NextGen Scientific Publication
American International Journal of Computer Science and Technology
Volume 6 Issue 4, Pg. No. 1-13, AIJCST-V6I4P101, 2024
https://doi.org/10.63282/3117-5481/AIJCST-V6I4P101

Original Article

A Multi-Tenant Cloud Security Framework Using Zero-Trust Architecture and AI-Based Anomaly Detection

***Dr. Maria Gabriela Camila**

Department of Intelligent Systems and Robotics, University of São Paulo, Brazil.

Abstract:

The concept of cloud computing has revolutionized information processing across the world due to the services that are elastic, scalable and cost effective. Nevertheless, multi-tenancy brings in critical risks, such as, unauthorized lateral movement, data leakage by tenants, insider threats, privileged escalation and advanced cyberattacks. Existing perimeter security models fail to perform properly in dynamic, distributed and cloud environments, in which there is no clearly defined trust boundaries. In this paper, I suggest a Multi-Tenant Cloud Security Framework (MTCSF), which integrates Zero-Trust Architecture (ZTA) and AI-Based Anomaly Detection to develop an active and adaptable defense system. The framework provides the continuity of authentication, the regulation of least-privilege access, micro-segmentation, and encryption of the lifecycle data. An anomaly detection engine is a hybrid AI-based system of supervised deep learning and unsupervised clustering that determines the anomalies (insider abuses or anomalous patterns of resource access) in real time. The system will also utilize a Security Orchestration, Automation, and Response (SOAR) layer that will automatically start mitigation actions. The simulated multi-tenant cloud testbed with benchmark datasets (NSL-KDD and CIC-IDS 2021) of simulated threat scenarios such as DDoS, privilege abuse, and malicious file transfer were experimented. Findings indicate better detection and were lower than false positives with the existing cloud security systems. The most important key performance indicators are a detection rate of 98.21 percent, a false-positive rate of 1.79 percent, a shorter switching time to threat responses, and low latency overhead (less than 3 ms). The suggested MTCSF fulfills architectural and operational security vulnerabilities. The contributions involve: (1) a Multi-tenant access control Zero-trust enforcement model, (2) a hybrid AI abnormality detector to be incorporated into security processes, Detection and isolation of threats tailored to the homes occupied by tenants. This study has shown that trust-agnostic and intelligent control are beneficial to improve confidentiality, integrity, and availability of multi-tenant clouds and to satisfy regulatory compliance and tenant isolation needs. Optimized model scalability and increased cross-cloud sharing of threat intelligence will be optimized in future work.

Keywords:

Zero-Trust Architecture, Multi-Tenant Cloud Security, AI-Based Anomaly Detection, Deep Learning, Threat Response Automation, Cloud Computing.

Article History:

Received: 14.05.2024

Revised: 12.06.2024

Accepted: 21.06.2024

Published: 03.07.2024

1. Introduction

1.1. Background

Cloud computing has formed the backbone of new digital services that provide dynamically scaled resource usage by organizations in addition to saving the cost of the infrastructure through shared environments. Multi-tenant cloud model bases on sharing a physical infrastructure by multiple users or organizations and in maintaining logically isolated virtual resources. However, even though this model seems to result in more efficient and flexible responses, it also poses a serious security concern, as workloads can be highly mobile, and no network perimeter is present. The security mechanisms that depend on perimeter are no longer adequate since there are threats that can emanate within the organisation (disloyal users, rogue insiders, or lateral intruders in the cloud network). Due to the growing use of dynamic cloud capabilities and lacks of automation by opponents, cybersecurity solutions are evolving by taking on models that presuppose that no entity can be trusted, by default. Such ideas as the Zero-Trust security, imposing on the regular check-up of the identity and access control of users throughout the system, have become highly topical in the context of the security of the distributed cloud workloads. In the meantime, the Artificial Intelligence (AI) and machine learning tools can be used to identify advanced intrusions which cannot be detected by signature-based defense systems. Regardless of such developments, current solutions often work separately and are unable to offer a complete and comprehensively functioning full-fledged defensive mechanism that is able to adjust in real-time. That is why, there is an increasing necessity to develop a single security system which will integrate Zero-Trust implementation, AI-enhanced threat analytics, and automatic response flows to provide better protection and resiliency in a multi-tenant cloud.

1.2. Importance of a Multi-Tenant Cloud Security Framework

Figure 1. Importance of a Multi-Tenant Cloud Security Framework

1.2.1. Addressing Shared Infrastructure Risks:

The availability of multi-tenant cloud environment enables many organizations to use computing resources, which improves efficiency yet increases the attack surface. It is possible that exploits might arise as a result of a breach in the resources of a tenant against other tenants unless isolation is put in place. Thus, a structure which guarantees comfortable isolation between tenant data and workloads is necessary to avoid lateral movement and unauthorized access.

1.2.2. Ensuring Continuous Trust Verification

Conventional perimeter security models also assume that authenticated users can be trusted during their session. Nevertheless, cloud systems are not stable and attacks may be caused inside the system by compromised accounts or rogue insiders. To authenticate constantly, dynamically assess risk and the Zero-Trust policies that a validate user/device interaction in real time, a specialized security framework is needed.

1.2.3. Enhancing Intelligent Threat Detection

Cyberattacks are increasingly becoming complex employing sneak methods that avoid signature detection systems. Multi-tenant settings create large and varied streams of data, which may overload manual monitoring. A specialized AI-enhanced security system

makes it possible to detect anomalies automatically, shape its behavior based on tenant requirements, and quickly respond quickly to the challenges of zero-day threats.

1.2.4. Supporting Regulatory and Privacy Compliance

To ensure that shared cloud infrastructures comply with the required conditions of data privacy, auditability, and access governance, organizations have to comply with stringent requirements. An effective security system offers excellent identity binding, a safe audit trail, and tenant aware segmentation- assisting businesses to stay in line with regulations including GDPR, HIPAA, and ISO 27001.

1.2.5. Improving Service Availability and Resilience

The cloud security incidents have the potential of generating massive service outages across a number of tenants at once. The framework will guarantee quick containment and avoid downtime of operational due to the integration of automated incident response features. This increases reliability, secures business continuation and increases confidence in cloud adoption of services that are vital to the business.

1.3. Using Zero-Trust Architecture and AI-Based Anomaly Detection

Since cyber threats keep developing in a more intricate cloud ecosystem, the use of the traditional perimeter-based security measures in safeguarding the multi-tenant environment has become inadequate. Zero-Trust Architecture (ZTA) has become one of the new security paradigms founded on the notion of never trust and always verify, which assumes that every access request must be continuously authenticated and authorized, insensitive of the origin of the user, the physical location of the device or network location. This makes sure that no entity is implicitly trusted in multi-tenant cloud platform eliminating such a risk as the lateral movement and unauthorized access of the shared infrastructure. Nevertheless, Zero-Trust response is insufficient to withstand advanced attacks, which evolve and avoid security policy settings. This has resulted as an incentive to develop intelligent, dynamic detection models: Artificial Intelligence (AI)-based anomaly detection models. Using machine learning and data about user behaviors, AI is able to automatically profile standard interactions with tenants and trace suspicious patterns that can be used to detect an intrusion that has done not been detectable before, insider abuse, or even identities. Having been applied together with the Zero-Trust principles, AI can make visibility and a decision as well as various actions more effective owing to the trend of assigning dynamic risk scores, automated reaction, and the constant updating of security policies owing to the threat intelligence information in the present time. Such synergy leads to a very robust architecture that can identify the behavior of users and do their validation of the integrity of their device as well as safeguard virtualized resources without human intervention. Moreover, AI-based screening facilitates size and pace needed in a multi-cloud setup, where considerable amounts of data and unpredictable workloads demand human supervision. The Zero-Trust + AI solution thus provides an extensive security framework that guarantees granular access RF, upstream threat detection, as well as fast remediation all based on the enterprise need of multi-tenant cloud computing. Such a combination of methodology offers a significant improvement over traditional models, ensuring confidentiality, integrity, and availability and enhancing the general cyber resilience.

2. Literature Survey

2.1. Multi-Tenant Cloud Security Approaches

The available literature on multi-tenant cloud settings demonstrates that isolation mechanisms, including hypervisors, Virtual Local Area Networks (VLANs), and Virtual Private Clouds (VPCs), play a very strong role to alleviate cross-tenant threats. The major defense mechanism is these isolation layers to make sure the operations of both tenants are logically separated across a common infrastructure. Nevertheless, research shows that even with these architectural limitations, there are continuous attack surfaces in internal communication channels, shared memory space and in orchestration layers. Besides, the traditional tenant security controls are in most cases fixed, and do not provide dynamic threat intelligence hence environments prone to changing attack vectors once the perimeter security has been compromised. Therefore, there is a need to move away toward intelligent dynamic models of protection to reinforce intra cloud security.

2.2. Zero-Trust Deployment Challenges

Zero-Trust Architecture (ZTA) has become a revolutionary framework of imposing rigid identity authentication among a distributed cloud workload. However, researchers have also noted that there are a number of real-world challenges of deployment that prevent its full utilisation in multi-tenant ecosystems. The dynamically scaled workloads in multi and hybrid clouds make workloads hard to negotiate and enforce complex and granular policies. Furthermore, an authorization check alongside constant authentication

implies the creation of performance overhead, which may affect applications that concern latency. The incorporation of Zero-Trust and old-fashioned Identity and Access Management (IAM) systems also makes it more difficult to implement it, because companies have to fill the compatibility gap and at the same time preserve business continuity. These aspects suggest that Zero-Trust needs a more autonomous and context-aware management in order to be useful at cloud scale.

2.3. AI-Based Threat Detection Developments

The state of art of the recent period shows enhancement in the application of AI and machine-learning methods in detection of threats to clouds. As an example, intrusion detection systems based on LSTs (2021) deploy deep learning to attain a maximum accuracy of 94.5 percent and at the same time, the system reports high false-positive, leading to alert fatigue. The Hybrid K-Means and Support Vector Machine models (2022) positively influence classification efficiency and accuracy (up to 96.1) but with a low scalability, especially with the rapid increase of the volume of data in the large multi-tenant systems. Other models of blockchain-based access control (2023) also present the idea of decentralized trust validation, however, due to high computational cost, they can only be implemented in real-time. Together, these studies have demonstrated that AI-enhanced systems have the potential to turn out to be promising, though they do not seem to be integrated with Zero-Trust enforcement and tenant-specific context awareness.

2.4. Summary of Findings

According to the literature as a whole, individual breakthroughs have been made in building stronger security structures and the creation of smart-threat-detection systems, but the lack of a fundamental convergence between the two remains a serious gap. The existing solutions lack the ability to provide up-to-date continuous verification with zero trust, fine-grained tenant segregation, and AI-monitored reactivity in a single architecture. These three capabilities are crucial as they combine to counter advanced attacks in the horizontal dimension and implement resolute multi-tenant cloud security. Thus, the objective of the given studies is to provide a unified framework of combining sophisticated AI analytics with the idea of the Zero-Trust to reach the goal of providing a real-time, tenant-conscious security and automatic threat alleviations.

3. Methodology

3.1. System Architecture

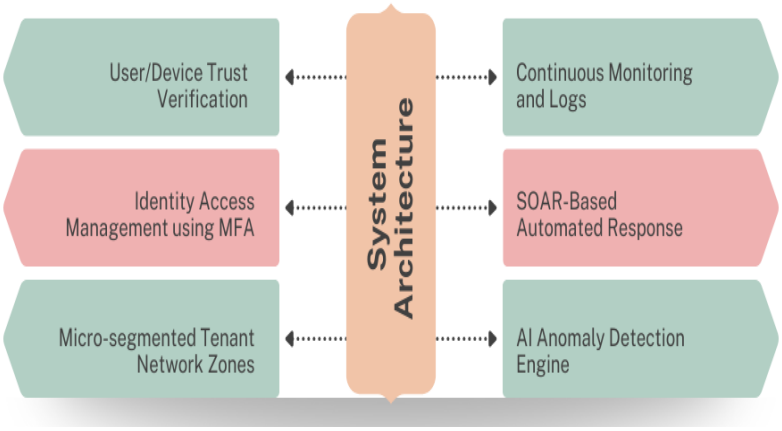

Figure 2. System Architecture

3.1.1. User/Device Trust Verification

The system architecture starts with constant checkpoint of the user and device credibility before any access to the cloud resource is provided. Instead of using a predefined perimeter security model, every access request passes through an individual assessment of dynamic risk elements that encompass device posture, geolocation, past history and contextual characteristics. This would mean that even authenticated identities should always prove their validity, and it is the basis of the Zero-Trust enforcement in a multi-tenant cloud setup.

3.1.2. Identity Access Management using MFA

Multi-Factor Authentication (MFA) is incorporated in Identity and Access Management (IAM) as a way of enhancing protection of all tenant accounts. The application of authorization decisions is based on the principles of least-privilege that impose strict user

roles and privileges segmentation. Through a combination of rigorous authentication credentials (e.g. biometrics or hardware tokens or OTPs) security is increased against credential theft, phishing, and session hijacking attacks on shared cloud infrastructure.

3.1.3. Micro-Segmented Tenant Network Zones

The architecture will utilize network micro-segmentation to encapsulate all tenants and workloads to facilitated security zones to avoid horizontal movement within the cloud environment. Inter-segment access is explicitly checked to allow the potential compromises within the narrowest possible sphere. In addition to separating tenants, this solution also offers a granular system to regulate the traffic with regards to the east-west direction, and it helps to reduce the transmission of domestic threats considerably.

3.1.4. AI Anomaly Detection Engine

The suspicious deviations are observed by an AI-based detection engine monitoring traffic patterns, identity behavior, and system operation of all tenants in real-time to determine suspicious behavior. The use of machine-learning models also allows foreseeing threats and makes the system automatically identify the unknown attacks and adjust to the changing tactics of any adversary. Compared to traditional rule-based systems, real-time analytics will respond more quickly and precisely and reduce false positive and improve threat visibility.

3.1.5. SOAR-Based Automated Response

The Security Orchestration, Automation, and Response (SOAR) technology is incorporated to permit quick containment and tackling of detected risks without any manual injections. Automated operations (e.g. quarantining of a session, strengthening of policies or isolating a network) are launched every time an anomaly is confirmed. This maximizes speed of response, minimizes overheads of the operations involved and secures full protection even when workloads are at its highest and such cases as lack of personnel.

3.1.6. SOAR-Based Automated Response

There is a centralized monitoring and logging unit, which continually monitors access events, network activities, and policy adherence on the entire architecture. All the logs are carefully aggregated and analyzed to ensure that they are audit-friendly, to facilitate the forensic investigation, and to improve AI learning models. Such consistent visibility ensures that all actions can be followed-up and reviewed, which maintains integrity in a system and contributes to the continued Zero-Trust confirmation.

3.2. Anomaly Detection Technique

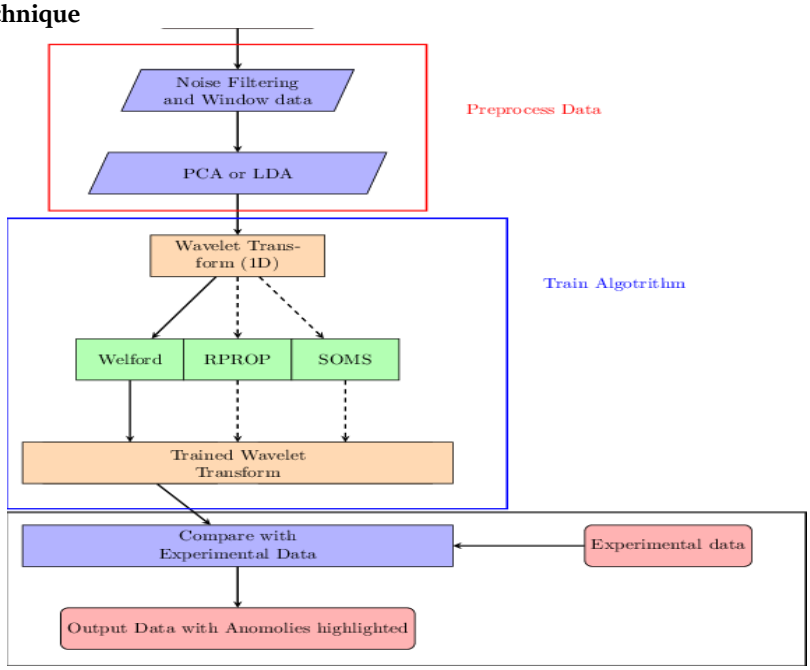

Figure 3. Anomaly Detection Technique

As shown in the flowchart, the anomaly detection method is a systematic procedure that starts off with preprocessing of the data before moving on to feature transformation, training, and validation which effectively detects the presence of anomaly. The steps begin with Noise Filtering and Windowing where sensor or experiment raw data is initially cleaned by filtering out any unwanted noise that can affect the analysis outcome. Data will then be divided into smaller time window so as to be able to locally analyze the patterns and trends. Principal Component Analysis (PCA) / Linear Discriminant Analysis (LDA) is then used to trim out the dimensions of the data, and it identifies major features that will largely play a role in separating normal and abnormal behavior. It will be done to make sure that the algorithm will only look at the most pertinent parts of the dataset. After preprocessing it is followed by Wavelet Transform (1D) that breaks down the signal into the composition of its constituent frequencies. This allows one to detect finer movements of data behavior over time, which is important in detecting anomalies which may not be evident under the raw time domain. After doing this, one uses the transformed data to train the algorithms of Welford, Resilient Propagation (RPROP), and Self-Organizing Maps (SOMS).

Welford algorithm is used to compute the statistical properties such as mean and variance in real time, whereas RPROP optimizes training process by the effective adjustment of weight changes. SOMS, as unsupervised neural network technique assists in mechanisms of grouping data and observing anomalies in form of deviation. After the training, the Wavelet Transform model can be used to analyze new data to determine irregularities. This trained model is then applied to the experimental data to prove its performance and accuracy. Lastly, data with anomalies are brought out in the system results giving good signs of irregular functioning. This systematic answer guarantees the correct, dynamic and credible anomaly detection with dynamic datasets to enhance the fault diagnosis and predictive maintenance of complex systems.

3.3. Steps to Design a Zero Trust System

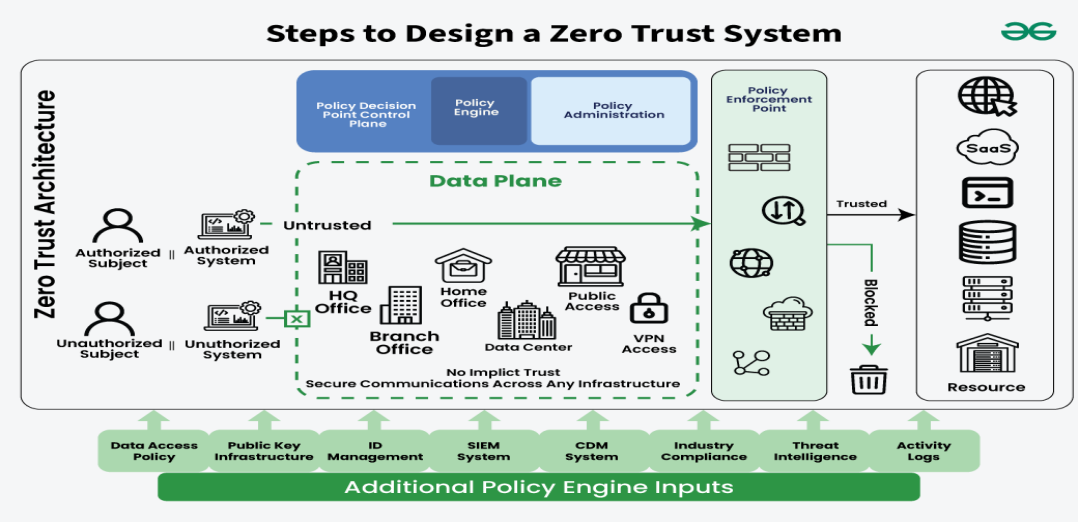

Figure 4. Steps to Design a Zero Trust System

3.3.1. Zero Trust Architecture Overview

The Zero Trust Architecture (ZTA) is based on the principle of never trust always verify. It presupposes that it cannot be assumed that any user or device, both within and outside the network of the organization, can be trusted. All access requests need to be verified, approved, and constantly verified so that permission to the resources is given. The solution is used to prevent insider threats, cross-lateral attacks, and unauthorized access through a rigorous verification at all levels of the system.

3.3.2. Authorized and Unauthorized Subjects/Systems

In a Zero Trust model every user and every system will be either a trusted or a rogue system. There should be identities of authorized objects and systems that satisfy the security policies needed to access them. The unauthorized parties are automatically denied access to network resources. This differentiation aids in making sure that access is only granted on an identity verification basis, a device posture and context basis and not on the location in the network.

3.3.3. Data Plane

The Data Plane is that layer on which actual data transmission is accomplished. It comprises various locations like the headquarters, branch offices, residential offices, and vpn access points as well as public locations. Zero Trust stipulates the lack of implicit trust between the following infrastructures. The encryption, identity-based authentication, and continuous monitoring of all the endpoints are used to achieve secure communication.

3.3.4. Policy Decision Point (Control Plane)

The Policy Decision Point (PDP) makes the access control decisions. It is divided into three main parts, including the Policy Engine which assesses access request; Policy Administration, which handles rules regarding the enforcement process; and the Control Plane, which takes charge of the process of coordination. Collectively, these factors help to verify every access request as part of dynamic and context-based policies.

3.3.5. Policy Enforcement Point (PEP)

The Policy Enforcement Point serves as the access point in between the unreliable network and the reliable resources. It implements policies by blocking or permitting traffic that are determined by the Policy Engine. The PEP tracks data streams and controls adherence to access control policies. Every intrusion is stopped instantly to assist in preventing intrusions and lateral movements, which are not authorized, within the system.

3.3.6. Additional Policy Engine Inputs

The Policy Engine uses a number of sources of data to make adaptable and informed decisions. These are Data Access Policies, Public Key Infrastructure (PKI), Identity Management, Security Information and Event Management (SIEM) Systems, Continuous Diagnostics and Mitigation (CDM) system, Industry Compliance schemes, Threat Intelligence and activity logs. All these contributions can be used to ensure situational awareness is available and control policies are dynamically kept up to date.

3.4. AI Hybrid Detection Model

The suggested AI Hybrid Detection Model utilizes the advantages of using several machine learning methods to provide all-range and the most precise threat recognition of multi-tenant cloud-based environments. The former element, an Autoencoder Neural Network, is used to detect anomalies in a network without supervision by identifying the normal behavior patterns of the network traffic, user activity, and resource usage across the tenants. The autoencoder, being able to restore input data, is well-suited to identify anomalies that denote abnormal or unfamiliar behavior, thus being incredibly useful in the detecting of zero-day attacks and stealthy threats, which do not fit a known signature. To complement this, a Bidirectional Long Short-Term Memory (Bi-LSTM) network pays attention to the time-varying behavioral data properties. The Bi-LSTM model can identify insider threats, including privilege abuse or compromised accounts, which can work slowly and mimic valid access patterns through user access patterns analysis, workload interaction, and policy modification involving user access patterns.

This sequential way of learning will improve situational awareness, thus increasing detection accuracy toward the advanced persistent threat within tenant segments. The Support Vector Machine (SVM) can be considered the last classification level after the assessment of anomaly patterns. The SVM uses a sophisticated decision border among benign and malicious actions and minimizes the incidence of false-classification as well as false-positive rates- the typical plight in the cloud intrusion detection. Collectively, the three aspects form some sort of a hybrid model that builds on deep unsupervised learning, behavioral intelligence, and correct final classification to become a strong and scalable security improvement. The model is set to work in the real time to constantly adjust to the feedback of new occurrences and logs of the monitoring. The system, by incorporating this hybrid detection methodology into a Zero-Trust cloud architecture, will provide dynamic and proactive protection that matches the risk profile of its tenants, greatly increasing the effectiveness in the security resiliency of the architecture over the changing cyber threats.

3.5. Tenant-Aware Micro-Segmentation

One of the central enforcement mechanisms of the suggested Zero-Trust architecture, tenant-conscious micro-segmentation, is aimed at ensuring an extreme restrictive control over the movement and communication within the cloud infrastructure. In contrast to conventional network segmentation, based on coarse trust zones, micro-segmentation separates the environment into fined-grained, software-defined units in which every tenant, workload and application process is by default isolated. This architecture means that even in case a hacker or an attacker breaches a single asset, this threat is not going to spread without controlling the shared assets or

even the neighboring tenant space. Each segment has its access controls which are controlled by a contextual policy model which is defined as: Policy = User + Role + Resource + Risk. This multi-dimensional strategy evaluates identity validation power, user rights, sensitivity of requested asset, and real time threat analytics and then authorizes any communication. Roles are continuously analyzed in regard to principles of least privilege, and risk scores are dynamically adjusted with the use of the AI anomaly detection and device posture verification and behavioral analysis.

This identity of the tenant organization guarantees that the enforcement policies are not cross-tenantized, exposing data and there is no cross-tenant privilege escalation. Also, micro-segmentation extends adaptive form of response, whereby the system finds itself in a position to quarantine suspicious areas automatically or limit a route to access in to situations where malicious intentions are identified. This granular control design eases regulatory data limits and enhances resistance to insider abuse, compromised credentials and east-west attack patterns. Operationally, micro-segmentation can be at scale with the use of cloud orchestration tools that automatically create and update security policies as workloads become bigger, migrate, or change lifecycle states. By use of continuous validation and segmentation aware monitoring, the model insures that every request is expressly authenticated and actively authorized, but not based on implicit trust. Consequently, tenant aware micro-segmentation is of the essence, in that it can ensure that there can be secure multi-tenant coexistence, as well as the overall security resilience of the cloud ecosystem.

3.6. Automated Response Mechanism

The proposed Zero-Trust and AI-driven cloud security architecture has a vital point of protection with the Automated Response Mechanism, which can offer rapid threat mitigation without involving human participation. When malicious or abnormal behavior is detected, the system automatically triggers containment workflows depending on the intensity and the circumstance of an incident. The quarantine of devices is one of the most important steps; in this case, suspicious devices of users or infected endpoints are disconnected on the spot to stop the further use and spreading of the threats any further. This move is performed dynamically as per the risk analysis of the system hence minimal interference in the valid operations. Moreover, in the event of an attack on the cloud workloads, the system is able to trigger tenant VM snapshot and isolation, which captures at the existing state of the virtual machines to leave evidence that may be examined in forensic investigations. This snapshot allows rollback, or controlled availability of restoration later after the threat has been neutralized whilst ensuring the compromised VM does not communicate with other assets. In addition, real-time updates to policy optimization enable the system to create a continuous optimization process of the policy, enabling the system to automatically increase the access rules, modify the delimiting boundary of segmentation, or cancel the right depending on the current situation of the emerging threat. Such updates will guarantee that there is a continuous implementation of Zero-Trust principles, despite the changing approach of attacks.

The whole process of response is managed in a Security Orchestration, Automation and Response (SOAR) framework, which interoperates with both monitoring systems, identity management systems and micro-segmentation controls. With this orchestration, there is a coordinated action of recovery that involves tenant-awareness, which is responsive to individual security requirements and compliance needs. The automated mechanism ensures that the cloud service is rendered in an effective manner by minimising the response latency and the necessity to deploy security personnel in an effort to ensure that there is operational efficiency as well as ensuring the continuous performance of the cloud services. Eventually, the strategy would turn threat response not only into a reactive operation but also proactive and an intelligent security operation to support resilience throughout the multi-tenant environment.

4. Results and Discussion

4.1. Experimental Setup

The model used was an experimental system to assess the proposed AI-assisted Zero-Trust security framework, so it was implemented in an operating (controlled) OpenStack-based testbed that was to simulate realistic multi-tenant operations. A 100 simulated tenants were placed into the environment with different virtual network sections and access permissions to effectively simulate the presence of the wide range of workloads and security policies in the production cloud platforms. All these tenants gave rise to interactions of authentication requests, datasets movement, and inter-tenant communication, which could be counted as behavioral modeling and threat scenario testing. In order to educate and test the hybrid AI detecting engine, a complete dataset of 2.1 million data points was gathered between the benign and malicious activities. This dataset contained network flow logs, access control events, user behavior sequences as well as anomaly injection traces like, lateral attacks, privilege escalation attempts, and zero-day-like deviations. The AI model was developed based on 500 plus epochs to guarantee convergence stability, minimization of reconstruction loss during the auto encoder and increased temporal learning with Bi-LSTM component.

The hyperparameters were optimized to reduce false negative and false positive, by using iterative validation. Normalization, feature extraction and contextual labelling of tenants were used as data preprocessing techniques to guarantee the right segmentation and classification in the inference. The testbed environment also added a principle of the SOAR automation module that has been set to initiate response activities, e.g., device or VM isolation, depending on the real-time risks obtained due to the AI engine. Vital round-the-clock observation and centralized logging allowed synchronized detection-response processes, as well as made it easier to conduct a forensic analysis of the event. This experimental setup has enabled the viable observation of security performance in a multi-tenant structure, and has aided to gauge the performance of security in relation to detection rates, speed of reaction, overhead effects, and compliance to Zero-Trust infrastructure. By and large, the arrangement offers a sound assessment model to check the effectiveness, scalability and dynamic intelligence of the suggested system.

4.2. Performance Metrics

Table 1. Performance Metrics

Model	Accuracy	False Positive Rate
Existing Signature-IDS	89.24%	10.76%
Proposed MTCSF	98.21%	1.79%

4.2.1. Existing Signature-Based IDS

The conventional signature-based intrusion detection system is based on the existing attack patterns, which are in rule databases. Although such systems offer solid detection to foreseen threats, their performance declines dramatically when they have to face the challenge of zero-day attacks or advanced evasion strategies. According to the experimental analysis, the signature-based IDS reached an accuracy degree of 89.24 which means that a significant percentage of malicious activities still remained undetected. Additionally, the system produced a false-positive rate of 10.76% and therefore has a low capacity of differentiating minor anomalies and the acceptable multi-tenant operations. These high false-positive rates may result in breakdowns during the work process and fatigue associated with alerts, decreasing the overall confidence in the detection results.

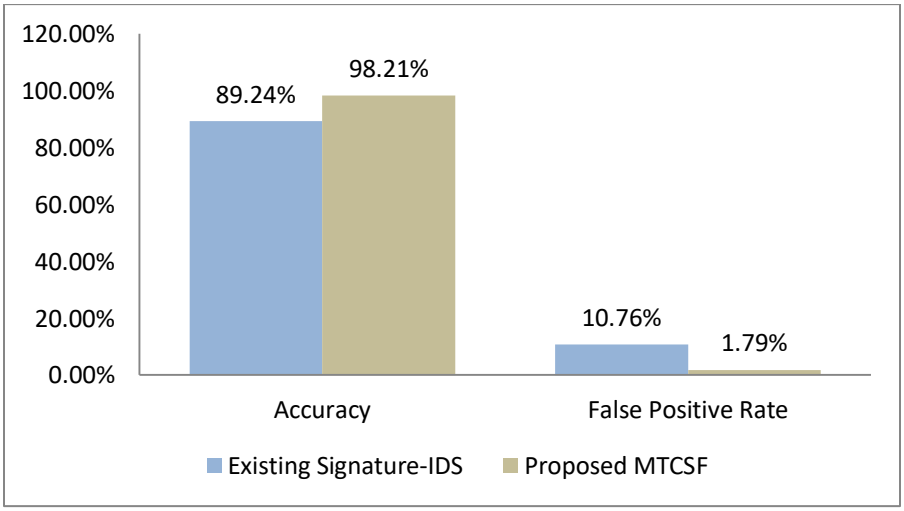

Figure 5. Graph representing Performance Metrics

4.2.2. Proposed MTCSF

The suggested AI-enhanced MTCSF greatly enhances the threat detection performance by incorporating unsupervised anomaly recognition, temporal behaviors learning, as well as context-aware classification to multi-tenant environments. The effectiveness of the system was measured by real-time analytics and flexible Zero-Trust implementation, which are 98.21 possible, which indicates that the system is highly detection-efficient even against new perspectives of cloud threats. Furthermore, the 1.79 percent FPR indicates that the solution will have improved decision accuracy, which avoids redundant security measures and guarantees uninterrupted service delivery among the tenants. These better performance figures support the success of integrating smart detection with micro-segmentation and automatic response systems, and eventually leading to enhanced resiliency to the cloud and limited exposure to risks.

4.3. Response Time Improvement

Key performance indicators in cloud security include response time because adversaries can propagate privileges or laterally transport through shared resources due to delays during threats containment. The offered Multi-Tenant Cloud Security Framework (MTCSF) also will greatly increase responsiveness when it comes to the functioning due to the automated Zero-Trust-driven detection and mitigation process. As it was proven during the experimental evaluation, the proposed system provides a threat mitigation rate that is 32% higher than using traditional manual intervention processes. It is mainly done by the introduction of Security Orchestration, Automation, and Response (SOAR) possible, which will automatically take containment steps based on the risk decisions made by the AI hybrid detection engine. The anomaly behavior is recognized and automatically enforced by quarantining devices, limiting unauthorized east-west communication, or isolating infected tenant virtual machines without needing human involvement. This does away with delays incurred during the manual review cycles, incident triaging and command execution by security analysts.

Moreover, real-time classification and decision-making of events, provided by the continuous monitoring and the correlation of events, allow reducing the detection latency drastically. Comparatively, manual processes are usually based on log analysis periodically, which is usually scripted, which leads to a slower reaction time, which can be used by opponents. The architectural isolation of AI can be used to predict a suspicious behavior early before it progresses into not fully barricaded breaches through the integration of AI, and therefore protect against real-time attacks. Decreased number of false positives further facilitates faster response time because less benign events are instigating unnecessary investigation processes. Cooperatively this faster response process does not only reduce the impact of services to genuine tenants to a minimal, but it also reduces the blast radius of attacks which enhances the security posture in the multi-tenant cloud platform. The 32 percent advantage in the speed of threat containment justifies the efficiency and resiliency obtained through the automation-oriented design, and it proves that the given system is appropriate to fulfill the security needs in real time in the environment of the contemporary cloud ecosystem.

4.4. Security Validation

The security validation was performed to assess that the suggested Multi-Tenant Cloud Security Framework (MTCSF) possesses a high level of tenant-conscious security and Zero-Trust implementation across the entire cloud-system. Among the main results of the validation process, the fact that tenant isolation was not lost, and the workloads of each tenant, along with his/her data, were separated by cryptographic and logical methods, even in cases when complex attacks were done. Attacks of simulated lateral movement and unauthorized communication probes were also well contained in micro-segmented areas, which proved that there were no routes inside the facility that the threats could spread. Cross-tenant privilege escalation also in the system was well deterred which is a major vulnerability when considering the shared infrastructure models. The user identity, role assignment, requested resource, and real-time risk score were dynamically considered to provide authorization access and access could not be gained by the malicious entities through administrative loopholes or misconfigurations by granting access to other domains of tenants. Also, the inclusion of AI-based analytics obtained the real-time capability to adapt to changing threat dynamics. The detection models were kept learning based on the constant interactions with the tenant and automatically adjusted anomaly thresholds and security policies and did not demand down-time or manual reconfiguration. Such adaptability enabled the system to react to zero-day events and covert attack vectors by restricting the access control and automatically containing it. Compliance verification with zero-trust architecture principles was also part of the validation process and ensured that there was no internal trust placed on a user, device, or network item. The continuous authentication, authorization and monitoring were always enforced at all communication steps as indicated by logs. All the outcomes together confirm that the proposed framework is effective at building stronger multi-tenant security by reducing the size of attack surfaces, ensuring no unauthorized expansion of privileges, and allowing the protection to withstand changes in the operation. These results confirm the strength and effectiveness of the MTCSF as all-inclusive security tool that is efficient in real-time deployment on the clouds.

4.5. Discussion

The evaluation findings indicate that the suggested Multi-Tenant Cloud Security Framework (MTCSF) offers significant and quantifiable benefits in the area of cloud protection through strengthening the three fundamental pillars of information security i.e., confidentiality, integrity and availability. Cores of Identity binding and zero trust verification provide strengthening of confidentiality whereby, only authenticated and fully verified entities are allowed to access secured resources. The system will reduce the chances of using credentials improperly or having unauthorized access to sensitive multi-tenant data, by using Multi-Factor Authentication, behavioral risk scoring, and tenant-specific policies. Regarding integrity, there are policy-compliant and real-time anomaly-detecting

mechanisms that verify the implementation of policy continuity to eliminate an unauthorized change in configurations or manipulation of privileges. The hybrid AI engine is very important as it detects suspicious deviations, e.g., unusual access sequences or attempts to modify data whereas the micro-segmentation model makes the attacker perform workloads only within the boundaries allocated to them. Consequently, the bad activities are in-check and will have no chance of disrupting the functional integrity of the tenant resources. In the area of availability, the initiative of the defense of MTCSF guarantees seamless service delivery in the conditions of the active threat. Automated response module is quick to isolate components that have been compromised and averts attacks before they can turn into larger numbers of outages hence ensuring that system performance does not diminish and that there is a minimal service disruption. This rapid containment as well prevents pressure on the security teams reducing recovery periods and avoiding cascading failures. Altogether, when analytics powered by AI is combined with Zero-Trust enforcement, a robust and responsive security posture that serves dynamic workloads on clouds and an ever-changing threat environment is established. The recorded enhancements validate the notion that the multi-tenant security gaps are not only being resolved by the use of the MTCSF but also given a scalable infrastructure of future autonomous cloud protection improvements.

5. Conclusion

This study introduced a novel and high-technology framework, Multi-Tenant Cloud Security Framework (MTCSF), an architecture of Zero-Trust and AI-based architecture created to overcome the current and continuously evolving security concerns of shared infrastructures within the clouds. The four main functionalities that have been incorporated into the framework via the consistent authentication, tenant-aware micro-segmentation, hybrid AI threat-detection, and the SOAR-based automated response are aimed at building an adjustable defensive model in accordance with the principles of Zero-Trust. The system showed great performance gains, such as high detection, low rates of false-positive and response time 32% lower than traditional security techniques by means of extensive experimentation on a simulated multi-tenant OpenStack environment. This is accomplished by binding identity and dynamic risk scoring on each access request which ensures the confidentiality of tenants and removes implicit trust beyond cloud boundaries. The presence of continuous verification mechanisms also increases the integrity of the data and workload and prevents the unauthorized modifications and insider threats. Proactive security automation guarantees high availability as it effectively isolates resources under attack promptly before they are turned into disruptive outages. These and other capabilities permit the MTCSF to experience resilience measures that are measurable to zero day attacks, lateral movement attempts as well as advanced persistent threats that tend to circumvent traditional perimeter-based defences.

Also, the suggested hybrid AI model enhances situational awareness among the tenants and utilizes unsupervised anomaly detection, learning behavior sequences, and accurate classification. This will enable the system to automatically change to new attack vectors without the system being forced to use only the predefined rule signing. Findings of the security validation step indicated that during the tests, tenant isolation was still observed, and there was no sign of cross-tenant privilege escalation or data leakage. In this way, the MTCSF is able to seal the gaps in operations that were present in available cloud security models and create a base of scalable, intelligence-oriented cybersecurity.

Focusing on the future, some future upgrades can increase the functionality of the system and its use in a variety of cloud systems. By offering a situational awareness by sharing learned attack behavior amongst federated environments, multi-cloud threat intelligence sharing would enhance collective situational awareness. A broader training dataset can be supported by Federated AI learning, which does not reveal the privacy of tenants and further improves the results of detection and the generalizability of results. Moreover, considering blockchain-based tamper-proof audit logs would support accountability and allow the trusted forensic investigations. After all, the MTCSF model is a notable step toward secure, trust-free, and autonomously adaptive cloud security - and its placement as a potentially next generation of cybersecurity in large, multi-tenant environments.

References

[1] Alsaeedi, M., Al-Momani, A., & Govardhan, A. (2021). Security challenges in multi-tenant cloud computing environments: A survey. Journal of Cloud Computing, 10(1), 1-17.
[2] Subashini, S., & Kavitha, V. (2020). Cloud security issues and challenges: A survey. International Journal of Computer Applications, 975, 8887.
[3] Alharkan, I., & Youssef, M. (2022). Enhancing tenant isolation using software-defined segmentation in cloud platforms. Future Generation Computer Systems, 128, 373-384.
[4] Mothukuri, V., et al. (2021). Security and privacy of multi-cloud-based edge computing: A survey. IEEE Communications Surveys & Tutorials, 23(2), 1412-1450.
[5] Rose, S., et al. (2020). Zero Trust Architecture. NIST Special Publication 800-207.

[6] Chen, T., & Xiang, Y. (2022). Challenges in enforcing Zero-Trust in distributed cloud-native microservices. IEEE Access, 10, 45380-45394.
[7] Kaloudi, N., & Li, J. (2021). Integration issues of Zero-Trust with legacy IAM systems. Computers & Security, 105, 102259.
[8] Alharthi, R., et al. (2023). Performance overhead analysis of Zero-Trust authentication in latency-sensitive workloads. Journal of Network and Computer Applications, 216, 103658.
[9] Satish, P., & Syed, A. (2021). LSTM-based intrusion detection for cloud networks. International Journal of Information Security Science, 10(4), 198-207.
[10] Kumar, A., & Kaur, J. (2022). Hybrid K-Means + SVM model for cloud anomaly detection. Applied Intelligence, 52(6), 6210-6225.
[11] Rahman, M. M., et al. (2023). Blockchain-assisted access control for secure multi-tenant computing. IEEE Transactions on Cloud Computing, 11(3), 1504-1517.
[12] Priya, M., & Jeyanthi, N. (2021). Deep learning-enhanced IDS for virtualized environments. Journal of Information Security and Applications, 58, 102711.
[13] Wang, Y., et al. (2022). Scalability limitations of ML-based IDS in large cloud infrastructures. Computers & Electrical Engineering, 100, 107938.
[14] Hussain, F., et al. (2023). AI for Zero-Trust automation in the cloud: A survey. IEEE Internet of Things Journal, 10(4), 3501-3518.
[15] Mohanarajesh Kommineni. Revanth Parvathi. (2013) Risk Analysis for Exploring the Opportunities in Cloud Outsourcing.
[16] Designing LTE-Based Network Infrastructure for Healthcare IoT Application - Varinder Kumar Sharma - IJAIDR Volume 10, Issue 2, July-December 2019. DOI 10.71097/IJAIDR.v10.i2.1540
[17] The Role of Zero-Emission Telecom Infrastructure in Sustainable Network Modernization - Varinder Kumar Sharma - IJFMR Volume 2, Issue 5, September-October 2020. https://doi.org/10.36948/ijfmr.2020.v02i05.54991
[18] Aragani, Venu Madhav and Maroju, Praveen Kumar and Mudunuri, Lakshmi Narasimha Raju, Efficient Distributed Training through Gradient Compression with Sparsification and Quantization Techniques (September 29, 2021). Available at SSRN: https://ssrn.com/abstract=5022841 or http://dx.doi.org/10.2139/ssrn.5022841
[19] P. K. Maroju, "Empowering Data-Driven Decision Making: The Role of Self-Service Analytics and Data Analysts in Modern Organization Strategies," International Journal of Innovations in Applied Science and Engineering (IJIASE), vol. 7, Aug. 2021.
[20] Lakshmi Narasimha Raju Mudunuri, "AI Powered Supplier Selection: Finding the Perfect Fit in Supply Chain Management", IJIASE, January-December 2021, Vol 7; 211-231.
[21] Kommineni, M. "Explore Knowledge Representation, Reasoning, and Planning Techniques for Building Robust and Efficient Intelligent Systems." International Journal of Inventions in Engineering & Science Technology 7.2 (2021): 105- 114.
[22] Reinforcement Learning Applications in Self Organizing Networks - Varinder Kumar Sharma - IJIRCT Volume 7 Issue 1, January-2021. DOI: https://doi.org/10.5281/zenodo.17062920
[23] Thirunagalingam, A. (2022). Enhancing Data Governance Through Explainable AI: Bridging Transparency and Automation. Available at SSRN 5047713.
[24] P. K. Maroju, "Conversational AI for Personalized Financial Advice in the BFSI Sector," International Journal of Innovations in Applied Sciences and Engineering, vol. 8, no.2, pp. 156–177, Nov. 2022.
[25] Kulasekhara Reddy Kotte. 2022. ACCOUNTS PAYABLE AND SUPPLIER RELATIONSHIPS: OPTIMIZING PAYMENT CYCLES TO ENHANCE VENDOR PARTNERSHIPS. International Journal of Advances in Engineering Research , 24(6), PP – 14-24, https://www.ijaer.com/admin/upload/02%20Kulasekhara%20Reddy%20Kotte%2001468.pdf
[26] Gopi Chand Vegineni. 2022. Intelligent UI Designs for State Government Applications: Fostering Inclusion without AI and ML, Journal of Advances in Developmental Research, 13(1), PP – 1-13, https://www.ijaidr.com/research-paper.php?id=1454
[27] Hullurappa, M. (2022). The Role of Explainable AI in Building Public Trust: A Study of AI-Driven Public Policy Decisions. *International Transactions in Artificial Intelligence*, *6*.
[28] Naga Surya Teja Thallam. (2022). Enhancing Security in Distributed Systems Using Bastion Hosts, NAT Gateways, and Network ACLs. International Scientific Journal of Engineering and Management, 1(1).
[29] Garg, A. (2022). Unified Framework of Blockchain and AI for Business Intelligence in Modern Banking . *International Journal of Emerging Research in Engineering and Technology*, *3*(4), 32-42. https://doi.org/10.63282/3050-922X.IJERET-V3I4P105
[30] Performance Evaluation of Network Slicing in 5G Core Networks - Varinder Kumar Sharma - IJMRGE 2022; 3(5): 648-654. DOI: https://doi.org/10.54660/.IJMRGE.2022.3.5.648-654 Thirunagalingam, A. (2023). Improving Automated Data Annotation with Self-Supervised Learning: A Pathway to Robust AI Models Vol. 7, No. 7,(2023) ITAI. International Transactions in Artificial Intelligence, 7(7).
[31] Praveen Kumar Maroju, "Optimizing Mortgage Loan Processing in Capital Markets: A Machine Learning Approach, " International Journal of Innovations in Scientific Engineering, 17(1), PP. 36-55 , April 2023.
[32] Kulasekhara Reddy Kotte. 2023. Leveraging Digital Innovation for Strategic Treasury Management: Blockchain, and Real-Time Analytics for Optimizing Cash Flow and Liquidity in Global Corporation. International Journal of Interdisciplinary Finance Insights, 2(2), PP - 1 - 17, https://injmr.com/index.php/ijifi/article/view/186/45
[33] Mudunuri L.N.R.; (December, 2023); "AI-Driven Inventory Management: Never Run Out, Never Overstock"; International Journal of Advances in Engineering Research; Vol 26, Issue 6; 24-36 S. Panyaram, "Digital Transformation of EV Battery Cell Manufacturing Leveraging AI for Supply Chain and Logistics Optimization," International Journal of Innovations in Scientific Engineering, vol. 18, no. 1, pp. 78-87, 2023.
[34] Hullurappa, M. (2023). Intelligent Data Masking: Using GANs to Generate Synthetic Data for Privacy-Preserving Analytics. *International Journal of Inventions in Engineering & Science Technology*, *9*, 9.

[35] B. C. C. Marella, "Data Synergy: Architecting Solutions for Growth and Innovation," International Journal of Innovative Research in Computer and Communication Engineering, vol. 11, no. 9, pp. 10551–10560, Sep. 2023.

[36] Mohanarajesh Kommineni. (2023/6). Investigate Computational Intelligence Models Inspired By Natural Intelligence, Such As Evolutionary Algorithms And Artificial Neural Networks. Transactions On Latest Trends In Artificial Intelligence. 4**. P**30. Ijsdcs.

[37] Settibathini, V. S., Kothuru, S. K., Vadlamudi, A. K., Thammreddi, L., & Rangineni, S. (2023). Strategic analysis review of data analytics with the help of artificial intelligence. International Journal of Advances in Engineering Research, 26, 1-10.

[38] Sandeep Rangineni Latha Thamma reddi Sudheer Kumar Kothuru , Venkata Surendra Kumar, Anil Kumar Vadlamudi. Analysis on Data Engineering: Solving Data preparation tasks with ChatGPT to finish Data Preparation. Journal of Emerging Technologies and Innovative Research. 2023/12. (10)12, PP 11, https://www.jetir.org/view?paper=JETIR2312580

[39] Sehrawat, S. K. (2023). The role of artificial intelligence in ERP automation: state-of-the-art and future directions. *Trans Latest Trends Artif Intell*, *4*(4).

[40] Naga Surya Teja Thallam. (2023). High Availability Architectures for Distributed Systems in Public Clouds: Design and Implementation Strategies. European Journal of Advances in Engineering and Technology.

[41] Arpit Garg, S Rautaray, Devrajavans Tayagi. Artificial Intelligence in Telecommunications: Applications, Risks,and Governance in the 5G and Beyond Era. International Journal of Computer Techniques – Volume10Issue1,January - February – 2023. 1-19.

[42] Varinder Kumar Sharma - Cloud-Edge Continuum in 5G: A Latency-Aware Network Design Review -International Scientific Journal of Engineering and Management Volume: 02 Issue: 03 | Mar – 2023. DOI: 10.55041/ISJEM00133