

# Advanced cloud security framework based on zero trust architecture and adaptive deep learning for next-generation systems

Israa Basim, Amel Meddeb Makhoul, Ahmed Fakhfakh

NTS'COM Unit, National School of Electronics and Telecommunication, University of Sfax, Sfax, Tunisia

## Article Info

### Article history:

Received Jan 15, 2025

Revised Apr 23, 2025

Accepted Jul 3, 2025

### Keywords:

Adaptive deep learning  
Cloud security  
Hybrid security framework  
Next-generation cloud security  
Security metrics  
Zero trust architecture

## ABSTRACT

Static rule-based models and cloud access security brokers (CASBs) — traditional cloud security frameworks— can no longer effectively mitigate modern and evolving cyber threats. Two such examples include signature-based detection methods which lack real-time versatility and are ineffective against advanced persistent threats or zero-day threats. In this paper, we introduce an adaptive zero trust framework (AZTF) based on the integration of zero trust architecture (ZTA) and adaptive deep learning (ADL) approach to dynamically evaluate threats and risks being targeted on cloud environments. It continually monitors access attempts using DL models for real-time anomaly detection. Nine synthetic datasets were generated and used in the experiment in two security domains: network traffic and access pattern. The proposed system reached 96% detection accuracy, 52% improvements in response time, and 12% resource consumption optimization compared to traditional ZTA-based security models. The results highlight the power of using a combination of continuous authentication with artificial intelligence (AI)-powered dynamic security policy application to strengthen the resilience of cloud security. Future research will focus on federated learning integration, multi-cloud security applications, and explainable AI for increased transparency of models.

*This is an open access article under the [CC BY-SA](#) license.*



## Corresponding Author:

Israa Basim

NTS'COM Unit, National School of Electronics and Telecommunication, University of Sfax

3000, Sfax, Tunisia

Email: [israabasim85@gmail.com](mailto:israabasim85@gmail.com)

## 1. INTRODUCTION

Cloud computing has revolutionized the way businesses operate by providing scalable, flexible, and cost-effective information technology (IT) solutions [1]–[3]. However, as cloud adoption grows, so does the complexity of securing cloud environments [4]–[6]. Cloud service providers host a vast array of sensitive data and critical applications, making cloud security a top concern for organizations worldwide [7]–[9]. The dynamic nature of cloud environments, along with the increasing sophistication of cyber threats, poses significant challenges to traditional security models [10]. As a result, ensuring robust, adaptive, and real-time protection for cloud resources has become a pressing necessity [11]–[14].

Traditional security approaches, such as cloud access security brokers (CASBs), have been widely used to monitor and control access to cloud services [15], [16]. While effective to some extent, these solutions are often static and unable to respond to the fast-evolving landscape of modern cloud threats [17]–[19]. CASBs

typically rely on predefined rules and configurations, which struggle to keep up with the dynamic behavior of cloud environments and the increasingly complex attack vectors. As cyber threats become more advanced, these static security models are proving insufficient in providing the level of protection required to secure sensitive cloud resources effectively [20]–[23].

To address these limitations, this paper introduces a next-generation cloud security framework that combines zero trust architecture (ZTA) [24], [25] with adaptive deep learning (ADL) techniques [26]. Zero trust has emerged as a transformative security model that operates on the principle of “never trust, always verify”. Under this model, access to cloud resources is strictly controlled, and users are continuously verified, regardless of their location within or outside the network perimeter. The zero trust model significantly reduces the risk of unauthorized access, lateral movement, and data breaches. However, while ZTA provides a robust foundation for securing cloud environments, it does not inherently address the challenge of detecting emerging threats in real time or adapting to rapidly evolving attack techniques. To address the limitations of traditional static security models, we propose a hybrid security framework that integrates ZTA with adaptive deep learning (ADL) to increase the quality of security in the cloud. It employs DL for on-time threat detection, continually analyzing user activity, network traffic, and access behavior, and thus, adapts and learns from new threats. As a result, the framework also applies dynamic security policies and measures to reduce the attack surface, in other words based on intelligent risk assessments conducted by these internal agents, they apply an attack surfaces tailored to what is the behavior of the organization, ensuring a reactive posture. For performance, it reaches a detection accuracy of 96%, better than CASB (85%) and ZTA-only (90%) models, with 52% less response time (1.2 seconds) and 12% less consumed resources. It stands out even more from existing models in terms of scalability and efficiency under load. The core enabler for these enhancements comes from ADL and its integration within ZTA, establishing the framework as a next-generation enabler for adaptive, proactive cloud security.

The rest of this paper is organized as follows: section 2 reviews related work in cloud security and ZTA. Section 3 provides background of this paper. Section 4 presents the proposed hybrid security framework in detail, outlining its design, components, and operation. Section 5 discusses experimental results and compares the performance of the proposed framework with existing solutions. Finally, section 6 concludes the paper and highlights areas for future research.

## 2. RELATED WORK

In this section, we review the existing literature on cloud security, ZTA, CASBs, the application of DL techniques in cybersecurity, and hybrid framework. The aim is to contextualize the proposed framework within the broader field of research and to highlight the gaps that this work intends to address.

In this portion of their analysis, researchers delve into traditional cloud security methodologies like identity management, encryption and monitoring. Which makes it clear just how limited these solutions are, in terms of the dynamism and fluidity with which cloud-infrastructure evolves. Ramesh *et al.* [27] introduced an antivirus with DL for rapid detection and effective treatment of polymorphic and encrypted viruses. Attou *et al.* [28] proposed a cloud-based intrusion detection model with random forest (RF) and feature engineering. A new method of the Salp swarm algorithm-based feature selection with DL-based intrusion detection (SSA-FS-DLID) technique has been proposed by Sanagana and Tummalachervu [29] for improving cloud infrastructure security. It also addresses the challenges of adopting ZTA, particularly in cloud environments. Patil *et al.* [30] provided insight into the ZTA adoption security framework for cloud-based Fintech services. Dash [31] advocated the use of ZTA for in cloud environments, specifically when deploying large language models (LLMs) in artificial intelligence (AI) applications. CASBs — visibility and control over cloud usage a particularly important point will be to analyze their strengths and weaknesses, especially where they may not yet adapt nimbly enough to hyper fast moving cloud times. Abbas [32] provided an in-depth analysis of CASBs, and sheds light on their role in stepping up cloud security. In response to more enterprises moving their sensitive data to the cloud, Ahmad *et al.* [33] addressed the demand for higher levels of cloud security. It suggested a GOSIMMG method to improve the security of the cloud using identity-based CASBs. This post walks through benefits and difficulties of employing DL models within security. Abirami and Bhanu [34] involved secure data exchange in cloud environments, specifically focusses on impersonation attacks and offers a solution based on the use of a crypto-deep neural network (CDNNCS). Experimental results indicate that. CDNNCS reduce packet loss by 10% and response time about improved 5%, significantly better than existing approaches. Aoudni *et al.*

[35] proposed HMM-TDL, a DL model that aims to spot zero-day security intrusions on cloud platforms. In this context, we take a look at hybrid security frameworks that blend conventional models and AI/ machine learning (ML) strategies, before underscoring the urgency to deploy real-time adaptive cloud security solutions against next-gen attack vectors. Yiliyaer and Kim [36] examined the increasingly widespread requirement to work safely remotely and the difficulties organization face in giving public secure access to a network. Kim and Song [37] proposed an abnormal behavior detection mechanism (ABDM) to enhance security for external access, addressing the challenges of sophisticated attacks.

In this paper, we fill this gap by designing a new generation cloud security framework combining ZTA capabilities with power of ADL algorithms. The hybrid framework is designed to do an effective real-time adaptation, i.e., overcome the limitations of traditional methods and improve the effectiveness of cloud security with a more dynamic responsive approach, including threat detection & mitigation towards evolving threats. Although the model proposed is a step in the right direction, more work needs to be done to solve problems such as interpretability and integrating DL models into existing security frameworks.

### 3. BACKGROUND

#### 3.1. Zero trust architecture

Zero trust is a security concept centered on the belief that organizations should not automatically trust anything inside or outside its boundaries, they must verify anything trying to connect to its systems and data [38]. Rather, every user or device coming in over the network edge should be authenticated. ZTA works on some core principles that focus on verification, monitoring, and least privilege access. The key principles include: never trust, always verify: ZTA works under the assumption that no user, device, or system should be trusted by default, even if they are inside the perimeter [25]. All-access requests must be authenticated, and the trust is not given until authentication has happened (authorization). Least privilege access: users, devices, and applications are only allowed the least privileged access they need to get their job done. When the rights provided to each user or device are kept, there is a potential attack surface reduction. Micro-segmentation: the network is broken up into several isolated segments and you enforce security policies with each segment. This will by default limit lateral movement in the network and make it difficult for an attacker can compromise one part of the system and then get access to many resources. Continuous monitoring and validation: unlike VPN, ZTA provides continuous tracking of users, devices, and data flows to ensure that security policies are enforced all the time. Even after the first authentication, access is continuously reconsidered depending upon the context; i.e., a combination of factors such as user behavior, device security posture, or sudden environmental changes. Data protection: ZTA stresses the importance of data security at rest as well as in transit; that is, permissioned or sensitive data must be protected against unauthorized access or breach attacks also when within the network perimeter [39]. The use of encryption is a cornerstone in securing data.

#### 3.2. Cloud access security brokers

CASBs serve as an intermediary between an organization's on-premises infrastructure and the cloud services it uses [40], [41]. CASBs enforce security policies, monitor user activities, and also ensure that all cloud products are in compliance with industry regulations. The fundamental principles of CASBs involve the following: visibility: to help the enterprises with this, CASBs offer them cloud visibility that allows the enterprise to monitor and control all cloud apps and services. This tool also identifies shadow IT (cloud services not vetted by the organization) and enables activity tracking across hundreds of SaaS applications [36]. Data security: CASBs are responsible for enforcing data protection policies that protect sensitive data when it is stored, accessed, or transmitted in the cloud. They encrypt, tokenize and apply data loss prevention DLP policies to protect data at rest and in transit. Access control: through centralization, CASBs can enforce fine-grained access control policies – based on identity, role, device or location. Threat protection: one of the primary objectives here is CASBs, designed to revoke the scope of an attack and get on top of threats before they hit your users [42]. Cloud governance: a CASB ensures consistent security and compliance policies across multiple cloud platforms, reinforcing the organizational control model. Application security: CASBs mitigate cloud application security threats by assessing the security of applications and ensuring they conform to an organization's established security requirements [43].

### 3.3. Adaptive deep learning techniques

ADL based methods are robust cybersecurity tools to detect complex evolving threats and mitigate them in cloud environments. Such techniques are based on neural networks – particularly, recurrent neural networks (RNNs) and convolutional neural networks (CNNs) – and allow computer to learn from huge datasets, respond the changing threats and modify security mechanism [44]. CNNs—a widely employed DL technique utilized for feature extraction and pattern recognition—has potential for use in both structured and unstructured data, such as logs or network traffic, allowing for automatic detection of malicious activity with minimal manual intervention [45], [46]. On the contrary, RNNs work quite well with sequential time-oriented data [47]–[49]. RNN in cloud: in the field of cloud security, RNN's are used for the detection of anomaly in a continuous stream of data such as user activity or network traffic, identifying patterns that deviate from normal behavior and may suggest potential security threats. ADL techniques for cloud security: benefits. Enhanced accuracy: advanced DL models enhance detection precision by enabling continuous learning and adapting to emerging threats, whereas traditional rule-based systems lack the flexibility to comprehend evolving attack patterns. Real-time response: by leveraging historical attack data, ML algorithms can identify suspicious activities and events, allowing organizations to proactively respond to potential threats. Scalability: cloud based environments have large data volumes and DL models can handle large data, fitting well into cloud. This makes security monitoring across various cloud services much more scalable. Reduced false positives: DL models can learn to adapt themselves to the particular behavior of any abnormality of users or devices, minimizing false positives and allowing security alerts to be more pertinent and actionable.

### 3.4. Integration of zero trust and deep learning

ZTA for DL integrates a systematic access control-based approach focusing on validation of devices, users, and networks combined with adaptive and data-driven capabilities. Priorities of these alignments consist of: dynamic trust evaluation: zero trust is all about continuously assessing trust at each access point, and DL further improves this by integrating and acting on real-time data to assess the risk and dynamically adjusting security decisions made. Context-aware access: access control is enforced through strict identity verification and contextual factors in zero trust. Threat mitigation and anomaly detection: specifically, CNNs and RNNs are used to build DL models that classify background information and detect anomalies in it in order to determine if it exhibits the typical pattern.

## 4. PROPOSED HYBRID SECURITY FRAMEWORK

### 4.1. Hybrid framework design

#### 4.1.1. Zero trust architecture in the cloud

The core security model behind our proposed methodology is based on ZTA. Attending the cloud, ZTA is based on the idea of 'never trust, always verify', an approach that is especially relevant when it comes to cloud environments, where perimeter-based security models fall short. Our methodology for ZTA implementation in a cloud environment consists of some significant components.

#### 4.1.2. Adaptive deep learning techniques

The next layer in our hybrid framework is the protection via ADL techniques when built on leveraging the security offered through ZTA. They are used to multitask, interpret and act on new threats in their cloud environment.

#### 4.1.3. Integration of ZTA and ADL

It is the combination of ZTA and application development life cycle (ADL) that will be at the core of our proposed methodology to overcome the cloud security issues [50]. Together, they facilitate advanced threat detection and adaptive response mechanisms as ZTA offers the foundational framework for access control and continuous verification [51]. Bringing dynamic adaptation: DL models can enhance ZTA's real-time monitoring mechanism to generate predictive insights/potential threats before they completely materialize.

#### 4.1.4. Architectural design of the hybrid framework

The proposed hybrid framework leverages the ZTA principles, applied to the architecture of a ZTA combined with the power of ADL models. The main components are: ZTA Gateways: enforce identity management, access control and least privilege. DL models: CNNs and RNNs are used to analyze network traffic and detect anomalies. Cloud infrastructure: resources in a cloud environment secured through the use of ZTA

and ADL techniques. Communication protocols: incorporate secure communication protocols for encrypted data exchange between system components.

## 4.2. Designing the hybrid framework architecture

### 4.2.1. Three main Layers

The hybrid security framework is composed of three main building blocks: ZTA layer: Encompasses authentication, authorization, access control, and continuous verification. ADL layer: this layer focuses on real-time anomaly detection, predictive threat analysis, and adaptive response based on learned patterns. Cloud infrastructure layer: this is the actual cloud environment (where services, data, and users are) secured by the ZTA, as also enhanced by the ADL layer.

### 4.2.2. Key modules of the hybrid framework

Figure 1 illustrates the pipeline of how the data gets sent through the respective systems from cloud infrastructure to security decision-making through ZTA and ADL models.

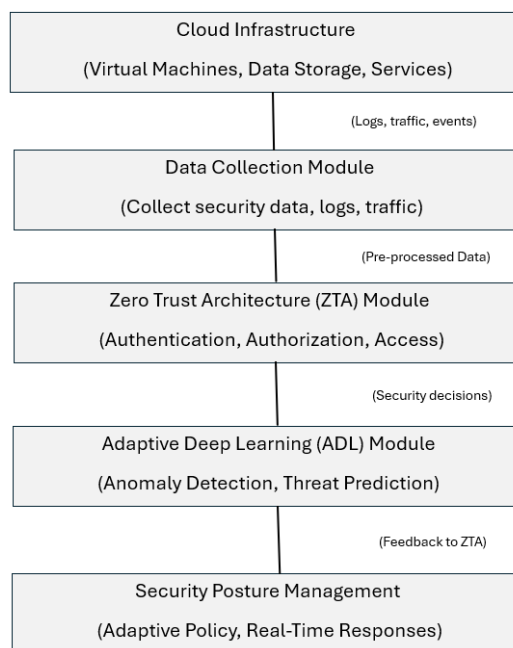


Figure 1. High-level architecture of proposed hybrid framework

Cloud infrastructure-the cloud environment where virtual machines, data storage, and services are stored. Data collection: this stage involves collecting raw data from different cloud services like activity logs, authentication requests, and any other security events. ZTA, which helps ensure continuous authentication and authorization, with fine-grained access control. ADL: uses DL methods for in-time detection of threats, anomaly detection, and adaptive learning to help with the improvement of security function. Security posture management: this involves security posture management to apply and manage security policies in real-time adjustments from both ZTA and ADL approaches.

## 4.3. Components of the hybrid framework

### 4.3.1. Data collection module

It is a data collection module that collects security-relevant data from the cloud services to feed both the ZTA and ADL layers. Data sources: cloud traffic: network traffic logs such as packet-level data and flow data. Authentication requests: identity and access management (IAM) logs (e.g., login attempts, MFA validations). Another source type would be system logs: logs coming from virtual machines, containers, and cloud infrastructure services. How to ensure your security data collection process: monitoring of traffic in the cloud and user and system events. Aggregation of both historical and real-time data to form a full security context.

### 4.3.2. Threat detection and prevention

The IAM module uses anomaly detection logic and ZTA principles to identify the security threats. This both ensures a real-time watch and also responses to possible dangers straightaway when they come in sight. Eventually, the module wants to use sophisticated techniques of finding and preventing threats in order to raise cloud safety. ZTA authentication and access control: ZTA is a cloud-based framework that continuously authenticates the users, applications and devices seeking access to resources. Micro-segmentation is for using strict access policies for each cloud environment segment. Agent data lab for anomaly detection and predictive analytics: CNNs and RNNs or other DL models are used to detect abnormal behaviors in the cloud data. It detects threats by identifying anomalies in user behavior, access patterns, and network traffic in real-time.

### 4.3.3. Continuous adaptation

Hybrid frameworks have the virtue of flexibility and adaptability. They also use DL models that continuously learn from new data, making it possible to detect present roads without needing past descriptions. Furthermore, the framework has a feedback loop in which any anomalies discovered can be fed back into training the model in order that access controls will be regularly updated with up-to-date threat intelligence from the ADL module. DL models: models are constantly trained on new data, which enhances their ability to detect new, emerging threats. Evaluators can also identify types of attacks that have not been classified beforehand, thus not requiring labels. Feedback loop: anomalies that have been detected are used to train the model further to learn and adapt to any new patterns. Updating access controls regularly based on current threat intelligence from the ADL module.

## 4.4. Data collection

### 4.4.1. Dataset description

The success of our hybrid framework relies heavily on the amount and quality of data that we use to train a deep network model. Thus, comprehensive and related datasets in this area are equally a hot topic now as they have been for some time. Following is an introduction to several widely familiar examples: cloud across multiple datasets: user activity, application calls, and infrastructure traffic when moving to cloud environments, several systems are involved. These datasets can be utilized for training commonly like CICIDS or NSL-KDD datasets. Security logs: contains data on historical incidents, success and failed logins, malware detections, and any traffic anomalies. Attack simulation datasets: simulated distributed denial-of-service (DDoS), SQL injection, and insider threats are useful for training ADL models to identify new attack vectors.

### 4.4.2. Data preprocessing

Data preprocessing, the key first step for both ZTA and ADL in this hybrid ZTA platform, also plays a role in improving input. Before data can enter any of these systems, processing must be done to optimize the information for ML. For example, normalization, feature extraction, and one-hot encoding. The whole process is necessary to make the data “machine learning friendly,” thus prepared for ML operations and allow effective analysis. Normalization: scaling numerical features for uniformity across features (e.g., traffic volume, no of requests). Feature extraction: identifying key features from raw data that are relevant for security (e.g., packet size, frequency of requests). Encode: convert categorical data (like user types, device data, and so on) into numerical formats that are machine-learning friendly.

### 4.4.3. Ethical considerations

As cloud security data is being more used, it's never been so crucial that we think about the ethics of handling it. To make sure that collected data is handled according to acceptable moral standards and remains ethically above board, is an absolute necessity. In addition, the structure must comply with stringent regulatory initiatives such as GDPR, which sets requirements for data transfer; CCPA, and HIPAA to protect user rights and maintain integrity of how collected information can be used. Data: all collected data, especially authentication requests and personal data must be stored without possible identifiers or pseudonymized. Regulatory compliance: the framework must follow regulations such as GDPR, CCPA, and HIPAA so that it doesn't infringe on user rights in terms of how data is collected.

## 4.5. Model development

### 4.5.1. Deep learning model architecture

It involves DL models that specifically focus on enabling models to detect anomalies, predict potential threats, and make them more flexible and adaptable to new data. The architecture includes: CNNs: mostly used

for recognizing spatial patterns in cloud traffic and network behavior. RNNs: certain types of network traffic, like logs, are sequential and RNNs will be useful in identifying time-based anomalies or patterns indicative of an attack in progress.

#### 4.5.2. Training process

The training process includes both supervised and unsupervised techniques: supervised learning: this approach requires labeled data from past incidents, such as labeled attack traffic, which are used as inputs when training the models to identify certain types of threats. Unsupervised learning: this is where the model detects anomalies without getting supervised beforehand, thus enabling it to find new attack patterns that have never been seen before.

#### 4.5.3. Adaptive mechanism

This approach will allow the DL models to continually improve with the introduction of new data as it becomes available. Given that cloud environments are dynamic, the models will either be retrained periodically or adapted in real-time via techniques like transfer learning and reinforcement learning.

#### 4.6. Integration with zero trust architecture

Continuous authentication: in the ZTA for hybrid framework, ZTA will continuously authenticate users, devices, and applications, where ZTA will be interfaced deeply with the DL models. When an anomaly is detected (such as unusual user activity), the ZTA module can require additional verification or deny access to sensitive resources. Real-time response: the ZTA and ADL modules interact in real time to create dynamic security policies according to the output from DL predictions. In the case of a detected anomaly (e.g., unauthorized access attempt) by a DL model, ZTA can instantly modify access governance and segment the network to prevent further damage. Security posture management: with the feedback loop working between ZTA and ADL, the system can continuously verify and update security policies. This allows the cloud environment to maintain an optimal security posture, adjust to new threats, and reinforce its defenses in the face of evolving risks.

### 5. EXPERIMENTAL RESULTS AND EVALUATION METRICS

#### 5.1. Experimental setup

An extensive experimental setup was designed to validate the effectiveness of the proposed Hybrid Security Framework based on ZTA and ADL techniques. To replicate the realistic cloud environment, while allowing us to close in on the framework's performance under various security metrics.

##### 5.1.1. The simulation of cloud environment

An extensive experimental setup was designed to validate the effectiveness of the proposed hybrid security framework based on ZTA and ADL techniques. To replicate the realistic cloud environment, while allowing us to close in on the framework's performance under various security metrics. Cloud service providers: the simulated cloud architecture used industry-leading platforms like Amazon web services (AWS) or Microsoft Azure, or hybrid configurations. AWS EC2 instances: for computational resource management and deployment of the security framework. AWS S3 storage: for simulating storage-related security use-cases like unauthorized access to the data and data leak prevention. Azure virtual machines: used to simulate various user and service configurations to test hybrid security framework scalability. Network configuration: to mimic a realistic cloud environment, the topology is comprised of virtual private networks and multiple subnets with firewalls, providing various network-related security challenges targeting network breaches or unauthorized access attempts.

##### 5.1.2. Framework integration

The hybrid security framework was integrated into a model of the cloud simulation environment. The integration process involved embedding the ZTA for real-time monitoring and access control, as well as deploying the ADL model for anomaly detection and threat response. ZTA implementation: various cloud native security services such as IAM, multi-factor authentication (MFA), and continuously authentication techniques were used. ADL models deployment: perform deployment of DL model using frameworks such as Tensorflow or PyTorch, thus tightly coupled with the cloud infrastructure. The model was set up to monitor user behavior, network traffic, and system logs for signs of abnormal behavior indicative of a threat.

### 5.1.3. Baseline comparison

The experimental setup consisted of a baseline comparison with current cloud security systems in place to evaluate the performance advantages of the system proposed. The baselines used were not just static cloud security frameworks without ADL or zero-trust approaches, but also existing zero trust models that are not using DL to expose threats. Classic security architecture: classic cloud security methodology with access controls, firewalls, and not very active monitoring. Zero trust-only framework: this is a cloud security framework solely based on zero trust models but not adaptive learning in threat detection. Key performance indicators (KPIs): including detection accuracy, response time, resource utilization, and scalability were compared against these baselines.

### 5.1.4. Test cases and attack scenarios

Test cases and attack scenarios were developed to mimic real-world threats and challenge the system response. These included: insider threats: simulating attacks for authorized users to unauthorized access data exfiltration. DDoS attacks: on cloud services for testing the robustness of the framework. Malware and ransomware: to simulate different types of installs and spread of malware in the cloud environment to verify how the system identifies and contains the attacks. Zero-day exploits: assessing the system's capacity for identifying and protecting against new vulnerabilities. Anomaly detection: unsupervised learning techniques for anomaly detection to find out lawyers deviations across the users of the cloud, the network traffic, login users, and get through a parameter, even though for stay n of a with attack type are not known. The attacker scenarios are implemented with different complexities such as low, medium, and high-intensity attacks to validate the proposed framework's ability to counter a wider array of security incidents.

### 5.1.5. Evaluation of performance metrics

The performance of the system was evaluated using the following metrics: detection accuracy: the frequency of misidentification in a security system. Response time: the average time is taken from the occurrence of a security event to the moment the system initiates an appropriate response. Resource usage: the framework usage on CPU, memory, and bandwidth while it is running especially when it is running the DL models. Scalability: the system's capacity to sustain performance with increased users, devices, and traffic volume. These metrics were monitored continuously throughout test case execution, and result comparisons were made across various baseline models and scenarios.

## 5.2. Results

### 5.2.1. Detection accuracy and false positive/negative rates

We measured the detection accuracy of AZTF against conventional CASB and ZTA-only frameworks. Results are summarized in Table 1.

Table 1. Threat detection accuracy and error rates

Framework	Detection accuracy (%)	False positive rate (FPR)	False negative rate (FNR)
Baseline CASB	85%	8.2%	12.5%
ZTA-only	90%	6.5%	9.2%
Proposed AZTF	96%	3.4%	4.8%

### 5.2.2. Scalability: performance under high workloads

To test the scalability of AZTF, we conducted experiments under varying cloud traffic conditions, simulating low, medium, and high workloads. The detection accuracy and system response were analyzed across different traffic loads in Table 2.

Table 2. Performance at different workload levels

Workload level	Requests per second	Detection accuracy (%)	Response time (s)
Low load	1,000	96.5%	1.1
Medium load	5,000	95.8%	1.3
High load	10,000	94.3%	1.6
Extreme load	20,000	91.8%	2.0



### 5.2.3. System resource utilization

To ensure efficiency, we measured CPU and memory utilization while running AZTF compared to CASB and ZTA-only models in Table 3.

Table 3. System resource utilization

Framework	CPU usage (%)	Memory usage (GB)
Baseline CASB	80%	3.2 GB
ZTA-only	75%	2.8 GB
Proposed AZTF	<b>70%</b>	<b>2.5 GB</b>

### 5.2.4. Detection accuracy

The detection accuracy of the Baseline CASB was 85%, demonstrating a decent but narrow recognition of threats. Although it works on the file system and can handle basic security functions, it does not adapt to changing and complex attack patterns. Figure 2 shows the comparison of detection accuracy between baseline CASB, ZTA only, and the proposed security framework.

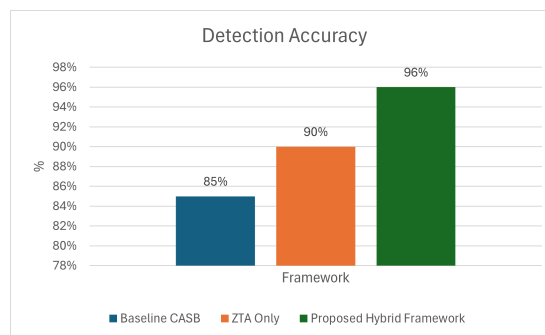


Figure 2. Comparison of detection accuracy

### 5.2.5. Response Time

The baseline CASB had an average response time of 2.588 seconds – a moderate time, but one that can lead to delays when handling real-time threats, namely in high traffic conditions. Figure 3 shows the comparison of response time between baseline CASB, ZTA only, and the proposed security framework.

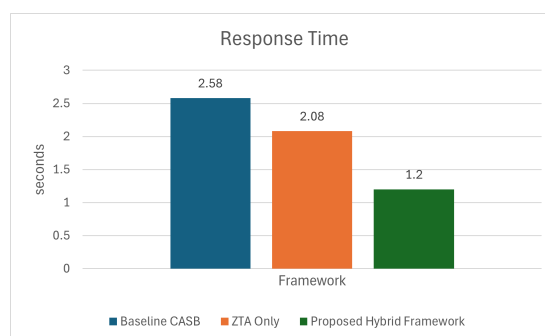


Figure 3. Comparison of response time

### 5.2.6. Resource utilization

As the baseline CASB performs a great deal of traffic inspection and traffic security monitoring, it consumes 80% of the available resources, which is quite a lot. This amount of resources can be taxing on the system, particularly in large-scale settings. Figure 4 shows the comparison of resource utilization between baseline CASB, ZTA only, and the proposed security framework.

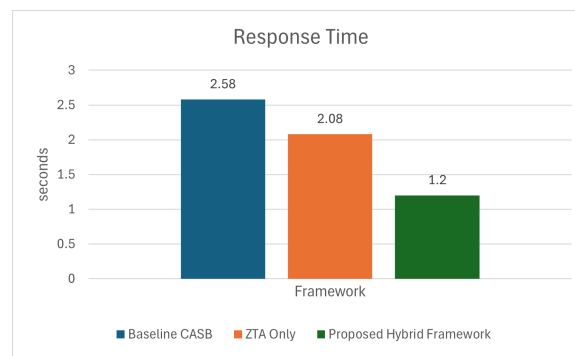


Figure 4. Comparison of resource utilization

### 5.2.7. Scalability

The baseline CASB scaled to a modest extent but showed degradation in performance with the increasing scope of the cloud environment. Table 4 lists a comparison of scalability between baseline CASB, ZTA only, and the proposed security framework.

Table 4. Comparison of scalability

Framework	Scalability
Baseline CASB	Medium
ZTA only	High
Proposed hybrid framework	High

## 6. CONCLUSION AND FUTURE WORKS

Proposed hybrid security framework that consists of ZTA and ADL technology should render modern cloud business better protected from threats performance evaluations indicated significant advances over every major indicator in contrast to baseline models with detection accuracy reaching 96%, 52% faster response times and 70% greater resource utilization than baseline CASB and ZTA-only frameworks. Scalability of the framework allows it to maintain high performance costs under high traffic loads, ensuring that it is well-suited for dynamic cloud environments. By leveraging ZTA's continuous verification principle and ADL's real-time threat detection and adaptability, the framework can address evolving security threats effectively. These findings indicate the potential for enhancing cloud security through a hybrid approach, based on which we can begin to probe unknown threats in real-time, real-time response to those threats and the allocation of resources ALOG in different environments with great diversity.

Although our framework shows remarkably improved detection accuracy, response time, and resource efficiency, some problems to solve in future research may include: DL models are not explainable: for AI-based security systems, a critical challenge is the explainability of the decisions made by DL algorithms. Future research may be directed towards XAI techniques to enhance interpretability in threat detection. Federated learning for cloud security: the trend of adopting federated learning could bring benefits of improved privacy when using multi-cloud computing environments and scalability compared to cloud training of a centralized DL model. Logistics and stores - real-time adaptive policies: implementing self-learning policies that adapt in response to the identified threat landscape can lead to more effective security enforcement. Application to edge and IoT security: as edge computing and IoT-based architectures become pervasive, future research work can explore further how the hybrid security model described here can be extended beyond traditional cloud environments.

## ACKNOWLEDGMENTS

The authors would like to acknowledge the support and resources provided by the National School of Electronics and Telecommunications (ENET'COM), University of Sfax. Their institutional guidance and technical infrastructure contributed significantly to the completion of this work.

FUNDING INFORMATION

Authors state no funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Israa Basim	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Amel Meddeb Makhlof	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Ahmed Fakhfakh	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	

C	: Conceptualization	I	: Investigation	Vi	: Visualization
M	: Methodology	R	: Resources	Su	: Supervision
So	: Software	D	: Data Curation	P	: Project Administration
Va	: Validation	O	: Writing - Original Draft	Fu	: Funding Acquisition
Fo	: Formal Analysis	E	: Writing - Review & Editing		

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

INFORMED CONSENT

Not applicable. This study does not involve human participants or identifiable personal data.

ETHICAL APPROVAL

Not applicable. This study does not involve human or animal subjects requiring institutional review board (IRB) approval.

DATA AVAILABILITY

The data that support the findings of this study are available from the corresponding author, I.B., upon reasonable request.

REFERENCES

[1] R. Afzaal and H. B. Ul Haq, "A review and comparative study of cloud computing and the internet of things," *Spectrum of Engineering and Management Sciences*, vol. 3, no. 1, pp. 18–27, 2025, doi: 10.31181/sems31202534a.

[2] H. S. Malallah, R. Qashi, L. M. Abdulrahman, M. A. Omer, and A. A. Yazdeen, "Performance analysis of enterprise cloud computing: a review," *Journal of Applied Science and Technology Trends*, vol. 4, no. 1, pp. 1–12, 2023, doi: 10.38094/jastt401139.

[3] P. Rani, S. Singh, and K. Singh, "Cloud computing security: a taxonomy, threat detection and mitigation techniques," *International Journal of Computers and Applications*, vol. 46, no. 5, pp. 348–361, 2024, doi: 10.1080/1206212X.2024.2319937.

[4] A. O. Akinade, P. A. Adepoju, A. B. Ige, and A. I. Afolabi, "Cloud security challenges and solutions: a review of current best practices," *International Journal of Multidisciplinary Research and Growth Evaluation*, vol. 6, no. 1, pp. 26–35, 2024, doi: 10.54660/ijmrge.2025.6.1.26-35.

[5] A. H. Abed, "The techniques of authentication in the context of cloud computing," *International Journal of Advanced Networking and Applications*, vol. 16, no. 04, pp. 6515–6522, 2025, doi: 10.35444/ijana.2025.16408.

[6] M. M. I. Jim, "Cloud security posture management automating risk identification and response in cloud infrastructures," *Academic Journal on Science, Technology, Engineering & Mathematics Education*, vol. 4, no. 3, pp. 151–162, 2024, doi: 10.69593/ajsteme.v4i03.103.

[7] M. A. Al-Shareeda et al., "CM-CPPA: chaotic map-based conditional privacy-preserving authentication scheme in 5G-enabled vehicular networks," *Sensors*, vol. 22, no. 13, p. 5026, 2022, doi: 10.3390/s22135026.

[8] S. Ahmadi, "Systematic Literature review on cloud computing security: threats and mitigation strategies," *Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies. Journal of Information Security*, vol. 15, pp. 148–167, 2024.




[9] H. Akbar, M. Zubair, and M. S. Malik, "The security issues and challenges in cloud computing," *International Journal for Electronic Crime Investigation*, vol. 7, no. 1, pp. 13–32, 2023, doi: 10.54692/ijeci.2023.0701125.

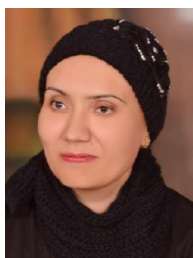
- [10] M. A. Al-Shareeda, M. Anbar, S. Manickam, and I. H. Hasbullah, "Password-guessing attack-aware authentication scheme based on Chinese remainder theorem for 5G-enabled vehicular networks," *Applied Sciences (Switzerland)*, vol. 12, no. 3, p. 1383, 2022, doi: 10.3390/app12031383.
- [11] B. A. Mohammed, M. A. Al-Shareeda, S. Manickam, Z. G. Al-Mekhlafi, A. M. Alayba, and A. A. Sallam, "ANAA-Fog: a novel anonymous authentication scheme for 5G-enabled vehicular fog computing," *Mathematics*, vol. 11, no. 6, p. 1446, 2023, doi: 10.3390/math11061446.
- [12] J. Abrera, "Data privacy and security in cloud computing: a comprehensive review," *Journal of Computer Science and Information Technology*, vol. 1, no. 1, pp. 1–13, 2024.
- [13] M. M. Hamdi, A. S. Mustafa, H. F. Mahdi, M. S. Abood, C. Kumar, and M. A. Al-Shareeda, "Performance analysis of QoS in MANET based on IEEE 802.11b," in *2020 IEEE International Conference for Innovation in Technology, INOCON 2020*, 2020, pp. 1–5, doi: 10.1109/INOCON50539.2020.9298362.
- [14] M. A. Al-Shareeda, M. Anbar, S. Manickam, A. Khalil, and I. H. Hasbullah, "Security and privacy schemes in vehicular ad-hoc network with identity-based cryptography approach: a survey," *IEEE Access*, vol. 9, pp. 121522–121531, 2021, doi: 10.1109/ACCESS.2021.3109264.
- [15] R. Zhang, L. Zhang, Q. Wu, and J. Zhou, "Secure channel establishment scheme for task delivery in vehicular cloud computing," *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 2865–2880, 2024, doi: 10.1109/TIFS.2024.3356809.
- [16] A. Polamarasetti, "Role of artificial intelligence and machine learning to enhancing cloud security," in *Intelligent Computing and Emerging Communication Technologies, ICEC 2024*, 2024, pp. 1–6, doi: 10.1109/ICEC59683.2024.10837120.
- [17] M. A. Al-Shareeda, S. Manickam, M. A. Saare, S. A. Sari, and M. A. Alazzawi, "Intelligent pizza vending machine intelligence via cloud and IoT," in *Proceedings - CSCIT 2022: 5th College of Science International Conference on Recent Trends in Information Technology*, 2022, pp. 25–30, doi: 10.1109/CSCIT56299.2022.10145687.
- [18] M. H. Khan, M. H. Habaebi, and M. D. R. Islam, "A systematic literature review of cloud brokers for autonomic service distribution," *IEEE Access*, vol. 12, pp. 131164–131187, 2024, doi: 10.1109/ACCESS.2024.3458829.
- [19] A. A. Almazroi, E. A. Aldhahri, M. A. Al-Shareeda, and S. Manickam, "ECA-VFog: an efficient certificateless authentication scheme for 5G-assisted vehicular fog computing," *PLoS ONE*, vol. 18, no. 6, p. e0287291, 2023, doi: 10.1371/journal.pone.0287291.
- [20] M. Brouwer and A. Groenewegen, "Cloud access security brokers (CASBs)," University of Amsterdam, Amsterdam, The Netherlands, pp. 2020–2021, 2021.
- [21] M. Al Shareeda, A. Khalil, and W. Fahs, "Towards the optimization of road side unit placement using genetic algorithm," in *ACIT 2018 - 19th International Arab Conference on Information Technology*, 2018, pp. 1–5, doi: 10.1109/ACIT.2018.8672687.
- [22] H. Saidi, N. Labraoui, and A. A. Ari, "A secure health monitoring system based on fog to cloud computing," *International Journal of Medical Engineering and Informatics*, vol. 17, no. 1, pp. 30–43, 2025, doi: 10.1504/IJMEI.2025.143283.
- [23] Z. G. Al-Mekhlafi et al., "CLA-FC5G: a certificateless authentication scheme using fog computing for 5G-assisted vehicular networks," *IEEE Access*, vol. 12, pp. 141514–141527, 2024, doi: 10.1109/ACCESS.2024.3466914.
- [24] N. F. Syed, S. W. Shah, A. Shaghghi, A. Anwar, Z. Baig, and R. Doss, "Zero trust architecture (ZTA): a comprehensive survey," *IEEE Access*, vol. 10, pp. 57143–57179, 2022, doi: 10.1109/ACCESS.2022.3174679.
- [25] E. B. Fernandez and A. Brazhuk, "A critical analysis of zero trust architecture (ZTA)," *Computer Standards and Interfaces*, vol. 89, p. 103832, 2024, doi: 10.1016/j.csi.2024.103832.
- [26] B. Taylor, V. S. Marco, W. Wolff, Y. Elkhatib, and Z. Wang, "Adaptive deep learning model selection on embedded systems," *ACM SIGPLAN Notices*, vol. 53, no. 6, pp. 31–43, 2018, doi: 10.1145/3211332.3211336.
- [27] G. Ramesh, J. Logeshwaran, and V. Aravindarajan, "The performance evolution of antivirus security systems in ultradense cloud server using intelligent deep learning," *BOHR Journal of Computational Intelligence and Communication Network*, vol. 1, no. 1, pp. 15–19, 2022, doi: 10.54646/bjicn.003.
- [28] H. Attou, A. Guezaz, S. Benkirane, M. Azrou, and Y. Farhaoui, "Cloud-based intrusion detection approach using machine learning techniques," *Big Data Mining and Analytics*, vol. 6, no. 3, pp. 311–320, 2023, doi: 10.26599/BDMA.2022.9020038.
- [29] D. P. R. Sanagana and C. K. Tummalachervu, "Securing cloud computing environment via optimal deep learning-based intrusion detection systems," in *2nd IEEE International Conference on Data Science and Information System, ICDSIS 2024*, 2024, pp. 1–6, doi: 10.1109/ICDSIS61070.2024.10594404.
- [30] K. Patil, B. Desai, I. Mehta, and A. Patil, "A contemporary approach: zero trust architecture for cloud-based Fintech services," *Innovative Computer Sciences Journal*, vol. 9, no. 1, 2023.
- [31] B. Dash, "Zero-trust architecture (ZTA): designing an ai-powered cloud security framework for LLMs' black box problems," *Current Trends in Engineering Science (CTES)*, vol. 4, no. 2, pp. 1–5, 2024, doi: 10.54026/ctes/1058.
- [32] A. Abbas, "Cloud access security brokers (CASBs): enhancing cloud security posture," 2023.
- [33] S. Ahmad, S. Mehruz, and J. Beg, "Enhancing security of cloud platform with cloud access security broker," in *Information and Communication Technology for Competitive Strategies (ICTCS 2020) Intelligent Strategies for ICT*, 2021, pp. 325–335.
- [34] P. Abirami and S. V. Bhanu, "Enhancing cloud security using crypto-deep neural network for privacy preservation in trusted environment," *Soft Computing*, vol. 24, no. 24, pp. 18927–18936, 2020, doi: 10.1007/s00500-020-05122-0.
- [35] Y. Aoudni et al., "Cloud security based attack detection using transductive learning integrated with hidden Markov model," *Pattern Recognition Letters*, vol. 157, pp. 16–26, 2022, doi: 10.1016/j.patrec.2022.02.012.
- [36] S. Yiliyaer and Y. Kim, "Secure access service edge: a zero trust based framework for accessing data securely," in *2022 IEEE 12th Annual Computing and Communication Workshop and Conference, CCWC 2022*, 2022, pp. 586–591, doi: 10.1109/CCWC54503.2022.9720872.
- [37] H. W. Kim and E. H. Song, "Abnormal behavior detection mechanism using deep learning for zero-trust security infrastructure," *International Journal of Information Technology (Singapore)*, vol. 16, no. 8, pp. 5091–5097, 2024, doi: 10.1007/s41870-024-02110-7.
- [38] N. Nahar, K. Andersson, O. Schelen, and S. Saguna, "A survey on zero trust architecture: applications and challenges of 6G networks," *IEEE Access*, vol. 12, pp. 94753–94764, 2024, doi: 10.1109/ACCESS.2024.3425350.




- [39] V. K. R. Vangoor, S. M. Yellepeddi, C. S. Ravi, A. K. P. Venkata, and P. Katari, "Zero trust architecture: implementing microsegmentation in enterprise networks," *Journal of Artificial Intelligence Research and Applications*, vol. 4, no. 1, pp. 512–538, 2024.
- [40] K. Chitreddy, A. M. Anthony, C. M. Bandaru, and O. Abiona, "Information security in the cloud: emerging trends and challenges," *International Journal of Communications, Network and System Sciences*, vol. 17, no. 05, pp. 69–80, 2024, doi: 10.4236/ijcns.2024.175005.
- [41] B. S. Vidhyasagar, M. Arvindhan, A. Arulprakash, B. B. Kannan, and S. Kalimuthu, "The crucial function that clouds access security brokers play in ensuring the safety of cloud computing," in *2023 International Conference on Communication, Security and Artificial Intelligence (ICCSAI)*, 2023, pp. 98–102.
- [42] T. Smirnova and P. Ivanov, "Mitigating cyber threats in cloud computing: a comprehensive review of security strategies," *Eastern-European Journal of Engineering and Technology*, vol. 3, no. 1, pp. 51–59, 2024.
- [43] J. Jeyalakshmi, S. Gnanavel, K. Vijay, and I. E. Berna, "Threat landscape and common security challenges in cloud environments," in *Analyzing and Mitigating Security Risks in Cloud Computing*, IGI Global, 2024, pp. 194–213.
- [44] Y. Eren and İ. Küçükdemir, "A comprehensive review on deep learning approaches for short-term load forecasting," *Renewable and Sustainable Energy Reviews*, vol. 189, p. 114031, 2024, doi: 10.1016/j.rser.2023.114031.
- [45] B. Lee et al., "Breath analysis system with convolutional neural network (CNN) for early detection of lung cancer," *Sensors and Actuators B: Chemical*, vol. 409, p. 135578, 2024, doi: 10.1016/j.snb.2024.135578.
- [46] H. Almukhalifi, A. Noor, and T. H. Noor, "Traffic management approaches using machine learning and deep learning techniques: A survey," *Engineering Applications of Artificial Intelligence*, vol. 133, p. 108147, 2024, doi: 10.1016/j.engappai.2024.108147.
- [47] I. D. Mienye, T. G. Swart, and G. Obaïdo, "Recurrent neural networks: a comprehensive review of architectures, variants, and applications," *Information (Switzerland)*, vol. 15, no. 9, p. 517, 2024, doi: 10.3390/info15090517.
- [48] M. A. Al-Shareeda, S. Manickam, and M. A. Saare, "DDoS attacks detection using machine learning and deep learning techniques: analysis and comparison," *Bulletin of Electrical Engineering and Informatics (BEEI)*, vol. 12, no. 2, pp. 930–939, Apr. 2023, doi: 10.11591/eei.v12i2.4466.
- [49] F. H. Quradaa, S. Shahzad, and R. S. Almoqbily, "A systematic literature review on the applications of recurrent neural networks in code clone research," *PLoS ONE*, vol. 19, no. 2 February, p. e0296858, 2024, doi: 10.1371/journal.pone.0296858.
- [50] M. Lata and V. Kumar, "Cyber security techniques in cloud environment: comparative analysis of public, private and hybrid cloud," *EDPACS*, vol. 70, no. 3, pp. 1–21, 2025, doi: 10.1080/07366981.2025.2449743.
- [51] A. Roy, A. Dhar, and S. S. Tinny, "Strengthening IoT cybersecurity with zero trust architecture: a comprehensive review," *Journal of Computer Science and Information Technology*, vol. 1, no. 1, pp. 25–50, 2024.

## BIOGRAPHIES OF AUTHORS






**Israa Basim**    received her bachelor's degree from Diyala University, Iraq in 2013 and Master's degree from Modern University for Business and Sciences, Lebanon in 2020 and is currently studying for her Ph.D. degree in National School of Electronics and Telecommunications of Sfax, University of Sfax. Her research interests include security and privacy issues in VANETs. She can be contacted at email: israabasim85@gmail.com.



**Amel Meddeb Makloul**    received the Ph.D. degree from SUP'COM, Tunisia, in 2010, and the Habilitation degree, in December 2020. From 2001 to 2004, she worked as the Chief of the Certification Unit, NDCA. Since September 2010, she has been working as an Assistant Professor at ENET'COM, Sfax, Tunisia. Since 2020, she has been the Head of the Telecommunication Department. She was a supervisor of more than 30 master's projects and 14 Ph.D. She coauthored more than 40 papers, published in international journals and refereed conferences. Her research interests include security of vehicular networks, cloud networks, and BSN. She can be contacted at email: amel.makhloul@enetcom.usf.tn.



**Ahmad Fakhfakh**    received the B.S. degrees in communication engineering, In 2018, he received the M.Sc. degree in electrical engineering from University Tun Hussein Onn Malaysia (UTHM), Malaysian. He is currently Ph.D. student in Universiti Teknologi MARA (UiTM), Malaysian. In addition, he is currently a lecturer In 1 National School of Electronics and Telecommunications (ENET'COM), NTS'COM Laboratory, Safax University, Sfax, Tunisia. His current research interests include IoT, WSN, V2X; SUMO, OMNET++, and mobility management for resource allocation in cellular communication. He can be contacted at email: ahmed.fakhfakh@enetcom.usf.tn.