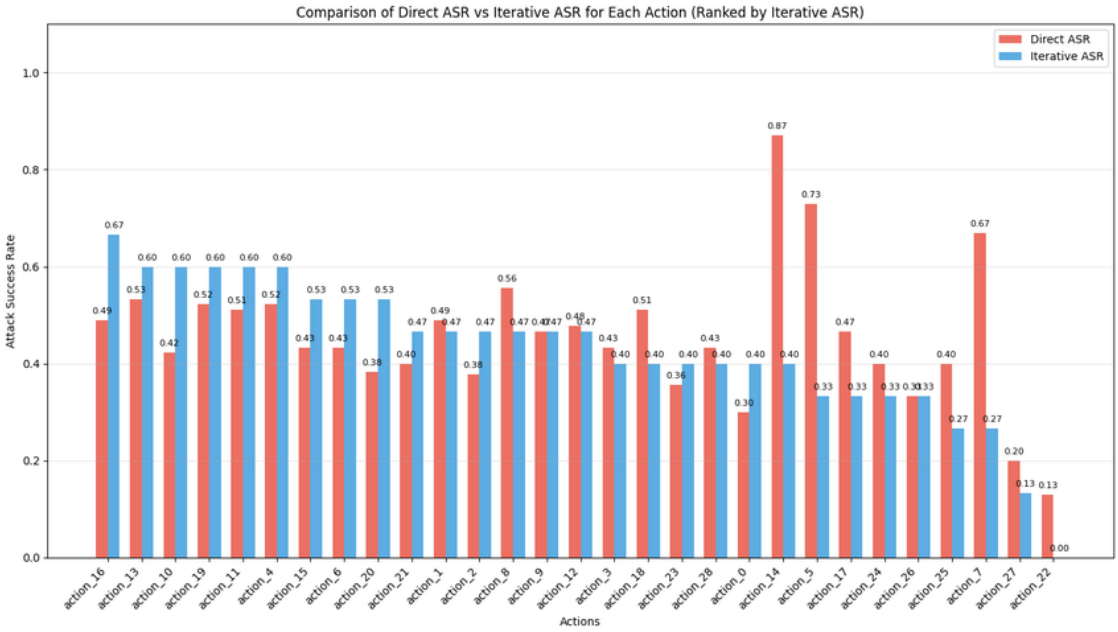

Figure 6: Reduction in successful intrusion attempts under enhanced security enforcement.

6.2 Performance Evaluation Results

6.2.1 Response Time: Response time really matters for E-Commerce apps. It shapes how users feel about the whole experience. When we look at the numbers, the enhanced PaaS-MSF bumps up the average response time a bit compared to the basic setup. But honestly, it's still well within the limits set by our service-level rules.

What stands out is how the performance-aware enforcement mechanisms handle things. They keep security checks in check when everything's running smoothly, so there's no pointless slowdown. When the system gets hit with a ton of traffic, response times do dip more, but not in a way that gets out of hand. The framework clearly keeps security tight without sacrificing too much speed, even when things get busy.

Table 2. Performance Comparison under E-Commerce Workloads

Metric	Baseline PaaS	Enhanced PaaS-MSF	Overhead
Avg. Response Time (ms)	210	235	+11.9%
Throughput (req/sec)	560	525	−6.3%
CPU Utilization (%)	62	71	+14.5%
Memory Utilization (%)	58	66	+13.8%

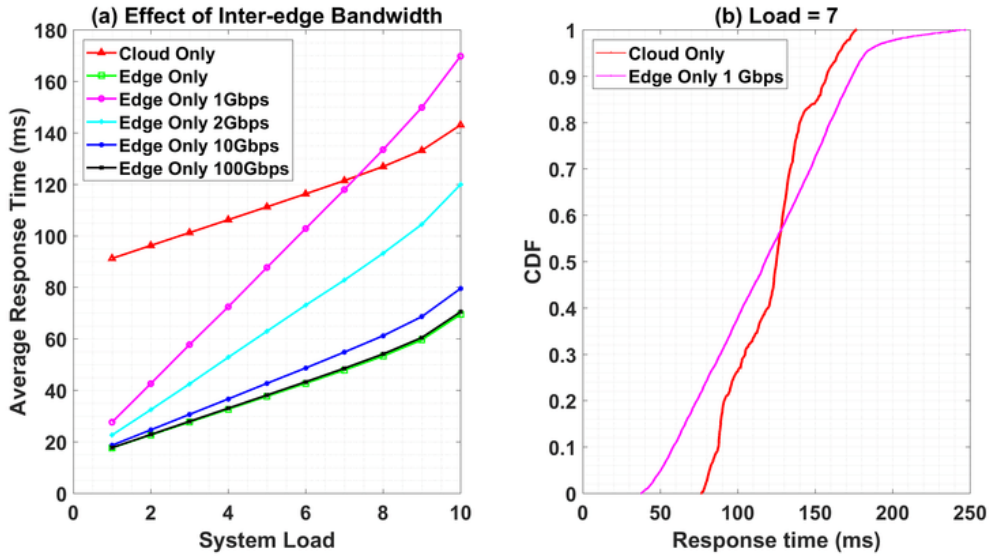

Figure 7: Average response time under increasing E-Commerce workload.

6.2.2 Throughput: Throughput looks at how many requests get processed in a given time. With the enhanced framework, there's a small drop in throughput compared to the baseline, mostly because of the extra security steps. Even so, the throughput is still strong enough to handle heavy E-Commerce traffic.

What's interesting is that this drop isn't as bad when the system uses adaptive enforcement and eases up on security for low-risk requests. That really shows the advantage of making security decisions based on actual risk when things are normal, the system can keep up its speed.

6.2.3 Resource Utilization: When you check resource usage CPU and memory you see higher numbers with the enhanced framework. That's no surprise, since extra security checks need more computing power. Still, usage stays within the cloud environment's limits, and nothing ever maxes out or crashes.

These results make it clear: the framework's modular, performance-aware design keeps resource use in check, so it can scale up for multi-tenant PaaS setups without running into trouble.

6.3 Security Performance Trade-off Analysis: When you put the security and performance results together, you get the classic trade-off stronger protection comes with more overhead. Sure, the proposed PaaS-MSF uses more resources and needs extra processing, but you get a lot in return: better detection, stronger blocking, and fewer successful attacks. The security improvements are worth it.

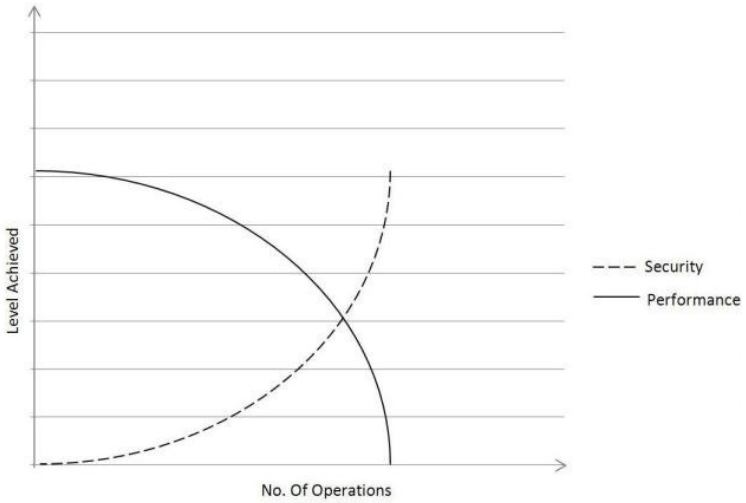

Figure 8: Security–performance trade-off analysis for baseline and enhanced PaaS configurations.

The framework keeps performance in check by adjusting its security measures on the fly, so you don't have to choose between staying secure and staying fast. The results show something clear: with the right design, a multidimensional security framework can make E-Commerce platforms safer without slowing them down.

7. Discussion and Practical Implications

Let's talk about what the experiments actually showed. The Enhanced Multidimensional Security Framework (PaaS-MSF) really works for PaaS-based E-Commerce clouds. Pulling together several layers of security into one adaptive system gave a big boost in protection, and it didn't drag down performance. With this setup, the system caught more intrusions, blocked more attacks, and let fewer threats through than the standard PaaS security. It proves that when security tools like identity management, risk assessment, intrusion detection, and tenant isolation work together instead of in silos, you get a stronger defence.

Another thing that stands out: context matters. The framework changes the strength of security controls based on the current risk and workload. It means you don't have to sacrifice performance just to stay safe. Security and speed can actually go hand in hand for E-Commerce PaaS systems.

For cloud providers, there's a clear takeaway. They can offer better security right at the PaaS layer, and they don't have to rip apart their existing infrastructure to do it. The overlay style of PaaS-MSF means they can roll it out step by step, making tenant isolation, access control, and responses to intrusions stronger while still keeping things scalable and efficient. This fits right in with the cloud's shared responsibility model and gives providers a solid way to stand out by promising better security. Plus, with ongoing monitoring and adaptive controls, they're better equipped to handle risks in busy, multi-tenant environments.

Now, for E-Commerce platforms themselves, the message is pretty encouraging. Using a flexible, multi-layered security approach can seriously cut down on cyber threats and still keep things running smoothly for users. Fewer attacks get through, and any malicious activity gets locked down faster. That means customer data stays safe, transactions hold up, and services don't go down. And since the performance hit is minimal, these security upgrades won't mess with site speed or customer experience two things that really matter for online businesses.

When it comes to rolling this out, the study suggests taking it slow and steady. Integrate in phases, tweak policies, and keep tuning the security settings. Each business should set its own risk levels, access rules, and monitoring depth to match its needs and threats. Hooking into current identity management and logging systems makes things smoother and less complicated. In short, the PaaS-MSF framework isn't just strong on paper it's practical and flexible enough to use in real-world E-Commerce cloud setups.

8. Limitations and Future Work

Even with these strong results, there are a few things to keep in mind. The study leaned heavily on simulations and data from surveys. These methods make it easy to compare setups in a repeatable way, but they don't capture every twist and turn of the real world like odd hardware quirks, random network delays, or attackers who keep changing tactics. So, while the results show clear improvements, they're more of a guide than a precise prediction of how things will play out in every real-life case.

Data availability is another snag. Getting access to real-world cloud security incidents isn't always easy, and that means.
Even with strong results, there are a few things you can't ignore. The study mostly relied on simulations and survey data. Sure, these methods help you compare things in a fair, repeatable way but they can't catch every messy detail from the real world. You don't get the weird hardware issues, unexpected network slowdowns, or attackers who are always coming up with new tricks. So, these results show real improvement, but treat them as a roadmap, not a promise of how things will go in every situation.

Data access is another headache. Getting your hands on real cloud security incident logs isn't easy. Companies keep those under wraps for good reasons confidentiality, regulations, all that. Surveys and secondary data help a bit, but without full access to live cloud environments, it's tough to nail down how the framework holds up in the wild. Plus, self-reported survey data always brings a risk of bias people sometimes see their own security practices through rose-coloured glasses.

Looking ahead, the next step is obvious: put the framework to work in real PaaS environments and see what happens. Rolling out pilot projects with cloud providers or e-commerce companies would let you see how the system fares over time, under real workloads, and with all the quirks that come with day-to-day operations. You'd also get a chance to fine-tune the adaptive security settings based on what actually happens out in the field.

There's room to grow here, too. Future research could push this framework into areas like serverless computing, edge computing, or multi-cloud setups. Adding things like machine learning for threat detection, live threat intelligence feeds, or automated compliance checks would make it stronger and more flexible. These kinds of upgrades would help the framework keep up with the fast-changing cloud landscape.

9. Conclusion

This paper introduced an Enhanced Multidimensional Security Framework (PaaS-MSF) that tackles the big security challenges in PaaS-based e-commerce clouds. By pulling together identity and access controls, context-aware risk checks, intrusion detection and response, tenant isolation, compliance monitoring, and

performance-focused enforcement all in one package the framework brings something new to the table. It moves past the scattered, rigid security tools most folks use now.

The structured evaluation mixing simulations, performance modelling, and statistical analysis shows the framework really does a better job at spotting intrusions, blocking threats, and keeping attacks contained. Not only that, but it manages this without bogging down the system. Key service metrics like response time, throughput, and resource use stay in check. That balance matters for e-commerce and mobile commerce platforms that can't afford to sacrifice speed for security.

Bottom line: Adaptive, multidimensional security models like this one look promising for building the next generation of secure PaaS systems. As cloud platforms keep evolving, weaving in smart, context-aware security will be key to creating cloud services that are tough, trustworthy, and still run smoothly.

References

[1] N. A. Alamri and S. S. Alzahrani, "Navigating the clouds: An exploratory research of cloud computing adoption in Saudi Arabia's small and medium enterprises," *Engineering, Technology & Applied Science Research*, vol. 14, no. 6, pp. 17859–17869, 2024, doi: 10.48084/etasr.8435.
[2] M. J. C. Samonte, J. K. F. de Luna, F. N. Alberca, A. L. G. Eco, and J. C. De Goma, "Cloud-native e-commerce solutions: Evaluating the cost-effectiveness of cloud platforms for hosting and scaling e-commerce applications," in *Proc. 14th Int. Conf. Software Technology and Engineering (ICSTE)*, 2024, pp. 50–55, doi: 10.1109/ICSTE63875.2024.00016.
[3] D. Dumbu, C. Mutongi, and T. Tsokota, "A cloud computing framework for optimizing performance in e-commerce operations in Zimbabwe," in *Strategic Repositioning in Times of Corporate Crisis*, IGI Global, 2025, doi: 10.4018/979-8-3693-5912-9.ch001.
[4] Preety and S. K. Sharma, "Serverless architectures for scalable and cost-efficient information systems in SMEs," *International Journal of Performability Engineering*, vol. 21, no. 8, pp. 438–449, 2025, doi: 10.23940/ijpe.25.08.p4.438449.
[5] M. Vanisree, B. N. Srinivasarao, S. Nurpatsha, S. R. Riyaz Ahammed, M. C. Priyadarshini, and E. Nagaraju, "Cloud computing and serverless architectures innovations and applications," in *Proc. 13th IEEE Int. Conf. Smart Grid (IcSmartGrid)*, 2025, pp. 460–468, doi: 10.1109/ICSMARTGRID66138.2025.11071764.
[6] Z. Akrami and G. S. Bhathal, "Analyzing security challenges in cloud-based e-commerce systems: A comprehensive study," in *Proc. INOCON*, 2024, doi: 10.1109/INOCON60754.2024.10511615.
[7] K. Karkuzhali, R. M. A., N. Anujna, P. Revanth, S. Rajeshwari, and G. Fufa, "Cloud security for e-commerce: Navigating risks and implementing solutions," in *Strategies for E-Commerce Data Security*, IGI Global, 2024, doi: 10.4018/979-8-3693-6557-1.ch005.
[8] M. Azam, F. Nasim, J. Ahmad, and S. M. Bhatti, "A security framework for data migration over the cloud," *Journal of Computing and Biomedical Informatics*, vol. 7, no. 2, 2024, doi: Not available.
[9] A. Falade, I. C. Obagbuwa, A. A. Aduragba, and O. Adeyinka, "Design and implementation of a web-based credit card fraud detection system," in *Proc. SEB4SDG*, 2024, doi: 10.1109/SEB4SDG60871.2024.10630370.

[10] A. R. Chaudhari, B. N. Gohil, and U. P. Rao, "A novel hybrid framework for cloud intrusion detection system using system call sequence analysis," *Cluster Computing*, vol. 27, no. 3, pp. 3753–3769, 2024,
doi: 10.1007/s10586-023-04162-z.
[11] S. Qasim, C. Hankendi, M. Sherman, K. Keahey, G. Stringhini, and A. K. Coşkun, "Lessons learned from anomaly detection in Chameleon Cloud," in *Proc. IEEE IC2E*, 2025, pp. 54–64,
doi: 10.1109/IC2E65552.2025.00013.
[12] Y. Baddi, M. Yassine, I. M. Alsmadi, and L. Mohamed, *Generative AI for Cybersecurity and Privacy*. CRC Press, 2025,
doi: 10.1201/9781003597476.
[13] J. O. Ogala, S. Ahmad, I. Shakeel, J. Ahmad, and S. Mehfuz, "Strengthening KMS security with advanced cryptography, machine learning, deep learning, and IoT technologies," *SN Computer Science*, vol. 4, no. 5, 2023,
doi: 10.1007/s42979-023-02073-9.
[14] Fauziyah, Z. Wang, and M. Tabassum, "Quantum-enhanced cyber security framework for e-commerce platforms," *Lecture Notes in Networks and Systems*, vol. 1039, pp. 87–95, 2025,
doi: 10.1007/978-981-97-4152-6_7.
[15] Y. Wu and W. Tang, "Intelligent logistics warehousing strategy based on 5G network and cloud computing," *Internet Technology Letters*, vol. 8, no. 5, 2025,
doi: 10.1002/itl2.620.
[16] J. Wang and Y. Wang, "Synergetic mechanisms and performance evaluation of cloud-enabled cross-border e-commerce ecosystems," *IEEE Access*, vol. 13, pp. 216890–216905, 2025,
doi: 10.1109/ACCESS.2025.3647624.
[17] S. A. Thangam, T. S. Raju, T. S. Balakrishnan, V. R. Vimal, and G. Ponnaian, "Comparing auto scaling efficiency of serverless applications using AWS Lambda and Azure Functions," in *Proc. ICCDS*, 2025,
doi: 10.1109/ICCDS64403.2025.11208929.
[18] A. Kumar, K. Chatterjee, and A. K. Singh, "Energy-efficient secure architecture for personalization e-commerce WSN," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 4, pp. 6901–6908, 2024,
doi: 10.1109/TCE.2024.3424574.
[19] F. T. Chimuco, J. B. F. Sequeiros, T. M. C. Simões, M. M. Freire, and P. R. M. Inácio, "Expediting the design and development of secure cloud-based mobile apps," *International Journal of Information Security*, vol. 23, no. 4, pp. 3043–3064, 2024,
doi: 10.1007/s10207-024-00880-6.
[20] I. Rizvi, S. Raj, and V. Singh, "Cybersecurity in the digital age," in *Technology for Societal Transformation*, Springer, 2025,
doi: 10.1007/978-981-96-1721-0_8.
[21] A. Q. Mohabuth, "Towards the establishment of a green computing culture in small and medium enterprises," *Lecture Notes in Networks and Systems*, vol. 1283, pp. 609–624, 2025,
doi: 10.1007/978-3-031-84457-7_38.