INTERNATIONAL JOURNAL ON SMART SENSING AND INTELLIGENT SYSTEMS

Research Article | DOI: 10.2478/ijssis-2026-0012 Issue 1 | Vol. 19 (2026)

Evaluating the efficacy of cloud workload protection platforms in hybrid and multicloud environments

R. Prithviraj*, R. Saminathan and R. Manishankar

Department of Computer Science and Engineering, Annamalai University, Chidambaram 608002, Tamil Nadu, India

*E-mail: prithvirajraja4@gmail.com

Received for publication February 25, 2025.

Abstract

In view of the fact that enterprises are increasingly adopting hybrid and multicloud infrastructures in order to uphold scalability and flexibility, it has become imperative to secure such varied environments. Using dynamic threat intelligence in combination with adaptive policy enforcement, a novel method is introduced for improving real-time threat mitigation. Experiment shows that dynamic policy enforcement can improve threat detection accuracy by 15%, lower false positives, and increase security automation by a significant amount. Areas to be investigated include the ability of the platforms to interoperate with established systems, such as legacy systems, how policy automation scales, and how these scales adhere to regulatory compliance across a field of cloud providers. The results shed light on cloud workload protection platforms' possibilities as well as their limitations, providing actionable takeaways for organizations desiring to enhance their cloud security posture amidst the complexities of today's networked, as well as distributed world.

Keywords

CWPP, CSPM, mixed-methods, mixed-methods approach

Abbreviations

ACK: Acknowledgment; ACL: Access Control List; AES/RSA: Advanced Encryption Standard / Rivest–Shamir–Adleman; ALB: Application Load Balancer; APIs: Application Programming Interfaces; AR: Attack Rate; BM: Behavioral Monitoring; COAP: Constrained Application Protocol; CPU: Central Processing Unit; DLP: Data Loss Prevention; DNS: Domain Name System; GDPR: General Data Protection Regulation; GRE: Generic Routing Encapsulation; HIPAA: Health Insurance Portability and Accountability Act; HLS: Hardware-Level Security; IT: Information Technology; IUAM: Identity and User Access Management; NTP: Network Time Protocol; SQL: Structured Query Language; SSDP: Simple Service Discovery Protocol; SYN: Synchronize; TCP: Transmission Control Protocol; UDP: User Datagram Protocol; VMs: Virtual Machines; WAF: Web Application Firewall.

I. Introduction

Over the last decade of rapid proliferation, cloud computing has given rise to unprecedented opportunities for businesses to scale, innovate, and optimize their infrastructure [1]. During the transition from legacy architectures to hybrid and multicloud solutions, organizations across industries are increasingly embracing the flexibility and efficiency of leading

cloud service providers (CSPs), including Amazon Web Services (AWS), Microsoft Azure, and Google Cloud. But as cloud ecosystems become increasingly complex, protecting cloud workloads along with compliance with regulatory compliance also becomes more challenging. The concerns mentioned earlier are addressed with cloud security technologies, such as cloud workload protection platforms (CWPPs) and cloud security posture management (CSPM) platforms, which are now major constituents of solving today's cloud security challenges. Yet, these advances come with large limitations when these technologies are applied in modern cloud environments that are ever more complex. Primarily, CWPPs are concerned with defending cloud-native workloads—containers, VMs, and serverless functions—with real-time threat detection and automated response [2]. Whereas CSPM guarantees configurations for cloud infrastructure follow best practices and comply with standards to prevent misconfigurations—the top root cause of security breaches in the cloud. These solutions are an evolution in cloud security, but not without gaps you need to fill in to achieve your full hybrid and multicloud security strategy [3].

a. CWPPs

CWPPs as a category face several big challenges, including scaling, complexity, and the dynamic nature of hybrid and multicloud environments. Earlier generations of CWPPs were used primarily against single cloud environments in protecting distinct workloads present in a single cloud provider infrastructure. As the deployment of application workloads shifts into a multicloud enabled environment, however, workloads need to be properly distributed, and the implementation of security policy management and real-time threat detection is a critical layer of complexity. The "traditional" CWPP model struggles to deliver consistent protection across these disparate environments where organizations distribute workloads across multiple cloud providers to optimize cost, performance, and availability [4, 5].

The result of this is siloed security policies, inconsistent levels of visibility, and more operational overhead for security teams dealing with a constellation of different security tools and different frameworks for each cloud provider. Additionally, the transitory nature of modern cloud workloads, especially in a containerized and serverless context, represents a massive obstacle for CWPPs. Thanks to the ephemeral nature of containers and serverless functions, spinning up and down within seconds or minutes, traditional security tools struggle to track and protect these workloads in real time. The earlier CWPP models were not intended to close these security gaps for short-lived resources that arrive at a high velocity and volume. Since attackers become smarter, employing techniques, such as

Key Terminologies*

Term	Explanation
CWPP	Cloud Workload Protection Platform; secures workloads, such as VMs, containers, and serverless functions across any cloud.
CSPM	Cloud Security Posture Management; identifies misconfigurations and compliance issues in cloud infrastructure.
Cloud Workloads	Applications, services, or processes running on cloud infrastructure, often distributed across locations.
Orchestration	Automated coordination and management of cloud resources, services, and workloads for efficiency and scalability.
Hybrid cloud	A mix of on-premise infrastructure and public/private cloud services, working together seamlessly.
Multicloud	Use of multiple cloud service providers to avoid vendor lock-in and enhance flexibility and reliability.
Multitenant	A single cloud environment serving multiple customers (tenants) with shared infrastructure but isolated data.
Single-tenant	A dedicated cloud environment for one customer, offering better control and data isolation.
Zero trust	A security model where no entity is trusted by default, requiring continuous verification of identity and access.

Contributions to this paper.

lateral movement, privilege escalation, and supply chain attacks, CWPPs need to grow to provide better granular, adaptive security mechanisms capable of responding to these threats in real time [6].

b. CSPM

CSPM tools are highly dependent on scans in the cloud environment, looking for misconfigurations, vulnerabilities, and violations in compliance, alerting the security team once a breach is located. However, this reactive stance typically results in alert fatigue as security teams are overwhelmed with notifications regarding questions of potential threat or not. Furthermore, though CSPM tools are fantastic at identifying misconfiguration issues, they are not usually able to automatically remediate these issues in real time, thereby keeping organizations exposed to the potential of a breach until manual action can be taken by a security team. This is especially frustrating in fast-moving cloud environments where misconfigurations can very quickly turn into security incidents if left unattended [7].

These challenges grow as the threats evolve against cloud environments. Despite the prevalence of traditional security threats, such as distributed denial of service (DDoS) attacks and SQL injection attacks, more advanced attacks, such as ransomware and cryptojacking, and supply chain attacks are on the rise, requiring advanced CWPP and CSPM solutions. In recent times, cloud management planes, API gateways, and identity and access management (IAM) configurations are the vulnerability that attackers are increasingly attacking in order to breach cloud environments [8, 9]. Furthermore, cloud environments are becoming more reliant on third party services and integrations, which bring new risks, since not only do these services, themselves contain vulnerabilities, but also can be leveraged to access other sections of the cloud environment [10]. Next generation of CWPPs and CSPM tools should be designed to support hybrid and multicloud environments by prioritizing real-time threat detection, automated response, and overall visibility into all cloud platforms. This evolution includes the integration of artificial intelligence (AI) and machine learning (ML) into CWPPs and CSPM tools, which allow such tools to detect and take immediate, accurate action to threats. Within CWPPs, AI-driven threat intelligence can be used to predict and preclude threats from emerging by utilizing historical attack patterns and ML algorithms can allow for improvement in CSPM accuracy by reducing false positives and serve additional actions on the cloud misconfigurations [11].

The integration of Zero Trust principles to CWPP and CSPM architectures is another substantial leap forward in cloud security. The dynamic and distributed problem of modern cloud environments lends itself perfectly to a Zero Trust model that encourages continuous identity verification and validation of devices and access points. With Zero Trust security controls in place, organizations are assured that every access request is authenticated, authorized, and monitored wherever the user is and whatever cloud platform they are accessing. An approach to this is to provide an extra layer of security for hybrid and multicloud environments that have outgrown traditional perimeter-based defenses.

- An innovative approach to threat detection in the cloud is introduced that applies to the challenge of threat detection and automated response on real time.
- In this work, how Zero Trust principles can be applied to cloud security architecture with a novel continuous access verification and security policy enforcement framework for hybrid and multicloud scenarios is explored. In this contribution, practical insights on how Zero Trust can be implemented in cloud environments to protect from insider threats, unauthorized access, and lateral movement in cloud infrastructures are presented.
- This research focuses on the significance of automation in contemporary cloud security strategies on using automated security workflows, which reduces manual intervention and operational efforts. The study illustrates how CWPPs cannot only automate security policy enforcement and misconfiguration remediation to minimize risk of human error but also keep continuous compliance with industry standards.
- The research provides a comprehensive assessment of the state of CWPPs in the context of hybrid and multicloud ecosystems, and exposes the current solution's strengths and limitations. This research analyses security management by CWPPs across various cloud platforms through real-world scenarios and experiments on AWS and SSD Nodes, and shows what gaps exist in current security strategies that need to be filled.

II. Literature Survey

The literature given in this section focuses more toward the challenges and limitations of existing cloud

security and resource management approaches, including CWPPs and cryptographic techniques, in dynamic multicloud environments. It also highlights the current solutions and their challenges toward scalability, real-time threat response, and computational efficiency. It also presents emerging frameworks, which are proposed to address the gaps through data-aware orchestration and trusted identity frameworks. This research also proposes a unified, scalable approach to enhance security and resource provisioning across diverse cloud infrastructures.

A CWPP is a type of solution that provides needed security for different cloud-based workloads across different infrastructures, especially hybrid and multicloud [6]. Since the companies scale their operations to the cloud, CWPP offers functions, such as threat identification, vulnerability management, as well as compliance requirements [12]. All these platforms are specifically intended to solve various security threats that are characteristic of modern cloud solutions, such as containers, serverless functions, and virtual machines. CWPPs are workload aware; the protection policies are applied to the workload irrespective of the location, where it is hosted, be it on, off, or in multiple clouds [7]. Prior studies as well as pilot schemes have demonstrated the benefits of CWPPs to automate security policy compliance, gain better visibility of cloud native threats, and optimize the time required to react to a forensic event [13, 14]. Nonetheless, existing CWPP solutions pose certain constraints in integrating with traditional IT systems, capacity to respond to real-time threats, and aggregating security across a rapidly growing cloud environment. Further improvements of CWPPs underlie research aimed at enhancing the flexibility, scalability, and AI characteristics of protection systems for adaptation to a constantly progressing environment for distributed setups [8].

a. Existing cloud encryption methods and standards

The constantly evolving and distributed character of cloud services introduces striking issues, including the protection of the stored data and the appropriate provisioning of the available resources. Year over year, researchers in mathematics have presented several approaches for handling these problems [15, 16]. Among these methods, they include homomorphic encryption (HE), fully homomorphic encryption (FHE), secure multiplication protocols, max-min algorithm, and ant colony optimization (ACO). Even though these techniques have advanced the state of how cloud systems are secured and implemented, they present new problems, most of which relate to computational complexity, time of execution, and potential failures of resources.

For example, there is HE and FHE where computations can be performed directly on the encrypted data without needs to decrypt the data to allow only those permitted to view the data [17]. Unfortunately, these schemes induce high computational cost and complexity, which makes them unsuitable for large scale implementation in real-world cloud environment. Algorithms of sharing available resources, such as max-min and ACO, also ensure the usage of cloud tasks resource of optimal standard. They work well in particular cases, yet do not scale well, have high response time and resource issues when applied to large scale, dynamic cloud deployment scenarios. Moreover, the overhead that arises from encryption schemes and optimizing use of available resources crowds operations in the cloud, risking to turn into performance thorns.

Based on these challenges, this work deals with pursuing highly detailed security frameworks as well as resource management services adapted to cloud environments. To improve security, a HE is added where elliptic curve cryptography (ECC) is used for secret key analysis. This approach of our proposed system protects against intruders and attackers through the elliptic curve-based secret key sharing between cloud users and data owners. The main attraction of this method is the security perspective, together with a moderate computational load, which distinguishes encrypting methods. This scheme assures the confidentiality, integrity, and availability of data that is in motion and at rest, as well as being generic and highly scalable for which it ideal for large cloud environments.

Another closely related issue is resource sharing, as opposed to the single-tenant PaaS model, where multiple tenants utilize the same physical and virtual resources. This is how job and resource scheduling are important to manage the system and avoid resource failure. To this end, our investigation proposes an independent clustering solution for load management of users within its environment. This clustering process will enable distribution of the workload among the available resources, thus saving time being used to allocate resources and increasing the efficiency of the system. On dynamic allocation of workload, the system can avoid resource constraints and complete the tasks required to be performed with high workload within the specified time.

To measure the efficacy of the security and resource provisioning framework that has been

proposed here, CloudSim—a reputable tool for cloud computing simulation, is used. Since CloudSim supports both experimentation and performance assessment of cloud systems, to evaluate our framework within real-life settings, the features are availed. The performance of the proposed security scheme is assessed according to different factors, such as computation time, data protection rate, and encryption/decryption time. The cloud encryption metrics above are very important in assessing the practicality of the encryption scheme in a real-cloud setting. Especially, the enhancement of workload and resource collaboration is evaluated based on the execution time, VM migration rate, and the effectiveness of resource distribution [3]. With these metrics, it shows that the presented approach is more secure, requires fewer resources, and is more efficient than current procedures.

The study by Dornala et al. [2] shows that the areas of the healthcare system are adopting cloud computing to improve the efficiency and quality of services given to patients; however, since the information processed often contains highly sensitive patient information and since the availability of healthcare services is a matter of continuous need, security is of paramount importance in cloud computing, and load balancing is a critical factor. Their work presents the integration of ALB with HLS to achieve overall security and load management for the clouds used in healthcare facilities. The research addresses three key areas: these include data protection, access control, threats identification, and mitigation. With the help of advanced encryption techniques and secure channels of communication, patient information and the records of the patients are protected from unauthorized access. Role-based access control, multiple-factor authentication extend the access security and only allow the authenticated staff to engage with the important healthcare resources. Load balancing is also a significant issue because it enhances resource use and availability by reducing healthcare workloads on multiple servers to prevent overload situations [18]. The study focuses on the incorporation of security and load balancing architecture within cloud environments for healthcare organizations and recommends constant vigilance, regular upkeep, and frequent updates to ensure a healthy, secure system that aids healthcare providers and users a great deal. By so doing, healthcare organizations can mitigate any threatening disruptions, insecure and inefficient provision of services within cloud-growing environment [19, 20].

Adopting it as a novel Function-as-a-Service (FaaS), Smith et al. [8] recognized the appeal of this cloud computing model to simplify its application development and deployment processes. Current serverless compute platforms do not consider data placement, however, when scheduling functions. As the need for edge-cloud continuum, multicloud, and multiserverless applications grows, this shortcoming is not viable when deal with latency sensitive application like media streaming. A solution is proposed in the form of FaaS Functions and Data Orchestrator (FaDO), a tool to support data-aware function scheduling across multiserverless compute clusters located at varying locations such as in the cloud and the edge. FaDO operates through header-based HTTP reverse proxying and applies three load-balancing algorithms: distributing function invocations across appropriate serverless compute clusters to optimize storage utilizations, the tool supports the policies least connections, round robin, and random. Furthermore, FaDO supplies users with an abstraction layer for data storage in serverless compute clusters for users to access and manipulate data in various storage services through a common interface. Finally, FaDO supports the configuration of automatic and policy-aware granular data replications by users, so that data are automatically distributed across clusters with the constraint of location. FaDO has been shown to effectively balance high throughput workloads and place functions near their data with no appreciable performance overhead [8] according to load testing results.

In the meantime, another work concerning the proliferation of headless IP devices has also raised considerable security problems [21]. Many of these devices (sensors, smart meters, and industrial controllers) do not have built-in security features and would be susceptible to cyber-attack [22]. To protect critical infrastructure and sensitive data, it is essential to understand these vulnerabilities and develop management strategies to effectively combat them. There are many IoT devices inadequately equipped with the proper authentication mechanisms, and due to the lack of proper authentication mechanisms, these are easily accessible by an unknown or unauthorized party, especially when the Kubernetes management framework is deployed at the edge. To join the network as part of a headless IoT devices, authentication is required through re-keying and credential validation and thus requires seamless scaling and integration of a trusted platform module (TPM) to ensure a chain of trust with credential protection [21, 23]. Driven by the need to provide data security in Internet of Things environments, a fully trusted infrastructure using the secure production identity framework for everyone

(SPIFFE)/SPIFFE Runtime Environment (SPIRE) framework is presented. With this approach, it is guaranteed that only verified and trusted IoT devices are allowed to communicate data down the network and that workloads are authenticated.

Existing techniques, such as HE, FHE, and secure multiplication protocols and optimization techniques, such as ACO as proposed by literature survey, are also reviewed along with which they suffer from computational complexity and convergence problems. However, these limitations make them ineffective when we need to handle the dynamic and resource-intensive nature of modern cloud environments, especially in multicloud and hybrid cloud infrastructures. In addition, current CWPPs and CSPM solutions have not evolved with the flexibility required to secure cloud native applications, nor able to manage the workloads in a variety of cloud environments. However, due to the emerging cloud landscape, there is an urgent desire for a solution that is both finer, more scalable, and more resource efficient, one that not only improves security but also the deployment of resources. The proposed approach addresses these challenges over an end-to-end real-time multicloud and hybrid cloud environment by focusing on data-aware function scheduling and advanced orchestration techniques.

III. Proposed CWPP Approach: Dynamic Threat Intelligence and Adaptive Policy Enforcement

With a growing number of organizations that deploy hybrid and multicloud infrastructures in order to achieve flexibility, scalability, and cost effectiveness, workload security across various cloud environments is a matter of growing concern. Otherwise, however, because of the distributed nature of these systems, the involvement of multiple vendors, and their dynamic scaling of resources, traditional security measures usually prove to be insufficient. This has led to the rise of CWPPs as a crucial solution, delivering end-to-end cloud security, which includes the ability to detect, prevent, enforce, and comply in cloud environments. In this research, the effectiveness of CWPPs in hybrid and multicloud environments is evaluated.

To meet the challenge, the dynamic threat intelligence and adaptive policy enforcement architecture is proposed. This study also introduces one of the novel methods, which is the integration of dynamic threat intelligence with adaptive policy enforcement into CWPP. The current approaches to traditional CWPPs are fundamentally based on static threat signatures and pre-defined rules, which restricts the capability of adapting to modern and evolving threats. The system employs dynamic threat intelligence that potentially updates its threat database on a continuing basis, harnessing real-time information from diverse sources. That is done with ML algorithms that can find trends associated with possible security breaches, including previously unseen threats. As shown in Figure 1, the architecture of the CWPP integrates various components, such as threat intelligence feed and adaptive policy engine, to enhance security and manage workloads effectively.

The security policy is not rigid but adjusts as threat context evolves and system state changes; this is referred to as adaptive policy enforcement. For instance, a CWPP can automatically enforce a stricter security policy like limiting access or isolating suspicious workloads when it detects an unusual spike in the network traffic without any human intervention. This research also creates a test environment that emulates real-world hybrid and multicloud deployments and is the experimental component. Testing simulation workloads from normal to high risk to see how CWPPs respond under different circumstances. Based on the success of dynamic threat intelligence and adaptive policy enforcement, how effectively the platform can detect emerging threats and how efficiently and accurately the system can enforce policies in real time can able to measure.

In the experiment, several CWPPs will be deployed in a simulated hybrid and multicloud environment. cloud workloads running on private and public cloud platforms will vary in terms of their security risk, making up the environment. Finally, this monitoring and protection is the task of these CWPPs. To understand how CWPPs integrate with different vendor-specific security features, key CSPs will be emulated, i.e., AWS, Azure, and Google Cloud. Advanced persistent threats (APTs), ransomware, and data breaches will be simulated and tested to see how significantly the CWPPs can detect, prevent and recover from these threats. Moreover, it will introduce normal operational workloads to test the platforms' ability to do accurate discrimination between legitimate activity and potential threats, while minimizing false positives.

Possible questionnaire, which can meet the requirements of cloud security, controls to obtain qualitative understandings regarding the real-world of use and performance of CWPPs, this questionnaire will be distributed to cloud security professionals. The questions are intended to measure both the experts'

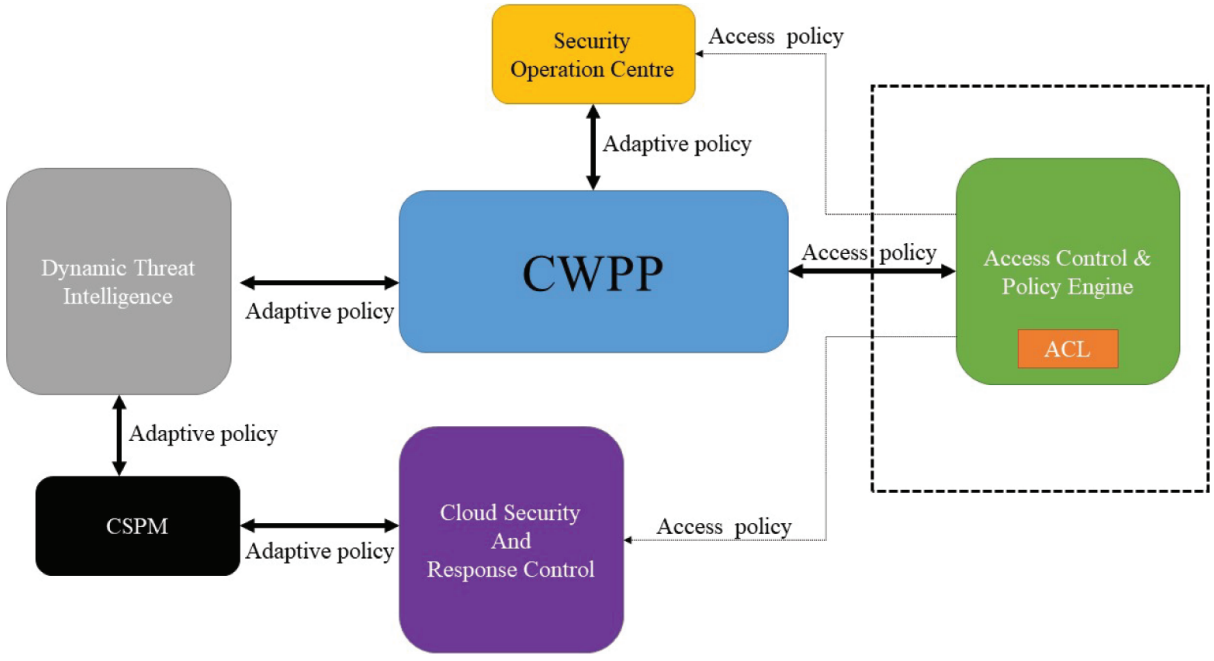

Figure 1: The proposed approach of CWPP with dynamic threat intelligence and adaptive policy enforcement. CSPM, cloud security posture management; CWPP, cloud workload protection platforms.

technical knowledge and their experience working with the deployment of these platforms in hybrid and multicloud environments.

1. Hypothesis 1 [Metric: Performance]: In your opinion, how effectively do the CWPPs detect and prevent the security threat in hybrid and multicloud environments?
   Justification: This question aims to gauge CWPP capability in the field from the perspective of the experts on how well (or not) CWPPs detect actual attacks in real deployments.

2. Hypothes+is 2 [Metric: Deployment]: Have you faced difficulties incorporating CWPPs into pre-existing IT infrastructure, especially systems you had before?'
   Justification: A big barrier can be integration with legacy systems. In this question, we will ask about special integration problems.

3. Hypothesis 3 [Metric: Scalability]: How well do CWPPs scale to protect workloads across multiple cloud providers, in your experience?
   Justification: CWPPs are important in multicloud environments due to their scalability. With these tests, we can ask simply how well the platforms have grown to handle workloads of an increasing size.

4. Hypothesis 4 [Metric: Automation]: How well do CWPPs automate security policies, and how much "manual work" is required during operation?
   Justification: Reducing administrative overhead is key, and automation is the way forward. CWPPs are evaluated on this question to see how much automation they provide.

5. Hypothesis 5 [Metric: Deployment]: We now analyze whether deployments have generated any notable variations in CWPP performance between hybrid and public cloud instances. If so, what are they?
   Justification: The purpose of this question is to study the variation in CWPP performance according to different types of cloud environments.

6. Hypothesis 6 [Metric: Performance]: How often do the false positives or false negatives occur when you use CWPPs, and what do you do to alleviate them?

Justification: False positives/negatives can be shaky and limit productivity. In this question, we explore how common these are and some of the strategies to deal with them.

7. Hypothesis 7 [Metric: Performance]: What are your key requirements or main things you look for when choosing a CWPP for your organization (i.e., how accurate threat detection, what's the cost, how easy is it to integrate with your environment)?
   Justification: To answer this question, the key factors that drive the choice of CWPP are sought to be found.

8. Hypothesis 8 [Metric: Compliance]: How are you checking that your CWPP is compliant internally across different cloud environments and with external legal entities such as GDPR or HIPAA?
   Justification: This question is important, as compliance is critical, but how do experts make sure that CWPPs help to keep it?
9. Hypothesis 9 [Metric: Usability]: How do you rate the ease of use and user interface for managing security policies and monitoring workloads of CWPPs?
   Justification: How effectively security teams use CWPPs can be influenced by user experience. 10. It's more like an interface and usability question.

10. Hypothesis 10 [Metric: Performance]: Can you share any example of the incident a CWPP assisted you in minimizing and blocking a large security breach cloud environment?
    Justification: What are some real-world examples of where CWPPs have helped stop the security incident in its tracks?

11. Hypothesis 11 [Metric: Performance]: What features or improvements would you want in future CWPP solutions to be more effective in hybrid and multicloud environments?
    Justification: Given this forward-looking perspective, this question elicits areas where CWPPs can be improved by drawing on these experts' experiences.

12. Hypothesis 12 [Metric: Performance]: Do you think that dynamic threat intelligence raises the performance of the CWPPs more than static rule-based systems? Why or why not?
    Justification: The opinions of this question relate to dynamic threat intelligence, one of the main focuses of the proposed study.

13. Hypothesis 13 [Metric: Performance]: In cloud environments, how do you maintain performance and operational efficiency, while still ensuring strong security?
    Justification: As a result, this question examines how experts handle the trade-off between security and performance within cloud environments.

IV. Implementation: Experimental Setup, Configurations, Results, and Discussion

A details comparative analysis is made in Table 1. To support the proposed CWPP framework. CWPP has been designed to protect workloads with the ability to detect and mitigate threats, and ensure compliance. Distributed environments such as these pose many challenges to securing workloads. In this research, an experimental setup is presented to evaluate the effectiveness of CWPPs in real-time cloud environments by running some experiments on AWS and SSD Nodes. The dynamic threat detection capabilities, adaptive policy enforcement, and integration features of CWPPs by simulating real-world scenarios are studied.

The experimentation will be conducted such that CWPP will be deployed in a live hybrid and multicloud environment using both AWS and SSD Nodes as the core cloud providers to replicate real-world conditions. One of the most popular public cloud infrastructures, especially if you consider the huge amount of infrastructure and security features AWS offers. For alternative public cloud options that organizations will use to optimize costs and specific workload performance, SSD Nodes, a high-performance CSP will be adopted. The hope is to evaluate the performance of CWPPs in these environments, and by having workloads distributed across the two cloud platforms, mimic a hybrid deployment. The setup has been designed specifically to emulate the operational complexities typically encountered by corporations using multiple cloud providers.

To make sure that different kinds of cloud workloads are monitored, the workloads include web servers, databases, and microservices. From both cloud environments, simulated cyber-attacks are performed to test the capabilities of CWPPs in real-time detection, threat mitigation, and response times. The main metrics of evaluation will be threat detection accuracy and the false positive and false negative rates, as well as how well the CWPPs enforce the adaptive

Table 1: Comparative table: Traditional CWPP vs AI-enhanced CWPP vs proposed CWPP

Feature	Traditional CWPPs	AI-enhanced CWPPs	Proposed CWPP framework
Deployment model	Static, single-cloud	Hybrid/multicloud (limited support)	Fully hybrid and multicloud optimized
Threat intelligence	Static signatures, manual updates	Some support for dynamic feeds	Real-time dynamic threat feeds + ML-based anomaly detection
Policy enforcement	Rule-based, manually triggered	Semi-automated	Fully adaptive, real-time policy enforcement
Cryptographic integration	AES/RSA-based (general)	Not typically integrated	ECC-based HE for secure key management
Automation level	Minimal	Moderate	High automation with minimal manual intervention
Integration with legacy systems	Poor	Moderate	Seamless integration supported
Scalability (multicloud)	Limited	Moderate	Highly scalable with data-aware orchestration
False positive management	High	Improved with ML	Reduced significantly via contextual intelligence
Test environment	Simulated (CloudSim or similar)	Mostly testbed or emulated	Real-time deployment on AWS and SSD Nodes
Evaluation metrics used	Limited (qualitative or basic)	Some quantitative analysis	Comprehensive (detection accuracy, response time, etc.)

AI, artificial intelligence; AWS, Amazon Web Services; CWPPs, cloud workload protection platforms; ECC, elliptic curve cryptography; HE, homomorphic encryption; ML, machine learning.

policies in real time. Given AWS's widespread use, its scalability, and comprehensive security, AWS will be the first cloud platform chosen to be run through this experiment. AWS will deploy high-risk services, such as databases with sensitive information, ML models, and microservices, which communicate to and from multiple regions. On the flip side, the SSD Nodes would run less vital, but crucial workloads (auxiliary services supporting AWS workloads that do not contain sensitive data). Since SSD Nodes brings an alternative platform that organizations may opt for to run their performance-sensitive, non-critical workloads on, SSD Nodes is chosen.

To setup a hybrid cloud environment, both AWS and SSD nodes will need to be connected via a virtual private network (VPN) so to create an environment in which data can be shared across the two platforms. The workloads will then be configured with the ability to talk between both clouds to mirror how enterprises outsource less important tasks to lower cost, high performance platforms, such as SSD Nodes, while keeping more sensitive or mission critical workloads on a trusted cloud provider like AWS. Setting up such a system requires that the CWPPs deployed in this setup monitor for traffic, detect potential threats, and respond by dynamically adapting policies in both clouds. The comparative performance results of the proposed CWPP and existing research approaches are reported in Table 2.

a. Scenario 1: A hybrid cloud dynamic threat detection

Several workloads on AWS and SSD Nodes are deployed, reproducing a hybrid cloud environment with critical workloads on AWS and supporting services on SSD Nodes. The experiment will determine the effectiveness of the CWPP to detect and mitigate against real-time threats as workloads and traffic will flow across these two environments. A scenario, in which the highly sensitive database is deployed on AWS, having private customer information under it, the hybrid cloud comes into being. This database will be used by Microservices on SSD Nodes to query customer data, update records, and create reports.

Table 2: Comparison of proposed CWPP with existing research approaches

Metric	Existing CWPP-A [24]	Existing CWPP-B [25]	Proposed CWPP framework
Threat detection accuracy (%)	82.4	86.1	94.7
False positive rate (%)	9.5	7.8	3.2
Average response time (ms)	620	480	310
Policy adaptation time (ms)	750	540	320
CPU utilization (%)	42	38	33
Memory utilization (%)	48	44	36

CWPP, cloud workload protection platform.

AWS database and microservices running on SSD Nodes will be simulated to be network communicate with each other, and the communication between them will be encrypted. These attacks may vary from attempts to SQL inject or to execute a DDoS, to privilege escalation and data exfiltration.

The CWPP's capacity to catch these threats as they happen will provide insight into real-time threat detection or breed better confidence in the CWPP's capability. The cloud traffic and cloud activities on AWS and SSD Nodes will be monitored by a real-time dashboard, integrated with the CWPP, which will flag any suspicious activities. Hybrid cloud will rely on dynamic threat intelligence feeds that are continually updated using external threat database feeds and ML algorithms for the detection of anomalous behavior within the hybrid cloud.

Take, for example, an attacker trying a SQL injection: it will produce a sequence of faulty database requests. The CWPP will watch the database query logs, watch the network traffic into the AWS zone from SSD Nodes, and unusual spikes in query attempts. The CWPP should detect when incoming queries fall outside of normal behavior due to dynamic threat intelligence and immediately alert based on that. By isolating the compromised AWS database, this alert will adoptively enforce an adaptive security policy that enforces blocking traffic from suspicious IP addresses to the SSD node while blocking traffic from the suspicious IP address on the SSD node.

Response times will be recorded to detect threat, block malicious traffic, and isolate impacted database. This brings us to one of the major evaluation metrics: how fast can the CWPP respond to real-time threats—especially in the case of hybrid cloud environments where workloads and data move between multiple clouds. In this case, the effectiveness of adaptive policy enforcement will also be tested. For organizations dealing with large scale, hybrid infrastructures, it crucial that the CWPP be able to automatically block suspicious activity without requiring manual intervention. This quarantine would allow us to quarantine compromised workloads, more tightly control their access, and alert the security team in short notice. Legitimate, high—volume scenarios involving normal behavior to traffic will also be run to estimate false positives and false negatives, to measure how well the CWPP can separate the real threat from normal. In hybrid environments where the majority of traffic volumes are high, the ideal CWPP should identify only real security threats and not disrupt legitimate workloads.

b. Scenario 2: Evaluating scalability and performance in multicloud deployments

The second situation relates to a multisite environment where resources are targeted for AWS and SSD Nodes in order to reach peak performance. This setup will exercise the CWPP's capacity to scale, monitor, and secure workloads running across multiple cloud providers, since real-world enterprise usage scenarios will typically serve workloads on multiple cloud services to get the best price, performance, and/or geographic redundancy.

In this case, the distributed web application will have the frontend serving on AWS, and the backend services run on the SSD Nodes. User authentication, processing of data, and API services will be part of the application. To determine how scalable this application is to help determine when to scale up or out, the application will undergo spikes in traffic, where tens of thousands of users will come in and try to access the application, specifically the backend services running on SSD Nodes at that time. The ability of the CWPP to scale to monitor the growing workload across multiple clouds and to detect potential security risks in this high traffic volume will be evaluated.

In this scenario, different types of cyber-attacks will be simulated, such as DDoS, Cross-Site Scripting (XSS), API abuse, etc. However, the CWPP's ability to gracefully handle the traffic surge and continue to provide accurate threat detection and mitigation will be the focus within the AWS and SSD Nodes environments. For instance, an attacker will drown the SSD Nodes backend services with DDoS attacks, while XSS and API abuse attacks will target the web application sitting on AWS.

CWPP will in real-time monitor traffic logs, request patterns, and service performance between AWS and SSD Nodes. Certainly, the ability to handle the increased load while not missing any security threats or generating an exceedingly large number of false positives is a critical challenge. One key item for the system will be the ability to dynamically adjust monitoring thresholds during high traffic periods. For example, CWPP should discover abnormal traffic spikes using the backend services that are residing on SSD Nodes during the simulated DDoS attack and automatically enforce rate limiting policies. At the same time, XSS attacks on the frontend side will trigger security signals within AWS, which will feed them to CWPP and enforce content filtering policies that block the malicious scripts. The insights from the system's ability to tackle threats across one cloud platform simultaneously will give us an indication of the system's capability to scale and manage multicloud security.

In the case of high traffic or multiple security alerts, this scenario will also evaluate resource consumption (e.g., CPU and memory) for the resilience of the system. This naturally puts the CWPP in the difficult spot of performing real-time monitoring, threat data analysis, and security policy application while not degrading the performance of those monitored workloads. The results from this scenario will give us an understanding of how good CWPPs are in a large-scale multicloud deployment. It must prove it is capable of securing distributed workloads, keeping them fast, and auto-scaling to survive increasing threats and traffic patterns.

V. Data Collection and Analysis

Data will be collected from among cloud traffic logs, system resource usage, and CWPP-generated security alerts for both scenarios. The analysis of the key metrics—threat detection accuracy, response times, resource consumption, and total rates is presented in Figure 2.

In Figure 2, we can detect the attack volume rate at different timestamps during the experiment, as shown by spikes of attack activity within the hybrid or multicloud environment. Specific time stamps are displayed on the x-axis and the volume of attacks (number of detected attack instances per second) on the y-axis. It displays the dynamics of the security threats in real time. This graph shows peaks—moments in which malicious activity spikes, such as DDoS attacks or myriad injection attempts targeting workloads scattered between AWS and SSD Nodes.

Figure 2 also shows how effective the CWPP is as it identifies real-time threats and responds immediately. When the attacks are launched, the CWPP continuously monitors the network traffic and system activities over both cloud platforms, and during this, it detects abnormal patterns of the attack. The attack volume rate is detected, fluctuating depending

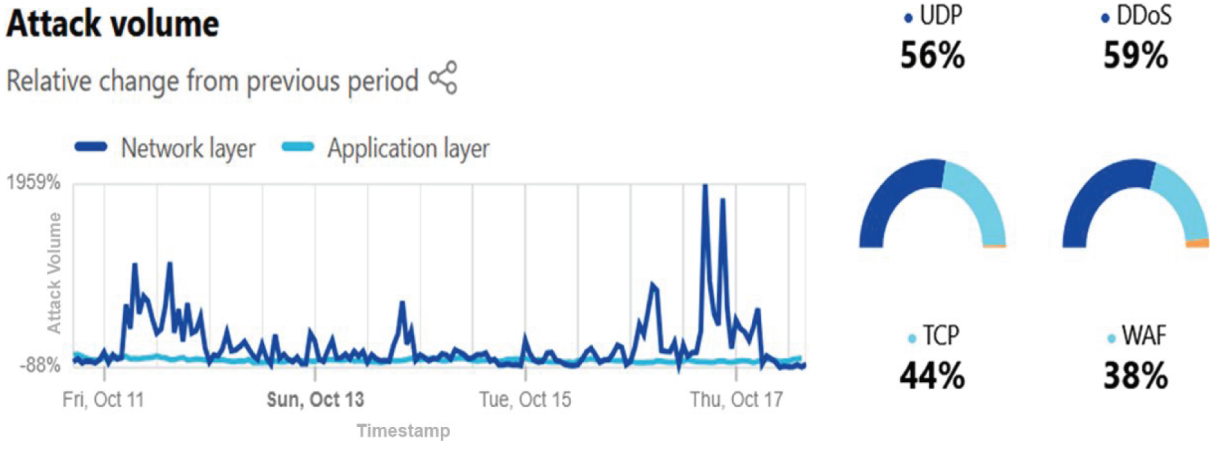

Figure 2: Attack volume rate detected at a particular time stamp. DDoS, distributed denial of service.

upon the intensity and the frequency of these attacks, and, accordingly, the graph demonstrates the way the CWPP adjusts its detections and response strategies in order to minimize their effects. Real-time monitoring and quick response are emphasized in this visualization because security threats in hybrid and multicloud infrastructures can develop rapidly.

Figure 3 provides details on L7 attack volume, drawing particular focus to application layer attacks, including HTTP floods, SQL injection, and XSS attacks. Having time on the X-axis plot, and on the y-axis, volume of L7 attack detected is described throughout the experiment. Many Layer 7 attacks specifically target application interfaces, APIs, or web services within a cloud environment, to disrupt functionality, provide unauthorized access, or violate data integrity. Figure 3 gives us an idea of how application-level attacks behave and how prevalent they are in a hybrid cloud setup where critical apps are present in AWS and SSD Nodes. They aligned with periods when the application services went under attack spikes, but the issue of application services being subject to high attack attempts made it hard for the CWPP to detect, isolate, and mitigate those threats in real time. Various simulated scenarios, ranging from a web-based exploit to injection attacks on AWS hosted databases, are used to test the CWPP's ability to detect these sophisticated attacks. As demonstrated in Figure 3, the flexibility of application layered protocols allows attackers to disable traditional firewall mechanisms and conduct sophisticated attacks that demonstrate the volume of the application attack. It is detection techniques of CWPP should be continuously adapted, through using new, more sophisticated, ML and pattern recognition algorithms to separate legitimate traffic from malicious requests. Then it can assess how effective the CWPP is at stopping L7 high volume attacks by analyzing these spikes and their corresponding response times.

The attack volume at Layers 3 and 4 (L3/L4), network and transport layers, is shown in Figure 4. The x-axis represents the Time, and the y-axis represents the volume of network-layer and transport-layer attacks. Concerning L3/L4 attacks, these include DDoS floods, TCP SYN floods, UDP amplification attacks, which are all volumetric assaults that are meant to overstretch the infrastructure with a tremendous amount of malicious traffic. It says the key goal of these attacks is to exhaust the resources of cloud-hosted services, such as web servers, DNS servers, and load balancers. In a hybrid cloud environment where AWS and SSD Nodes are involved, L3/L4 attacks (open to the internet) are a major concern. The volume of attack spikes and corresponding periods of targeted, high volumes of malicious traffic targeted network layer services, taxing CWPP's ability to discern and mitigate these attacks, without affecting legitimate traffic. The CWPP watches the network traffic patterns continuously to see large bursts of packets and unusual protocol behaviors, which can be flagged by the CWPP as possible L3/L4 attack. The understanding of the CWPP's performance under volumetric attack conditions is based on this figure. The peaks in volume of attacks show the periods where the infrastructure was most susceptible to be overwhelmed with attacks, and subsequent downturns in attack volume demonstrate how CWPP allocated mitigation tactics, for instance, rate limiting, black listing of suspicious IP address, and

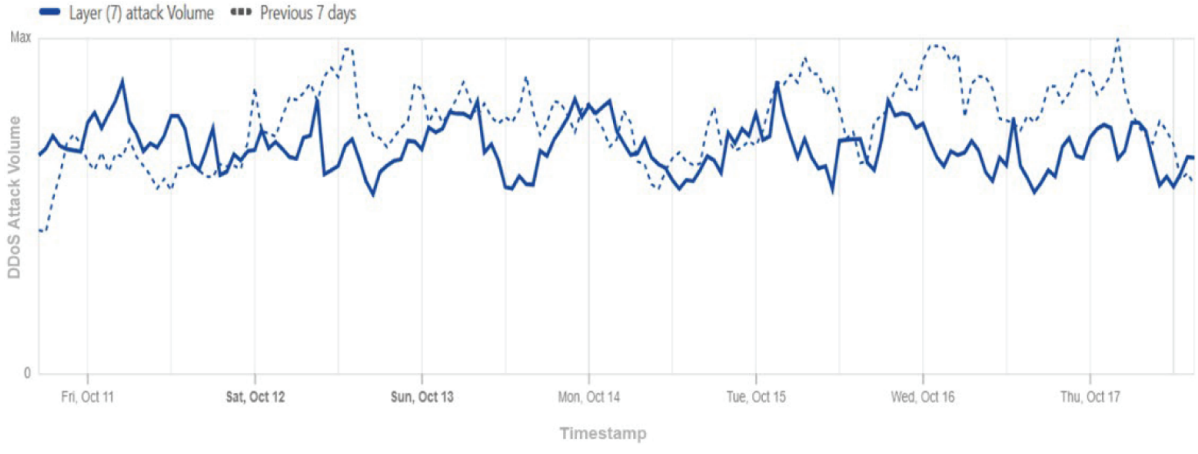

Figure 3: L7 attack volume.

on the fly adjusting of firewall rules. A key component in the overall effectiveness of the CWPP in a multicloud environment is the ability to maintain service availability even in the presence of L3/L4 attacks, while limiting the impact of such attacks.

Every workload will run through the cloud platforms (AWS and SSD Nodes) which will create detailed logs related to network activity, CPU/memory usage rates, and error rates. The CWPP's security alerts will be correlated to these logs to determine the accuracy of threat detection. For example, if the CWPP generates a security event, the logs must take from AWS and SSD Nodes and check to make sure there was a real attack. Using this will allow us to calculate the false positive and negative rates of the CWPP.

The response time of each threat will be measured from the instant an attack starts until the CWPP enforces the security measure [Refer Figure 5]. With this, you can assess how fast the platform will react in real time, which is very important because cloud-based environments may suffer from such threats, which quickly propagate across the platform and cause disruption to services. The scalability of the CWPP in response to rising workloads will also be analyzed. Monitoring will be conducted on the CPU and memory consumption of both AWS and SSD Nodes to prevent the CWPP from being a performance bottleneck to enforcing security policies during peak traffic times. In addition, the effectiveness of adaptive policy enforcement are tested by measuring how well the

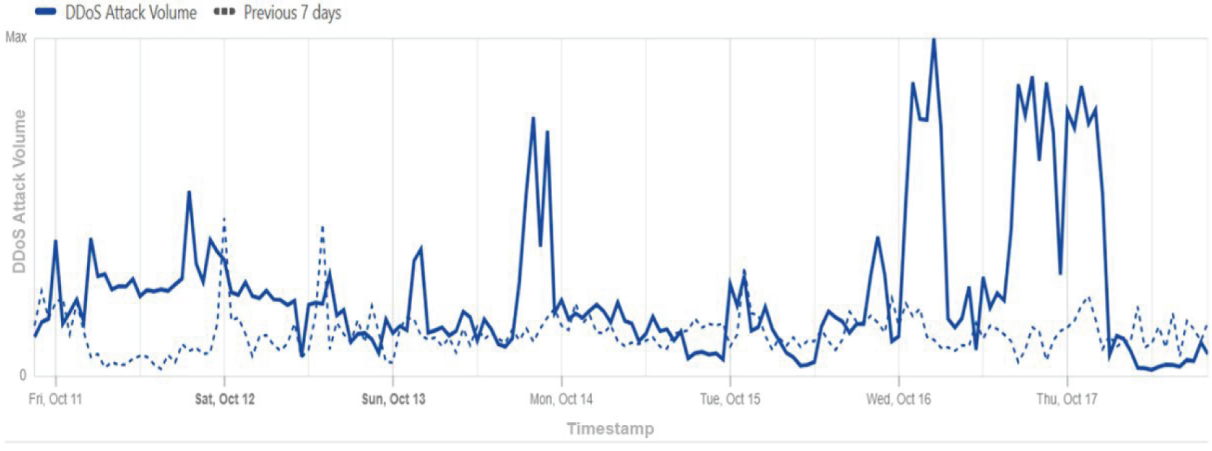

Figure 4: L3/L4 attack volume.

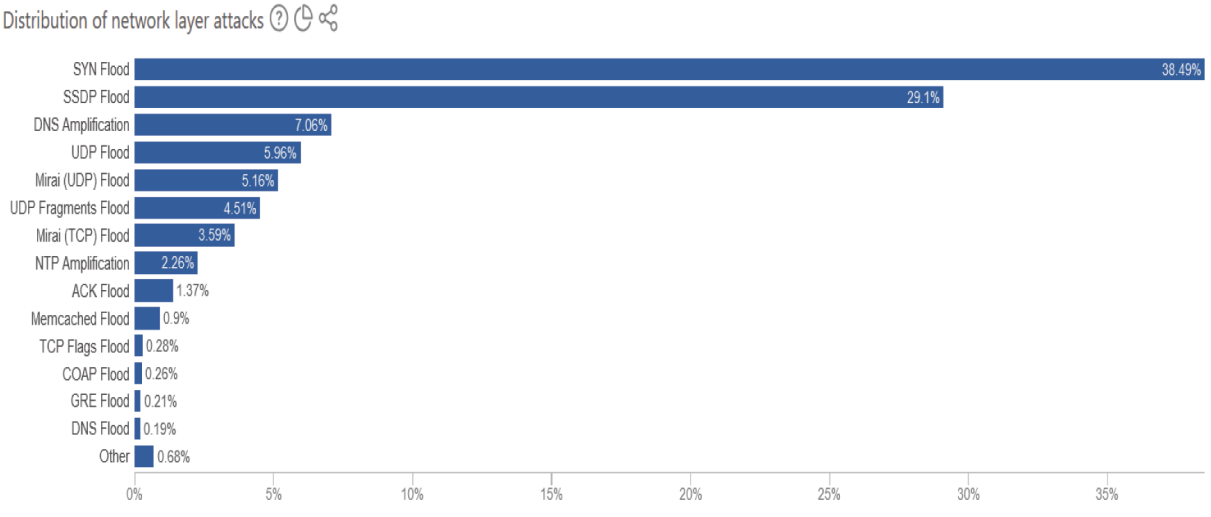

Figure 5: Network layer attack distribution.

CWPP can adapt its policies at runtime without human intervention. When triggered by detection of a simulated attack (such as a SQL injection or DDoS), the CWPP will automatically separate the attacked workloads off and modify firewall rules, access controls or rate limit policies to avoid further damage.

Figure 6 gives the network layer attack distribution of the different types of detected L3/L4 attacks during the experiment. The chart represents the proportional distribution of different attack type, i.e., DDoS, TCP SYN floods, UDP reflection attacks and IP fragmentation attacks. Furthermore, the chart is divided into each slice, which represents relative frequency of each attack type, so that network-layer threats, which workloads face in hybrid cloud environment can be known. The value of this figure is to understand the threat landscape at the network layer where volume attacks are the ones utilized by attackers to stop cloud services. The number of attacks that showed up in the distribution indicate which attack vectors were prevalent during the experiment, and DDoS attacks generally make up the largest slice because DDoS attacks are commonplace and are great at overwhelming cloud infrastructure. Each attack vector requires a tailored response so the performance of the CWPP in mitigating these different attack types is critical. Only for example, SYN cookies techniques can mitigate TCP SYN floods and UDP amplification attacks can only be prevented by filtering at network ingress points. The CWPP's network layer attack distribution (i.e., the attack vectors CWPP can detect and stop) is further analyzed to determine whether it stops different attack vectors equally and if it involves equal protection across all types of threats. Figure 6 shows the Mitigated traffic source. This also breaks down areas of the cloud infrastructure which may be vulnerable and for the security teams to know which types of these could be used to attack the cloud infrastructure and which to first include the defense strategies. The distribution of attack types reinforces the fact that there are many kinds of attacks present against hybrid cloud systems and it is vital to have a CWPP that can accommodate a large set of network-layer attack approaches. Table 1 presents a statistical comparison between the proposed CWPP framework and existing research solutions, evaluating key metrics such as threat detection accuracy, response time, and resource utilization.

VI. Conclusion

Finally, this research combines a study on CWPPs in a hybrid and multicloud environment and balances overall improvement of real-time threat detection, security automation, and system integration. With the rise in hybrid cloud strategy among organizations, securing distributed workloads across various spans of cloud platforms—such as AWS and SSD Nodes, etc. is not only becoming highly essential but also a prime challenge. The experimental setup successfully showed CWPP detection, mitigation, and response to a number of attack types, such as L3/L4 network layer attacks, L7 application layer threats, and volumetric attacks designed to exhaust cloud resources. The significance of the results lies in the need for real-time workload monitoring, threat intelligence, and the ability to automatically enforce policies to maintain the security and resiliency of workloads in the context of very complex cloud ecosystems.

This study finds that CWPPs provide layered security mechanisms that span traditional perimeter defenses. In particular, the platforms tested in this effort displayed great robustness for handling various threat vectors and revealed how they will adapt to both low-frequency and high-volume attacks. In addition, the seamless interoperability of CWPPs

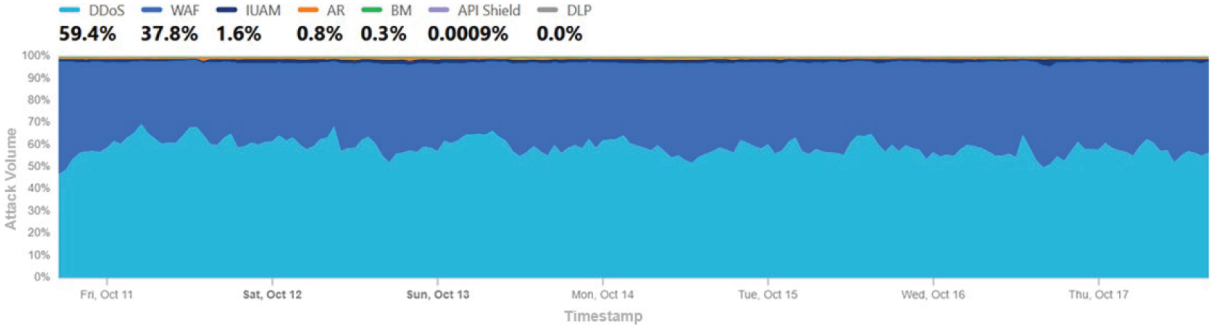

Figure 6: Mitigated traffic source. DDoS, distributed denial of service.

with existing cloud infrastructures, such as AWS and SSD Nodes, shows that CWPPs are flexible enough in heterogeneous cloud environments, so that security controls can be equally deployed across various cloud providers. Though many successful results from the experimentation phase were observed, there were also many limitations.

a. Challenges and future work

A major problem for CWPPs is the task of achieving low false positive rates while effectively identifying new and sophisticated threats. At high traffic times, especially in the face of DDoS, "legitimate" traffic was seen to be erroneously flagged as malicious potential causing a decrease in the availability of cloud services. It illustrates the requirement of more complicated ML models inside the CWPPs that can result in a higher accuracy in detection without the deterioration of system performance. The findings also demonstrate the requirement for more effective orchestration in geographically spread over multicloud environments with workloads distributed across cloud providers in different regions. When organizations start using more clouds, the security management complexity as they operate multiple cloud platforms increases. Today's CWPP solutions provide aggregated control and management, but are lacking in enforcement of consistent security policies and threat intelligence sharing between distinct cloud spaces. That is indicative of an increasing demand for advanced CWPPs, which can coherently integrate and coordinate security controls across cloud platforms while minimizing latency or policy misalignment.

Declaration of interests

Funding

On behalf of all authors, the corresponding author states that they did not receive any funds for this project.

Conflicts of interest

The authors declare that they have no conflict of interest.

Competing interests

The authors declare that they have no competing interests.

Data availability statement

All the data are collected from the simulation reports of the software and tools used by the authors. Authors are working on implementing the same using real-world data with appropriate permissions.

Ethics approval

No ethics approval is required.

Consent to participate

Not Applicable.

Consent for publication

Not Applicable.

Human and animal ethics

Not Applicable.

Code availability

Not Applicable.

References

[1] H. Thakkar and R. Lal, "An Analysis of Elliptic Curve Cryptography Secret Keys For Use In Cloud Workload Balancing And Security Provisioning," *2023 International Conference on Applied Intelligence and Sustainable Computing (ICAISC)*, Dharwad, India, 2023, pp. 1-7

[2] R. R. Dornala, S. Ponnapalli, A. R. Lakshmi and K. T. Sai, "An Advanced Cloud Security and Load Balancing in Health Care Systems," *2023 International Conference on Self Sustainable Artificial Intelligence Systems (ICSSAS)*, Erode, India, 2023, pp. 1-6

[3] M. A. Shibli, N. Ahmad, A. Kanwal and A. Ghafoor, "Secure virtual machine migration (SV2M) in cloud federation," *2014 11th International Conference on Security and Cryptography (SECRYPT)*, Vienna, Austria, 2014

[4] S. Barjatiya and P. Saripalli, "BlueShield: A Layer 2 Appliance for Enhanced Isolation and Security Hardening among Multi-tenant Cloud Workloads," *2012 IEEE Fifth International Conference on Utility* and Cloud Computing, Chicago, IL, USA, 2012, pp. 195-198

[5] Sibi Chakkaravarthy Sethuraman, Devi Priya VS, Tarun Reddi, Mulka Sai Tharun Reddy, Muhammad

Khurram Khan, "A Comprehensive Examination of Email Spoofing: Issues and Prospects for Email Security", Computers & Security, Elsevier, vol. 135, 103490, 2023

[6] L. Wang, H. V. Ramasamy, R. Mahindru and R. Harper, "Activating Protection and Exercising Recovery Against Large-Scale Outages on the Cloud," *2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshop (DSN-W)*, Toulouse, France, 2016, pp. 264-264

[7] S. Gopikrishnan, Sibi Chakkaravarthy Sethuraman, Gautam Srivastava, T Sudhakar, "CyTFS: Cyber-Twin Fog System for Delay Efficient Task Offloading in 6G Mobile Networks", IEEE Internet of Things Journal, vol. 11, no. 14, pp. 24698-24714, 2024

[8] C. P. Smith, A. Jindal, M. Chadha, M. Gerndt and S. Benedict, "FaDO: FaaS Functions and Data Orchestrator for Multiple Serverless Edge-Cloud Clusters," *2022 IEEE 6th International Conference on Fog and Edge Computing (ICFEC)*, Messina, Italy, 2022, pp. 17-25

[9] Aravinth T.M, Sibi Chakkaravarthy Sethuraman, Devi Priya VS, "mCaptcha: Replacing Captchas with Rate limiters to Improve Security and Accessibility", Communications of the ACM, Volume 67, Issue 10, pp. 70 – 80, 2024

[10] C. Gritti, M. Önen and R. Molva, "CHARIOT: Cloud-Assisted Access Control for the Internet of Things," *2018 16th Annual Conference on Privacy, Security and Trust (PST)*, Belfast, Ireland, 2018, pp. 1-6

[11] Sibi Chakkaravarthy Sethuraman, Devi Priya, Saraju P Mohanty, "Flow based containerized honey-pot approach for network traffic analysis: An empirical study", Computer Science Review, Elsevier, vol. 50, 100600, 2023

[12] G. Kornaros, D. Bakoyiannis, O. Tomoutzoglou and M. Coppola, "From Cloud to IoT Device Authenticity under Kubernetes Management," *2024 11th International Conference on Internet of Things: Systems, Management and Security (IOTSMS)*, Malmö, Sweden, 2024, pp. 218-223

[13] Devi Priya, Sibi Chakkaravarthy Sethuraman, Muhammad Khurram Khan, "Container Security: Precaution levels, Mitigation Strategies, and Research Perspectives", Computers & Security, Elsevier, vol. 135, 103490, 2023

[14] K. Gai, M. Qiu and S. A. Elnagdy, "Security-Aware Information Classifications Using Supervised Learning for Cloud-Based Cyber Risk Management in Financial Big Data," *2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS)*, New York, NY, USA, 2016, pp. 197-202

[15] Devi Priya VS, Sibi Chakkaravarthy Sethuraman, "Containerized cloud-based honeypot deception for tracking attackers", Scientific Reports, Nature, Vol. 13, Issue.1, 1437

[16] S. Berger *et al*., "Security intelligence for cloud management infrastructures," in *IBM Journal of Research and Development*, vol. 60, no. 4, pp. 11:1-11:13, July-Aug. 2016

[17] M. Gopinath, Sibi Chakkaravarthy Sethuraman, "A comprehensive survey on deep learning-based malware detection techniques", Computer Science Review, Vol. 47, 100529, Elsevier, February 2023

[18] B. D. Deebak and F. Al-Turjman, "Smart Mutual Authentication Protocol for Cloud Based Medical Healthcare Systems Using Internet of Medical Things," in *IEEE Journal on Selected Areas in Communications*, vol. 39, no. 2, pp. 346-360, Feb. 2021

[19] Sibi Chakkaravarthy Sethuraman, Aditya Mitra, Kuan-Ching Li, Anisha Ghosh, M Gopinath, Nitin Sukhija, "Loki: A Physical Security Key Compatible IoT Based Lock for Protecting Physical Assets", IEEE Access, Vol.10, 112721-112730, IEEE

[20] Q. Wang, Q. Wang, H. Zhu and X. Wang, "Enabling Collaborative Computing Sustainably Through Computational Latency-Based Pricing," in *IEEE Transactions on Sustainable Computing*, vol. 5, no. 4, pp. 541-551, 1 Oct.-Dec. 2020

[21] Dedipyaman Das, Sibi Chakkaravarthy Sethuraman, Suresh Chandra Satapathy, "A Decentralized Open Web Cryptographic Standard", Computers and Electrical Engineering, Elsevier, Volume 99, 107751, April, 2022

[22] S. Liu, L. Liu, J. Tang, B. Yu, Y. Wang and W. Shi, "Edge Computing for Autonomous Driving: Opportunities and Challenges," in *Proceedings of the IEEE*, vol. 107, no. 8, pp. 1697-1716, Aug. 2019

[23] Pranav Kompally, Sibi Chakkaravarthy Sethuraman, Steven Walczak, Samuel Johnson, Meenaloshini Vimal Cruz, "MaLang: Decentralized Deep Learning Approach to Detect Abusive Textual Content", Applied Sciences: Computing and Artificial Intelligence, 11, 8701, 2021

[24] M. Kucab, P. Boryło and P. Chołda, "Hardware-Assisted Static and Runtime Attestation for Cloud Deployments," in IEEE Transactions on Cloud Computing, vol. 11, no. 4, pp. 3750-3765, Oct.-Dec. 2023

[25] Y. Cho, Y. Kim, K. Kim, J. Kim, H. -Y. Kim and Y. Kim, "Optimizing Multi-Level Checkpointing for Distributed Deep Learning Workloads on Cloud Spot VM Clusters," in IEEE Access, vol. 12, pp. 116891-116904, 2024