A Comparative Review of AI-Driven Zero Trust Security Approaches for Secure Multi-Tenant SaaS Platforms

Smita Bisht* and Anoop Kumar

Department of Computer Science, Banasthali Vidyapith, Rajasthan, India
smitabisht1991@gmail.com*, anupbhola@banasthali.in

Abstract. Increased adoption of cloud computing and SaaS is attributed to scalability, flexibility, and efficiency on one side. On the other side, multi-tenant SaaS environments create certain security issues related to access control, tenant isolation, insider attacks, API security, and various cyber-attacks in general. An efficient approach for addressing these challenges is offered in the form of Zero Trust Architecture (ZTA) with a set of assumptions related to continuous authentication and "Never Trust, Always Verify" policy. For comparative analysis in the current literature review, we consider five papers dealing with the multi-tenant SaaS security, Zero Trust architecture, AI-based threat detection, identity and access management (IAM), and API security. We will evaluate the capabilities of these papers considering security aspects, ZTA implementation, machine learning techniques application, tenant isolation, performance evaluation, strengths, and weaknesses. As a result of comparative analysis, we see that the current approaches provide excellent results in some particular areas (e.g., tenant-oriented security, continuous trust assessment, AI-powered threat detection, IAM, workload isolation, or API security) however, none of them can incorporate all of the above-mentioned aspects in a unified multi-tenant SaaS security approach. Another significant drawback of the current papers is the use of different experimental environments and evaluation metrics in performance analysis. Thus, it becomes difficult to compare the results obtained in various papers. The main contribution of this literature review is the discovery of this gap and the research direction towards an adaptive AI-based Zero Trust framework with capabilities of behavior analysis, continuous trust/risk assessment, tenant-aware access control, and API security.

Keywords: Zero Trust Architecture, Multi-Tenant SaaS, Cloud Security, Artificial Intelligence, Identity and Access Management, API Security, Adaptive Risk Assessment.

1 Introduction

Cloud computing has become a revolutionary computing model in terms of offering scalable, on-demand and cost-efficient services via the Internet. The success of cloud computing has led to reduction in infrastructure costs, increased operational efficiency, and availability of computing resources anywhere and anytime. There are various cloud service models like IaaS, PaaS, and SaaS among others. However, SaaS has changed

© The Author(s) 2026
A. Shastri et al. (eds.), *Proceedings of the Fourth Workshop on Applications of Computational Intelligence and Interactive Systems (WACIIS 2026)*, Advances in Intelligent Systems Research 217,
https://doi.org/10.2991/978-94-6239-832-0_18

modern application delivery through provision of software applications via the Internet without need for installation or maintenance [19].

SaaS allows various organizations to use the same software application from a shared cloud infrastructure. In order to optimize the use of the resources and to keep costs at minimum levels, most of the SaaS providers use a multi-tenant architecture whereby various tenants use the same application instance but in a logically separate way infrastructure. Though this model comes with several benefits including efficiency in resource usage, scalability, simplified management and reduced deployment costs, security becomes a major issue [1][8][9].

The traditional approach of perimeter-based cybersecurity that was adopted to protect multi-tenant SaaS platforms from potential dangers is no longer sufficient in the current environment. Such a platform is exposed to various risks, such as breaches of access control, data leaks from one tenant to another, privilege escalation, insider attacks, attacks via API and lateral movements. Apart from this, the implementation of cloud-native services and distributed applications has expanded the attack surface [2], [21]. Thus, the need for intelligent cybersecurity measures is increasing with every passing day.

The Zero Trust Architecture (ZTA) has been shown to be a promising cybersecurity approach to current challenges due to its implementation of "Never Trust, Always Verify" principle. Unlike the traditional models, which trust an entity after verifying it, ZTA verifies each and every request for access to the platform based on user identity, device, context and security policy. Moreover, advances in AI and ML technologies have further augmented the capacity of Zero Trust in threat detection, behavioral and anomaly detection, risk assessment and policy enforcement [3]. The application of AI along with Identity-Aware Proxy (IAP), Continuous Adaptive Risk Assessment (CARA), Micro-Segmentation and Multi-Factor Authentication (MFA) technologies has helped Zero Trust in securing multi-tenant SaaS platforms in the cloud.

The present paper provides a comparative review of five case studies dealing with topics like Zero Trust Security, AI-based threat mitigation, multi-tenant SaaS protection, tenant isolation, and intelligent access control systems. The case studies selected for this comparative review are evaluated in accordance with their objectives, methods used, architectural features, security mechanisms implemented, ways of implementation, performance assessment, merits, and demerits. The review discusses current research trends, research gaps, and future research directions related to the development of adaptive AI-based Zero Trust Security systems [20].

Figure 1 illustrates the evolution of security models from traditional perimeter-based security to AI-driven adaptive Zero Trust architectures for securing modern multi-tenant SaaS platforms.

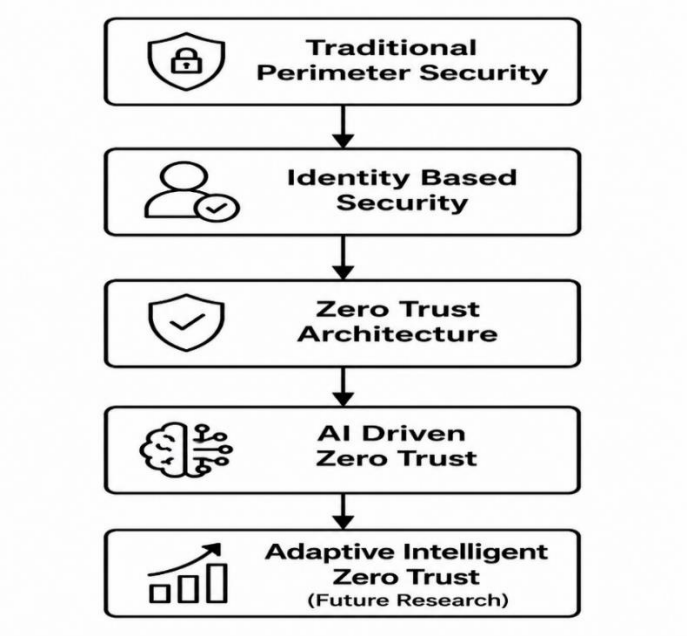

Fig. 1. Evolution of Security Models for Multi-Tenant SaaS

2 Review Methodology

In this paper, a focused comparative methodology was adopted to review research related to Zero Trust Architecture (ZTA), AI-powered cloud security and multi-tenant SaaS security solutions. Relevant papers were selected by utilizing combinations of keywords, namely: Zero Trust Architecture, multi-tenant SaaS security, AI-driven Zero Trust, tenant isolation, continuous trust assessment, identity and access management and API security.

Papers were included in further comparative analysis if they covered one or several security dimensions that are directly relevant to multi-tenant cloud or SaaS security, such as: tenant-aware security, implementation of Zero Trust architecture, adaptive trust/risk assessment, threat detection powered by AI/ML, identity and access management, workload isolation, and API security. Papers which were not covering these security dimensions to a sufficient extent or providing enough information about architectural, implementation or evaluation aspects for comparative analysis were not regarded as core papers.

Based on these criteria, five representative studies were selected for comparative analysis. These papers were selected due to their complementary coverage of the security dimensions, which is necessary for creating an integrated architecture of multi-tenant SaaS security solution. TOSSMA – Tenant Oriented SaaS Security Management, ZTA based on Identity Aware Proxy (IAP), Micro-Segmentation and Continuous Adaptive Risk Assessment (CARA) – continuous Zero Trust implementation,

ZephyrGuard – AI-powered threat detection and workload isolation, IAM framework – identity centric authentication and trust assessment, and API Security Gateway – tenant aware API protection.

Selected papers were compared using common parameters, which include: research objective, security mechanisms, Zero Trust capabilities, AI/ML usage, implementation environment, authentication and authorization, tenant isolation, continuous trust assessment, performance evaluation, strengths and limitations. The goal of this focused comparative analysis is not creating a systematic review of all existing literature on Zero Trust architecture, but comparing complementary security approaches and identifying capabilities which should be incorporated into existing multi-tenant SaaS security architecture.

3 Comparative Review of Selected Zero Trust Security Approaches

3.1 Tenant-Oriented SaaS Security Management Architecture (TOSSMA)

The rapid integration of multi-tenant Software as a Service (SaaS) solution has improved resource utilization and minimized costs for implementing the solution. However, there are some important security challenges that occur due to multi-tenancy such as tenant isolation, data confidentiality, access control and customization of security. In general, current approaches to solving security issues of SaaS solutions are provider-centric and do not provide any scope of customization of security policies of tenants [6][14][15]. In order to solve the above problem, Mohamed Almorsy, John Grundy, and Amani S. Ibrahim have proposed an architecture called Tenant-Oriented SaaS Security Management Architecture (TOSSMA).

TOSSMA has shifted the security management paradigm from provider-centric to tenant-centric, under which tenant can specify its own security policy without making any changes in the underlying SaaS application. TOSSMA makes use of the interception technique for incorporating various security controls like identification, authentication, authorization, auditing, input validation and cryptography at different levels of architecture which include system level, component level, class level, and method level [7]. In addition to this, run-time security customization allows customization of tenant specific policies without changing any application code.

The proposed architecture was evaluated through four SaaS applications including Galactic, PetShop and SplendidCRM. According to the experimental results, TOSSMA architecture offers an adequate solution for identity management, authentication, authorization, auditing, and input validation without causing high performance overhead [1]. Moreover, the performance degradation of the system depends mainly on the number of protected resources and tenant's own security policies, not the workload of the entire application.

While TOSSMA is capable of providing an adequate framework for the implementation of tenant-oriented security policies, there are a number of limitations of this

approach. It should be noted that TOSSMA architecture is based on static security policies and does not utilize AI and ML for the purposes of intelligent threat detection and decision making. Also, it does not include any of the main Zero Trust concepts like continuous risk assessment and trust evaluation [1]. Thus, TOSSMA is a good platform for the development of security in multi-tenant SaaS applications, but it requires AI-enabled Zero Trust features to become more robust.

3.2 Zero Trust Framework Using Micro-Segmentation, Identity-Aware Proxy and Continuous Adaptive Risk Assessment

Zero Trust Architecture (ZTA) stands out as one of the most efficient security architectures for securing cloud environments from emerging cyber threats [11][13]. While perimeter security architecture presumes that only a specific group of devices and users inside a defined network perimeter is secure, ZTA supposes that neither device nor any user or application can be trusted and, therefore, requires constant authentication before providing access to cloud resources. Adebayo Nurudeen Kalejaiye and Joye Ahmed Shonubi presented an all-inclusive zero trust model which combines IAP, Micro-Segmentation, and CARA to provide enhanced security in multi-tenant cloud environment.

The main purpose of the developed architecture is replacement of static authentication process with continuous verification of trust within the entire duration of a user session [2]. In contrast to the traditional method of verifying only user authentication data, the proposed architecture will evaluate various contextual factors like user identification, posture of the user's device, network characteristics, access behaviors, and other environmental factors.

Three major security components can be observed in the proposed security framework. Identity-Aware Proxy (IAP) is used for authentication and authorization of each request due to using contextual information and multi-factor authentication. Segregation of cloud infrastructure into security zones is done through Micro-Segmentation that increases isolation between tenants and reduces lateral movement [10][12]. Finally, Continuous Adaptive Risk Assessment (CARA) assesses the activities of users and devices along with the analysis of contextual information in order to calculate dynamic risk score [16].

This security framework was tested using several types of attacks such as insider attacks, credential abuse, unauthorized access and lateral movement. According to the simulation results, there is an increase in attacks detection, isolation among tenants, and access control compared to the traditional method of perimeter security [2]. Furthermore, CARA allows analyzing risks in real-time mode, whereas Micro-Segmentation prevents the propagation of attacks in shared cloud environment.

3.3 AI-Driven Zero Trust Enforcement in Multi-Tenant Kubernetes Clusters

The use of Kubernetes for cloud-native applications has created many security issues in multi-tenant environment settings, including lateral movements, privilege escalation, container compromise, and data exfiltration. The conventional methods of security such

as RBAC and static network policies offer inadequate protection against emerging security challenges. Therefore, the authors suggested an AI-enabled Zero Trust architecture named ZephyrGuard that can help in solving security problems in multi-tenant Kubernetes clusters installed in VxRail and AWS-EKS.

The main aim of ZephyrGuard is to improve Kubernetes security by means of workload monitoring and adaptive policy enforcement. Different from static methods of security management, the solution uses eBPF telemetry, LSTM-based anomaly detection, federated learning, Istio service mesh with mTLS, and policy synthesis using AI to conduct analysis of workload activity in real time [3]. In accordance with the dynamic trust score calculations, the framework creates isolation policies preventing any unauthorized access and lateral movements while ensuring tenants' privacy.

The framework was tested on a mixed infrastructure that comprised 120 Kubernetes nodes on VxRail and AWS-EKS. As per experimental results, the proposed framework showed better performance than conventional methods such as RBAC and Calico in terms of security. It resulted in an F1-score of 97.3%, 18 ms isolation latency, and 2.1% false-positive rate. Moreover, exfiltration of data through any attack was minimized to 11 KB compared to 2.7 MB in traditional methods, showcasing the efficacy of AI-enabled adaptive security. Compliance with the standards of NIST SP 800-207, GDPR, and PCI-DSS enhances its real-world usability.

However, there are certain limitations associated with the framework. Continuous monitoring and learning through AI incur roughly 5.2% computational overhead per node. Moreover, as the cluster gets larger, the accuracy of detection decreases, while deep learning is vulnerable to any adversarial attack [3]. Furthermore, the proposed security architecture is relevant only for cloud-native Kubernetes and not multi-tenant SaaS security architecture.

All in all, the integration of AI and Zero Trust security principles through ZephyrGuard proves to be highly beneficial in terms of workload segregation, adaptive access control, and intelligent threat detection in Kubernetes clusters. Nevertheless, future research ought to focus on lightweight trust prediction models, XAI technologies, scalability of cross-cloud trust orchestration, and generic Zero Trust architectures.

3.4 Authentication and Identity Management Based on Zero Trust Architecture

The concept of Identity and Access Management (IAM) is a crucial element of Zero Trust Architecture (ZTA) designed to ensure cloud security through the interaction of users, devices, and applications. Password and username authentication techniques alone are not sufficient to protect cloud infrastructure from advanced attacks, like credentials theft, session hijacking, and any other kind of unauthorised access to system components. That is why the authors introduced a Zero Trust architecture-based framework for authentication and identity management that consists of MFA, device authentication, ABAC, and continuous trust [22].

The main purpose of this framework is the implementation of an identity-centric security mechanism that will continuously authenticate users and devices in order to provide access to the cloud environment. Contrary to the traditional authentication

approach, the proposed framework works according to the "Never Trust, Always Verify" principle of the Zero Trust architecture by using explicit authentication and context verification in combination. The contextual attributes include user identity, device certificates, geographic location, IP address, authentication timestamp, and authentication tokens.

One of the main contributions made in this paper lies in the utilization of attribute-based access control (ABAC) by implementing the XACML architecture. In contrast to the RBAC model, the attribute-based access control allows more precise authorization taking into account user, resource and environmental attributes [4][17]. Also, this architecture utilizes a hybrid trust evaluation approach that computes dynamic trust scores depending on various contextual factors, including request history, geolocation, usage of the resource, previous access attempts, and organizational trust data. Authorization occurs only when the policies and trust evaluation meet certain security criteria.

There are multiple benefits of the architecture suggested, among which are improved user authentication due to the use of multifactor identification, secure device identification using digital certificates, flexible policy-based authorization provided by ABAC, and adaptive context-aware trust evaluation of the user [4]. At the same time, this architecture does not consider any advanced approaches in AI or ML to perform behavioral analysis or other intelligent activities and its evaluation is merely limited to proof-of-concept.

In summary, the proposed framework adds value to the process of implementing zero trust by using continuous authentication, context-based authorization, and dynamic trust evaluation. Nonetheless, the integration of artificial intelligence-powered behavior analysis and threat forecasting capabilities would make it more effective for securing multi-tenant cloud and SaaS platforms.

3.5 API Security Gateway and Data Access Control Model for Multi-Tenant Full-Stack Systems

The fast adoption of multi-tenant SaaS applications, developed in microservices and API architecture, leads to growing demand for secure communication between the user and cloud services. The API gateways have become the key component in securing the system but are still vulnerable to various types of attacks, including token forgery, privilege escalation, data access without the right permissions, and manipulations with API requests. Existing API security solutions are mainly focused on authentication and authorization and provide little functionality in terms of tenant-level security policies [15]. Thus, the authors have suggested using Zero Trust-based API Security Gateway and Data Access Control model for multi-tenant full-stack systems.

The main purpose of the framework is to ensure constant authentication and authorization, and secure access to APIs with high efficiency at large-scale traffic volumes. The framework uses JSON Web Tokens authentication, Open Policy Agent, GraphQL field-level authorization, caching of policies, and tenant-level policy evaluation. Each API request is authenticated, authorized and checked according to the tenant-specific security policies.

The proposed framework was tested based on a number of 1.77 million API requests with a load of 12,000 queries per second (QPS), and according to experimental results, the latency was found to be 74.2 ms on an average with a 99th percentile latency lower than 85 ms. The security evaluation revealed that the rate of detection of GraphQL field overreach is 94.1%, privilege escalation is 92.8%, request manipulation is 91.7%, token forgery is 89.5%, and silent probing is 86.3%.

Though having a number of merits, the proposed framework suffers from a few limitations as well. Firstly, it uses a rule-based mechanism of policy enforcement, where Rego policies have been used and has no provisions for AI or ML techniques for behavioral analysis, intelligent trust assessments, or threat detection. Secondly, the semantic policy modeling and cross-cloud policy orchestration still pose research challenges.

In general, the suggested API Security Gateway proves to be a good solution of implementing Zero Trust approach to ensure the security of application layer communications in the environment of multi-tenant SaaS architecture [5]. Nevertheless, incorporation of AI-based anomaly detection and intelligent policy orchestration would significantly improve its flexibility and security.

4 Comparative Analysis and Discussion

Table 1. Comparative Analysis of Selected Studies

Parameter	TOSSMA Framework	ZTA Framework	Zephyr-Guard	IAM Framework	API Security Gateway
Primary Focus	Tenant-Oriented SaaS Security	Zero Trust Framework	AI-based Kubernetes Security	Identity & Access Management	API Security Gateway
Cloud Environment	Multi-Tenant SaaS	Multi-Tenant Cloud	Kubernetes Hybrid Cloud	Cloud Computing	Multi-Tenant Full-Stack SaaS
Zero Trust Implementation	Partial	Complete	Complete	Complete	Complete
AI/ML Integration	No	Limited	Yes (LSTM + FL)	Proposed (Future Scope)	No
Authentication	Identity Management	Identity-Aware Proxy	mTLS	MFA + PKI	JWT
Authorization	Policy Based	Dynamic	AI Policy	ABAC	OPA
Continuous Trust Assessment	No	CARA	AI-based	Trust Score	Partial

Parameter	TOSSMA Framework	ZTA Framework	Zephyr-Guard	IAM Framework	API Security Gateway
Tenant Isolation	Yes	Yes	Yes	Partial	Yes
Performance Evaluation	Experimental	Simulation	Experimental	Prototype	Experimental
Main Contribution	Runtime Security Customization	Adaptive Zero Trust	Intelligent Threat Detection	Dynamic Authorization	Fine-Grained API Security

4.1 Comparative Analysis

Table 1 provides a comparative evaluation of the selected five papers in terms of their research aims, Zero Trust architecture, AI involvement, authentication, authorization, tenant isolation, and performance assessment. The comparative analysis indicates that despite the common purpose of improving the cloud security environment in all selected studies, each one of them deals with different aspects of Zero Trust Architecture.

Of all the five chosen papers, the Zero Trust Architecture framework proposed by Kalejaiye and Shonubi (2025) is considered the most comprehensive because it involves three key Zero Trust components: Identity-Aware Proxy (IAP), Micro-Segmentation, and Continuous Adaptive Risk Assessment (CARA). However, the Tenant-Oriented SaaS Security Management Architecture (TOSSMA) offered by Mohamed Almorsy, John Grundy, and Amani S. Ibrahim (2012) is mostly concerned with customization of security at the tenant level and runtime policies but fails to include continuous trust validation and artificial intelligence [1]. The most intelligent and adaptive zero-trust framework is ZephyrGuard proposed by Cherukupalle (2025) that involves Artificial Intelligence (AI), Long Short-Term Memory (LSTM)-based anomaly detection, and Federated Learning (FL). The same is true for the identity and access management framework by Ivana Kovacevic, Milan Stojkov and Milos Simic1 (2023) which stresses the importance of identity-based authentication and authorization through Attribute-Based Access Control (ABAC) and contextual trust assessment. Finally, Yu Mao, Xiangjun Ma and Jiawen Li (2025) provide an improved API security gateway with tenant-specific policies through their Zero Trust-based approach [5].

In conclusion, it can be seen that no one research work solves all the above problems of intelligent threat detection, trust assessment, tenant isolation, API security, and SaaS deployment. Hence, there is a requirement for a unified AI-based Zero Trust framework.

4.2 Comparison of Security Features

Table 2. Comparison of Security Features Across Selected Studies

Security Feature	TOSSMA Framework	ZTA Framework	ZephyrGuard	IAM Framework	API Security Gateway
Multi-Tenant SaaS Support	✓	✓	✓	Partial	✓
Zero Trust Architecture	Partial	✓	✓	✓	✓
AI / Machine Learning	✗	Limited	✓	Future Scope	✗
Continuous Authentication	✗	✓	✓	✓	Partial
Multi-Factor Authentication (MFA)	✓	✓	✗	✓	✗
Identity-Aware Proxy (IAP)	✗	✓	✗	✗	✗
Attribute-Based Access Control (ABAC)	✗	✗	✗	✓	Partial
Micro-Segmentation	✗	✓	✓	✗	✗
API Security	✗	Partial	✗	✗	✓
Dynamic Risk Assessment	✗	✓	✓	✓	Partial
Tenant Isolation	✓	✓	✓	Partial	✓
Policy-Based Security	✓	✓	✓	✓	✓
Experimental Validation	✓	✓	✓	Prototype	✓

4.3 Discussion

The evolution of security mechanisms in the chosen papers can be summarized in Table 2. Although all of them employ policy-based enforcement, the architecture approach is quite different. TOSSMA Framework allows for efficient customization of security policies, but the latter are static in nature. ZTA Framework offers a full-fledged implementation of Zero Trust with the help of identity verification, Micro-Segmentation, and adaptive risk assessments. ZephyrGuard extends the capabilities of Zero Trust model by adding AI for behavioral analysis and intelligent anomaly detection resulting in superior threat detection efficiency. IAM Framework allows improving identity and access management with ABAC and contextual trust evaluations but lacks intelligent threat detection capabilities API Security Gateway deals with the security of the API

layer through JWT, Open Policy Agent, and GraphQL authorizations but is still relying on policy enforcement.

The limitation that can be found in all the selected papers is the lack of a single solution that incorporates AI-driven threat intelligence, continuous trust assessment, intelligent policy orchestration, scalable tenant isolation, and Zero Trust security at all the stages. Such limitation could serve as an important research direction.

4.4 Performance Comparison of Selected Studies

Table 3 compares the performance of the selected approaches using key security evaluation metrics, including threat detection accuracy, response latency, false positive rate, scalability, and overall security effectiveness.

Table 3. Performance Metrics Reported in Selected Studies

Performance Metric	ZTA Framework	ZephyrGuard	API Security Gateway
Threat Detection Accuracy	High	97.3%	94.1%
Average Response Latency	Moderate	18 ms	74.2 ms
False Positive Rate	Low	2.1%	Not Reported
Large-Scale Evaluation	Simulation	120 Kubernetes Nodes	1.77 Million API Requests
Primary Evaluation Focus	Zero Trust Validation	AI Threat Detection	API Security Performance

4.5 Performance Discussion

Performance results from the selected papers are summarized in Table 3. ZephyrGuard achieves an F1-score of 97.3%, an isolation latency of 18 ms, and a false-positive rate of 2.1%, proving the promise of adaptive threat detection enabled by LSTM-based behavioral analytics and federated learning. The Zero Trust framework shows better security performance with the implementation of Identity-Aware Proxy (IAP), Continuous Adaptive Risk Assessment (CARA), and Micro-Segmentation, while the API Security Gateway shows good performance in securing APIs in cases of high-volume request processing.

Still, these performance results cannot be considered as a direct comparison between selected frameworks. Selected studies have been evaluated in different experimental environments, workloads, security scenarios, datasets, and performance metrics. Specifically, ZephyrGuard was evaluated in Kubernetes-based environment, Zero Trust framework was assessed in terms of simulation-based security scenarios, and API Security Gateway was tested with large-scale API requests processing. Hence, performance results listed in Table 3 reflect the performance of the selected frameworks in these specific experimental settings and not their superior performance compared to one another.

The comparison reveals important performance criteria for evaluating future multi-tenant SaaS security frameworks, specifically threat-detection efficiency, latency, false positives, scalability, and security efficiency under practical workload conditions.

5 Research Challenges, Gaps and Future Directions

A comparison between the chosen studies reveals substantial advancements made by using Zero Trust Architecture (ZTA) in cloud computing and multi-tenant SaaS environment. The proposed solutions help resolve the relevant problems of security, including tenant isolation, identity management, adaptive authentication, workload protection, API security, and policy-based authorization [18]. Nevertheless, each research project addresses a certain area of security issues and does not provide a full-fledged end-to-end approach.

The main problem for research lies in the lack of one single security framework capable of addressing tenant-aware SaaS security, continuous trust assessment, intelligent threat identification, API protection, identity management, and workload isolation. For instance, TOSSMA Framework concentrates on tenant-aware security but fails to integrate continuous trust verification and artificial intelligence into their security system. The authors of ZTA Framework offer a comprehensive Zero Trust Architecture based on Identity-Aware Proxy (IAP), Micro-Segmentation, and Continuous Adaptive Risk Assessment (CARA) but fail to integrate the use of artificial intelligence into their security system. Also, ZephyrGuard, IAM Framework, and API Security Gateway separately discuss Kubernetes security, identity management, and API security but do not integrate them within one single security framework [20].

There is another research gap that is related to the use of artificial intelligence (AI) and machine learning (ML) in adaptive security management. Although the success of AI in anomaly detection was proved by ZephyrGuard, currently, there are many security frameworks based on static policies and trust models which are unable to counteract the emerging cyber threats, insider threats, and the dynamics of the cloud environment.

As for the comparative analysis of different research, there were revealed some issues connected with scalability and deployment of different frameworks. In general, proposed frameworks were tested with the help of simulations, prototypes, or specific applications but not in large-scale enterprise SaaS settings. Besides, the achievement of the optimal combination of security, overhead, response time, and scalability remains problematic.

In summary, there is no doubt about the identified research gap in the literature review. None of the chosen papers combines the elements of tenant-aware security in SaaS, adaptive Zero Trust architecture, intelligent behavioral analytics using artificial intelligence (AI), continuous trust evaluations, risk assessment, identity-based access control, workload protection, and API security into a unified approach.

Thus, future research should concentrate on adaptive Zero Trust systems that will be able to assess the behavior of users, devices, and applications in real-time mode. Furthermore, such systems need to take into consideration context information as well. It is essential to mention that such features as XAI, federated learning, lightweight trust

prediction models, policy orchestration, and continuous compliance monitoring can bring significant benefits. From the existing research gaps, it is necessary for future Zero Trust architectures to incorporate AI-based behavioral analysis, continual trust evaluation, policy orchestration, API security, and intelligent access control of tenants into one system.

Figure 2 summarizes the major research gaps identified across the reviewed studies and highlights the need for a unified AI-driven Zero Trust framework capable of integrating adaptive trust management, intelligent risk assessment, and tenant-aware security mechanisms.

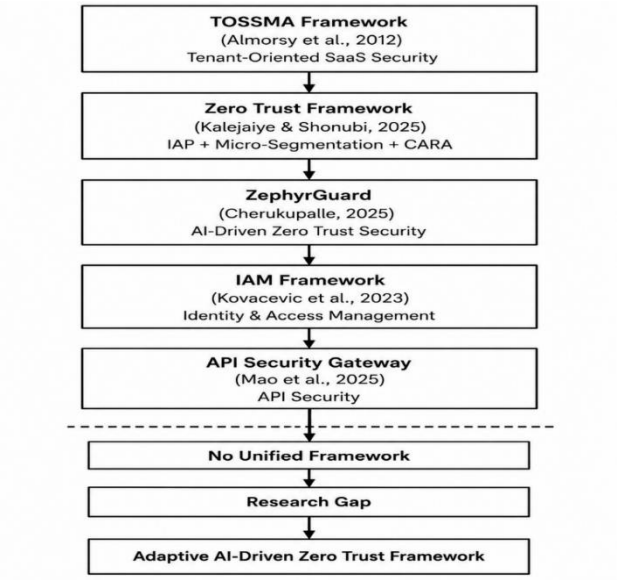

Fig. 2. Research Gap Identification

Table 4. Research Gap Matrix

Feature	TOSSMA Framework	ZTA Framework	Zephyr-Guard	IAM Framework	API Security Gateway	Gap
AI	No	Partial	Yes	No	No	Yes
Continuous Trust	No	Yes	Yes	Yes	Partial	Yes
API Security	No	Partial	No	No	Yes	Yes
SaaS	Yes	Yes	Partial	Partial	Yes	Yes
Tenant Isolation	Yes	Yes	Yes	Partial	Yes	Yes
Unified Framework	No	No	No	No	No	Major Gap

Feature	TOSSMA Framework	ZTA Framework	Zephyr-Guard	IAM Framework	API Security Gateway	Gap
Explainable AI (XAI)	No	No	Future	No	No	Yes

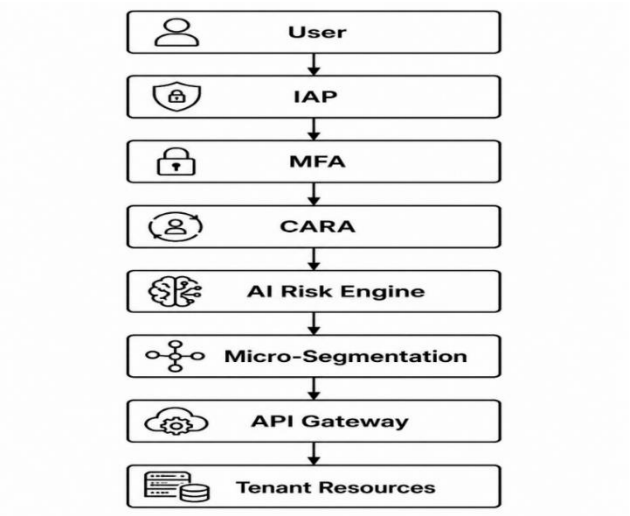

Fig. 3. Proposed Adaptive AI-Driven Zero Trust Security Architecture for Secure Multi-Tenant SaaS Platforms

6 Conclusion

Advances in cloud computing and multi-tenant Software-as-a-Service (SaaS) have revolutionized application deployment processes. Nevertheless, cloud and multi-tenant SaaS environments suffer from a range of security issues such as unauthorized access, tenant isolation, insider attacks, APIs security, and advanced cyber-attacks. This review paper offered a comparative analysis of five research papers dealing with Zero Trust Architecture (ZTA), tenant-oriented SaaS security, identity and access management, AI-based security, Kubernetes workload protection, and API security.

The comparative analysis showed that all studies discussed here address particular aspects of Zero Trust security. Some studies highlight tenant-specific security solutions, while others concentrate on adaptive authentication, threat intelligence, identity-aware access management, workload isolation, or API security. Yet none of the studies analyzed offers an integrated framework for AI-driven threat intelligence, continuous trust assessment, adaptive risk management, identity-aware access control, workload security, and API security within the context of ZTA. From the above gaps that have been identified, there is a requirement for an adaptive AI-driven Zero Trust framework that will be able to dynamically assess user behaviors, device trust, context, and application communications for intelligent decision-making. This is due to the fact that the use of

AI, XAI, Federated Learning, risk evaluation, and policy management in Zero Trust can bring great benefits for the security, scalability, and resilience of future multi-tenant SaaS platforms.

In conclusion, this literature review has given a thorough understanding of the Zero Trust research in the existing studies, research gaps and also future research directions. The results of this study can help researchers, practitioners, and cloud service providers design secure multi-tenant SaaS platforms.

Based on the identified limitations of existing approaches, Figure 3 presents a conceptual future research framework that integrates identity-aware authentication, AI-based behavioral analytics, adaptive trust evaluation, API security, and continuous monitoring within a unified Zero Trust architecture.

References

1. Almorsy, M., Grundy, J., Ibrahim, A.S.: Tossma: A tenant-oriented saas security management architecture. In: 2012 IEEE fifth international conference on cloud computing, pp. 981-988). IEEE (2012).
2. Kalejaiye, A.N., Shonubi, J.A.: Zero trust enforcement using microsegmentation, identity-aware proxies, and continuous adaptive risk assessment in multi-tenant cloud environments. International Journal of Computer Applications Technology and Research, vol. 14(7), pp. 61-77 (2025).
3. Cherukupalle, N.S.: Zero Trust Enforcement Through AI-Driven Isolation in Multi-Tenant Kubernetes Clusters on VxRail and AWS-EKS. In: 2025 9th International Conference on Inventive Systems and Control (ICISC), pp. 574-581 IEEE (2025).
4. Kovacevic, I., Stojkov, M., Simic, M.: Authentication and identity management based on zero trust security model in micro-cloud environment. In: Conference on Information Technology and Its Applications, pp. 481-489, Springer Nature Switzerland, Cham (2023).
5. Mao, Y., Ma, X., Li, J.: Research on API Security Gateway and Data Access Control Model for Multi-Tenant Full-Stack Systems (2025).
6. Sun, W., Zhang, X., Guo, C. J., Sun, P., Su, H.: Software as a service: Configuration and customization perspectives. In 2008 IEEE Congress on Services Part II (services-2 2008) pp. 18-25, IEEE (2008).
7. Cai, H., Wang, N., Zhou, M. J.: A transparent approach of enabling SaaS multi-tenancy in the cloud. In 2010 6th World Congress on Services, pp. 40-47, IEEE (2010).
8. Pervez, Z., Lee, S., Lee, Y.K.: Multi-tenant, secure, load disseminated SaaS architecture. In: 2010 The 12th International Conference on Advanced Communication Technology (ICACT), vol. 1, pp. 214-219, IEEE (2010).
9. Wang, D., Zhang, Y., Zhang, B., Liu, Y.: Research and implementation of a new SaaS service execution mechanism with multi-tenancy support. In: 2009 First International Conference on Information Science and Engineering, pp. 336-339, IEEE (2009).
10. Ravi, C., Shaik, M., Saini, V., Chitta, S., Bonam, V.S.M.: Beyond the firewall: Implementing zero trust with network microsegmentation. Nanotechnology Perceptions, vol. 21, pp. 560-578 (2025).
11. Emmanni, P.S.: Implementing a zero trust architecture in hybrid cloud environments. International Journal of Computer Trends and Technology, vol. 72(5), pp. 33-39 (2024).

12. Zanasi, C., Marchetti, M., Colajanni, M.: Cybersecurity Domains: A design pattern for creating Zero Trust Architectures through microsegmentation. In: 2024 IEEE Conference on Dependable, Autonomic and Secure Computing (DASC), pp. 15-22, IEEE (2024).
13. Mehraj, S., Banday, M.T.: Establishing a zero trust strategy in cloud computing environment. In: 2020 International Conference on Computer Communication and Informatics (ICCCI), pp. 1-6, IEEE (2020).
14. Krebs, R., Momm, C., Kounev, S.: Architectural concerns in multi-tenant saas applications. Closer, vol. 12, pp. 426-431 (2012).
15. Tiwari, P.K., Joshi, S.: A review of data security and privacy issues over SaaS. In: 2014 IEEE International Conference on Computational Intelligence and Computing Research, pp. 1-6, IEEE (2014).
16. Stevens, T.: Zero-Trust Microsegmentation (ZTM): A Policy-Enforced Model for Fine-Grained Security. Authorea Preprints (2025).
17. Bello, A. J., Diyan, M., Asghar, I.: Zero trust implementation for legacy systems using dynamic microsegmentation, role-based access control (RBAC), and attribute-based access control (ABAC). In: 2025 4th International Conference on Computing and Information Technology (ICCIT), pp. 181-189, IEEE (2025).
18. Mehmood, K.T., Saleem, U., Jumani, A., Ijaz, I., Rafique, A.A., Iqbal, R.: Implementing Zero-Trust Network Access (ZTNA) in Hybrid IT Architectures: A Comparative Study of Policy Enforcement, Identity Management, and Threat Containment Strategies. Annual Methodological Archive Research Review, vol. 3(5), pp. 124-49 (2025).
19. Mietzner, R., Leymann, F., Papazoglou, M.P.: Defining composite configurable SaaS application packages using SCA, variability descriptors and multi-tenancy patterns. In 2008 Third International Conference on Internet and Web Applications and Services, pp. 156-161, IEEE (2008).
20. Eboseremen, B. O., Ogedengbe, A. O., Obuse, E., Oladimeji, O., Ajayi, J. O., Akindemowo, A. O., ..., Erigha, E. D.: Secure data integration in multi-tenant cloud environments: Architecture for financial services providers. Journal of Frontiers in Multidisciplinary Research, vol. 3(1), pp. 579-592 (2022).
21. Varadharajan, V., Tupakula, U.: Security as a service model for cloud environment. IEEE Transactions on network and Service management, vol. 11(1), pp. 60-75 (2014).
22. Mietzner, R., Unger, T., Titze, R., Leymann, F.: Combining different multi-tenancy patterns in service-oriented applications. In: 2009 IEEE International Enterprise Distributed Object Computing Conference, pp. 131-140, IEEE (2009).

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (http://creativecommons.org/licenses/by-nc/4.0/), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

