ESP-JETA
ESP Journal of Engineering & Technology Advancements
ISSN: 2583-2646 / Volume 6 Issue 1 February 2026
Paper Id: JETA-V6I1P107 / Page No: 55-64

Original Article

Advances AI-Enabled Identification of Threats within Zero-Trust Architectures for Secure Cloud Infrastructures: A Comprehensive Survey

Rajendra Prasad Sola
IT Project Manager, Accenture, Independent Researcher, India.

Received Date: 23 January 2026 Revised Date: 02 February 2026 Accepted Date: 06 February 2026

Abstract: *The cloud computing has become a significant component of the majority of the current digital infrastructures. But with its extensive usage has come several complicated security challenges which are difficult to address using the traditional models of depending on perimeters. Among the effective ways of addressing these threats is the concept of Zero Trust Architecture (ZTA), which is premised upon the idea of never trust, always verify. Simultaneously, it is possible to find more complex and unknown cyber threats in the dynamic cloud environment with great potential of AI and ML technologies. The survey provides an elaborate account of the AI-based threat detection systems deployed on Zero Trust Architectures to secure cloud systems. It discusses the fundamental concepts of ZTA, its major architectural layers and plans of its implementation in the cloud ecosystems. The paper also examines the ML,DL and reinforcement-based techniques critically that are used in intrusion detection, anomaly detection and automatic response to security. The gap in the research that is filled by this survey analysis that uses AI intelligence and the zero trust paradigm allows understanding the future trend, illuminates the future direction, and course when creating resilient, flexible, and saleable cloud security systems.*

Keywords: *Zero Trust Architecture, Cloud Security, Threat Detection, Machine Learning, Deep Learning, Reinforcement Learning, Cybersecurity.*

I. INTRODUCTION

The use of cloud applications and platforms has transformed the modern computing to be flexible, scalable and efficient [1]. The cloud provides a viable infrastructure to the current business regardless of it being web application creation, data analysis, or enterprise implementation. The advent of cloud computing has transformed immensely the way businesses are being done as well as how they are delivering their services. Cybersecurity paradigm has undergone a paradigm shift in recent times, particularly as businesses are switching single-pane and on-premises models to cloud-based models, which are dynamic [2]. Past models of perimeter in which network protection was largely based on the capabilities to protect network edge with firewalls, VPNs and access control systems are no longer sufficient in an environment where data, users and services flow far beyond a defined network edge. The modern cloud ecosystems are defined in terms of distributed on SaaS, IaaS, and PaaS systems, everywhere-accessable assets, and API-, container-, and serverless technology [3]. The security protocols of the present day world must be more dynamic, smart and responsive to any emerging threats as they occur [4][5]. This situation necessitates the shift of traditional trust models to contextual and identity-based security and re-evaluates the risk posture with behavioral indicators, access context and resource sensitivity on a continuous basis.

These issues are being addressed by the current paradigm of security, which is Zero Trust Architecture (ZTA). This model is consistent with the principles of the Zero Trust Architecture (ZTA) that requires micro-segmentation, ongoing authentication, and the implementation of least-privilege security measures [6]. ZTA may reduce the risks of side movement and unauthorized access by using micro-segmentation, least-privilege access and the strong identity and access control [7]. Regardless of its potential, traditional ZTA applications are not conducive to real world use, particularly to facilitate real time threat environments, allow distribution to scale and minimize operational overhead.

AI comes in with the power to change paradigms here. AI and ML have been demonstrated to be very promising in cybersecurity, in particular, anomaly detection, intrusion prevention, and behavioural analytics [8]. Integrating ZTA allows AI-driven models to make adaptive, real-time decisions about access control based on threats to contextual elements, such as user behaviour, device health, and network anomalies. Besides, AI also increases the scalability of ZTA because it can automate the detection of threats in large, structured, and distributed data settings, which is essential in cloud-native and IoT environments. AI driven zero trust security allows providing effective security to cloud-based applications. A combination of identity-focused controls and AI-based risk assessment safeguards cloud workloads, APIs, and against lateral threat movements in distributed, ever-changing settings by limiting access to authorised users and devices.

A. Structure of Paper

The structure of this paper is as follows. Section II addresses Zero Trust Architecture in clouds. Section III evaluates the cloud infrastructure security environment. Section IV addresses AI-based methods of threat detection. Section V gives a comparative literature review of recent studies. Lastly, Section VI summarizes the paper and provides future research directions.

II. ZERO TRUST ARCHITECTURE: STRATEGIC CONTEXT

Cloud systems rely heavily on trust, but conventional methods of system evaluation have not been successful in instilling the necessary levels of assurance. When it comes to protecting networks, the old perimeter-based strategy just can't keep up with the latest innovations. The "zero trust" approach to network security is based on the tenet that one should never trust anything and should instead check everything frequently. In order to access resources, the access topic must be verified, regardless of whether it is in the internal or external network. The zero trust paradigm has been extensively studied and put into practice due to its ability to meet the increased requirements for network security. The Zero Trust Architecture (ZTA) introduced a whole new perspective on security. Unlike models that rely on trusting users, devices, or applications outside of the network, ZTA does not necessitate such trusting relationships. The first principle guiding ZTA is that there is no need to trust anyone, one need to verify, authorize, and validate any request to access the resources regardless of its source [9]. According to NIST SP 800-207, the ZTA model can strengthen security by applying policies in real-time, micro-segmenting, and using least-privilege access.

A. Core Components of ZTA

Modern security paradigms have undergone a sea change, with the advent of Zero Trust Architecture (ZTA). No user, device, or system—within or outside of an organization—can be trusted by default, and ZTA is based on this reality rather than the assumption that everything inside the network is trustworthy [10]. Figure 1 shows the ZTA conceptual model. It also shows the main parts of this solution, such as policy enforcement points, trust evaluation engines, services for continuous tracking, and secure sources. Based on NIST SP 800-207, this visual aid enables a systematic framework to support the theoretical discussion [11]. It is also important to prioritise lightweight cryptographic algorithms like Elliptic Curve Cryptography, homomorphic encryption, and post-quantum approaches to address technological challenges with limited systems, such as IoT devices, and to guarantee low-cost communication security.

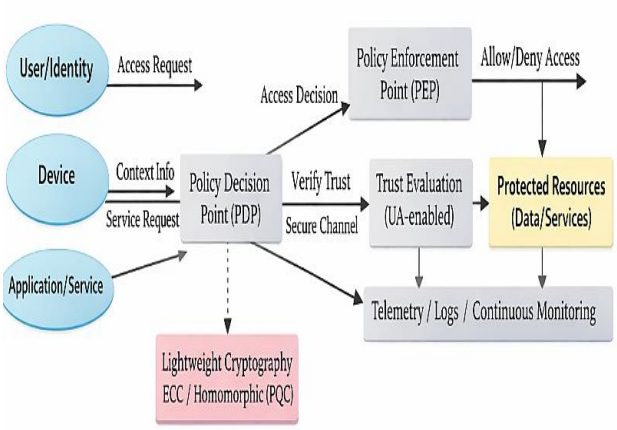

Figure 1 : Conceptual Model of Zero Trust Architecture (ZTA) Adapted from NIST SP 800-207

The following parts are usually included in ZTA models, though implementations may be different:

- Policy Decision Point (PDP): The process decides whether authorisation should be provided according to changing policies.
- Policy Enforcement Point (PEP): Implements the PDP's access decisions by approving or rejecting requests.
- Identity Provider (IdP): Verifies the legitimacy of individuals, gadgets, or services.
- Trust Engine or Context Analyzer: Conducts trust evaluations in real-time based on environmental characteristics such as device health, location, and time.
- Continuous Monitoring Module: Recording and analysing actions to identify unusual occurrences and guide policy revisions.

These parts are modified into lightweight, decentralised designs in ZTA models tailored to the IoTs. One example is the use of Internet of Things gateways as PEPs [12] and PDP decisions being made by engines in the cloud.

B. Zero Trust Basic Assumptions and Principles

ZTA was first suggested in 2010 by Kindervag, who was a lead analyst at Forrester. A zero trust architecture does not rely on location as a basis for security and does not trust any communication. In its place, robust access control with minimal authorisation requirements, security measures for every access, and traffic visualisation and analysis are necessities. Strengthened security is achieved by utilising these approaches, which differ greatly from the conventional perimeter-based security architecture. Zita is based on five fundamental assumptions:

- There is always a risk to the network.
- The entire network is vulnerable to both external and internal threats.
- It is not possible to judge the reliability of a network just by looking at its physical location. .
- Authentication and authorisation should be applied to all devices, users, and network traffic.
- Flexible security rules derived from multiple sources of data are essential.

These four tenets are thought to be upheld by the zero trust model according to the preceding assumptions.

- Authenticate users: Verify the identity of a user by analysing their location, device, and actions to establish their security. Make sure the user is who they say they are by implementing security methods like multifactor authentication.
- Authenticate devices: Use device identity and security to establish access control policies for all devices, whether they are company, BYOD, public, or mobile. The company's resources can only be accessed by authorised endpoints.
- Restrict access and permissions: Allow only the users with the rights they need to do their current tasks by using a role-based access control model on resources after users and devices have been verified.
- Adaptive: A multitude of sources, including people, their devices, and the activities linked to them, are continuously producing data. Modify and alter access controls automatically based on context using machine learning.

C. Implementation of Zero Trust in Cloud Infrastructures

Networking in the cloud is now fundamental to digital infrastructure, changing how businesses store, process, and access their data. Zero trust is typically a response to many trends in corporate networks, such as cloud-based assets, bring-your-own-device rules, remote users, etc., that do not originate from inside an enterprise-owned network perimeter. The focus of zero trust security is on safeguarding resources—accounts, services, workflows, assets, etc.—rather than network segments [13]. Reason being, network location is no longer considered the most important factor in security.

D. Network Segmentation

Zero-trust design also uses network segmentation to keep important assets separate and only let authorised systems and users access them. By focussing on a narrower sector, this feature helps to decrease security breaches. Because of this, it is simple to react to or identify security breaches. Numerous advantages can be gained via network segmentation in ZTA. It follows the philosophy of "never trust, always verify" and limits access to sensitive data, thus reducing the attack surface. It also enhances the performance of the network since the volume of traffic is decreased in each segment. It is also a cause of low latency and rapid response time. The zero-trust model also results in an easier compliance with the network segmentation.

E. Data Protection

Cloud environments are highly sensitive to data protection. To this end, zero trust architecture uses various encryption techniques that guarantee privacy and security. The zero-trust architecture is said to make use of both symmetric and asymmetric encryption [14]. Asymmetric is better concerning security when compared to symmetric where asymmetric is much faster. In case a company loses or destroys its access key, it is possible to recover its privately stored data with the help of the encryption techniques introduced in the ZTA. The network also benefits from encryption when it comes to authentication and meeting regulatory requirements. The overall effect is that it helps businesses keep their data safe and provide secure networks.

F. Identity and Access Management (IAM) Controls

The concept of ZTA when applied to the cloud network infrastructure is associated with a number of strategies that could be implemented to increase the levels of security and the reduction of risks. Strict identity and access management (IAM) policies are one of the aspects of ZTA implementation that is essential. Application of IAM rules enables organisations to restrict network resource access to users, devices, and applications that actually require it as per the principle of least privilege [15]. Network segmentation is also a technique applied by organisations to restrict lateral movement of the network and setting isolation to reduce the effects of the possible security breach.

G. Multi-Factor Authentication (MFA) Mechanisms

The use of the ZTA often presupposes the use of MFA that is another layer of protection that validates the identities of the users. The approach reduces the possibility of unauthorized access even when the credentials are compromised. The capabilities of ZTA have allowed anomaly detection and ongoing monitoring of businesses, thus enabling them to identify a

security threat immediately and act on it. The use of ZTA in cloud network architecture enhances defences, ensures data is more secure and meets the current standards of cybersecurity.

III. CLOUD INFRASTRUCTURE SECURITY LANDSCAPE

The IT world has been capable of revolutionizing cloud computing as it is flexible in its operations, economical and scalable [16]. Strong solutions are needed to guarantee the CIA of sensitive data and systems, as their adoption has brought up significant security issues. The most popular types of assaults, like as data breaches, ransomware, and distributed denial-of-service (DDoS) attacks, as well as insider threats, are made worse by the increasing usage of public clouds, containerisation, and the integration of loT. The intersection of cloud security and container security, edge computing, and inter-cloud trust models opens up new research and innovation [17]. One of the challenges with the security of the cloud is the need to deal with the vulnerabilities of the existing cloud models. As an example, attacks that make use of improperly set up virtual environments and APIs commonly result in unauthorized access and information leaks [18]. Table I provides data that highlights the importance of cybersecurity measures to protect against various types of cyberattacks. Since such attacks are ever on the rise and becoming more advanced, there is a need to be more alert and undertake effective security measures to protect against possible attacks.

Table 1 : Present Cyberattack Trends

Cyberattack Trends	No. of Attacks	Percentage
Malware attacks	5.6 billion	43%
Encrypted threats	3.8 billion	4%
Intrusion attempts	4.8 trillion	20%
Crypto jacking attacks	304.6 million	28%
Ransomware attacks	304.4 million	62%
IoT attacks	56.9 million	66%

A. Threats and Vulnerabilities

The security threats are very many in cloud environments and they undermine confidentiality, integrity and availability [19]. The changing nature of the threat has generated advanced attack vectors against various facets of cloud infrastructures especially application layers, networks and user access. The list of the prominent threats provided in Table II is listed in the form of an infographic below:

Table 2 : Common Cyberthreats and Associated Impacts in Cloud Computing

Threat	Impact
DDoS (Denial of Service)	Overwhelms services with traffic, causing downtime.
DNS Amplification	Leverages open DNS servers to flood a target with response traffic.
SQL Injection	Manipulates database queries, exposing or altering sensitive data.
CSRF (Cross-Site Request Forgery):	Exploits trust between browser and web application to execute unauthorized actions.
Session Hijacking	Steals session cookies to impersonate users and gain unauthorized access.
Ping of Death	Crashes systems with oversized ICMP packets, particularly in unpatched environments.
Slowloris	Keeps server connections open, exhausting resources and blocking legitimate requests.

B. Mitigation Strategies

Cloud computing is still under scrutiny by service owners who feel that there is not a level of maturity in the existing security technologies despite its transformational potential. The fill of this gap cannot be achieved without technical solutions, and it is also necessary to create such complex frameworks that assess and reduce the risks of security. As an example, such frameworks as the Cloud Security Alliance STAR program and ISO/IEC 27017 focus on compliance and governance, promoting the presence of trust in cloud services [20]. Having sufficient policy enforcement and technological innovation, the future of cloud computing can be harmonized to achieve the role of usability and security to continue its expansion and acceptance in the industries.

a) Core Security Techniques

Cloud computing needs a sound underlying security to ensure that sensitive data is safeguarded and that the risks are adequately addressed. This section establishes some of the main basic approaches that are the pillars of cloud security:

i) Encryption

Encryption has been one of the most necessary techniques of protecting information in the cloud. It encrypts the plaintext data with the help of cryptographic keys in a manner that only authorized individuals can decode the encrypted ciphertext to obtain access to confidential information. Such advanced practices like field-specific encryption increase level of security because different keys are used in different data fields. This reduce the chances of large scale compromise in case of a breach. The necessity to find a middle ground between data security and the usability of the SaaS application is one of the unique obstacles that cloud encryption imposes. Multi-key encryption and maintaining the searchability of encrypted datasets are some of the innovations that are being considered to overcome these issues.

ii) Tokenization

Sensitive data in tokenization are substituted with randomly generated values so that the original information is not accessible even in the event of a token breach. In contrast to encryption, tokenized data cannot be brought back to its original state, and it would be a great option to use in immensely sensitive datasets. Ensuring the security of sensitive data, including payment information and personally identifiable information (PII), is a typical practice in the cloud.

iii) Zero-Trust Architectures

ZTA assumes that there is no trust within or outside of the network's perimeter [21]. The process of authentication and authorisation should be done frequently to make sure that each access request is checked. This model can be particularly relevant to prevent insider attacks and unauthorized access in the dynamic clouds. Also, ZTA isolates resources and restricts further lateral movement in the event of a breach in addition to micro-segmentation and identification of devices, which enhances the effectiveness of security.

iv) DevSecOps Integration

DevSecOps offers the software developers the platform to consider security as part of the software development life cycle whereby security is factored in the software development cycle including in the planning and implementation stages [22]. The vulnerabilities can be identified and managed at the early development stage by such techniques as dynamic testing, static code analysis, and runtime monitoring. DevSecOps develops the culture of shared accountability, security as part of agile development practice.

b) Advanced Solutions

The emerging and advanced nature of the challenges that arise in cloud security has led to the need to use advanced solutions which leverage emerging technologies. This section will talk about these new approaches and how they will be revolutionary within the context of the cloud environment security.

- Blockchain for Data Integrity and Security: Blockchain technology is one that involves decentralised ledgers to ensure transactions and records in cloud setups, and the integrity and immutability of the data are guaranteed.
- Cloud-Native Security Tools: There are integrated solutions in cloud that provide and enhance security activities with a wide range [23].
- DevSecOps and Agile Security Integration: DevSecOps is premised to the culture of shared responsibility that the safety component of the software development lifecycle is taken into account at every point throughout its development.
- Automation and Compliance Orchestration: Modern businesses engage AI-based solutions to perform automation of compliance management and ensure regulatory compliance.

C. Emerging Challenges

Cloud computing has emerged as one of the essential infrastructure that any organization in the global world can enjoy, but such high-speed rate of adoption has presented several challenges that need to be addressed. The nature of cloud settings which are both complex and dynamic and may create vulnerabilities also present other issues that are dealt with in this section.

a) Trust and Governance Shared Models

The shared responsibility approach is one of the greatest challenges to cloud security. The consumer does not realize that CSPs are attempting to make the infrastructure safe, and this results in mistrust. Users tend to use CSPs to provide the security of their workloads despite them having the mandate to deal with features like virtual machines, configurations and also user access. These issues are heightened by the poorly aligned expectations and poor communication that lead to the gap in governance and compliance.

b) Complexities of Multi-Cloud Environments

The multi-cloud strategies have brought extensive variety of security practices, compliance standards and business processes [24]. Because there isn't any uniformity throughout providers, security management is more complicated, and new threats including misconfigurations, data breaches, and illegal access have surfaced. The necessity and problem of centralised IAM and standard security rules across platforms.

c) Data Sovereignty and Jurisdictional Issues

The issue of data sovereignty has become a major concern especially in multi-cloud environments. Several areas have different legal and regulatory standards that data storage and processing have to meet. It is also important to note that organizations have to set their way through the contradicting privacy regulations, including the provisions of the European Union (GDPR) and the United States to guarantee their adherence. Any failure in mishandling the cross-border data transfers may lead to harsh fines and penalties.

d) Insecure APIs and Integration Points

The use of APIs in cloud systems is extensively utilized to communicate, and integrate, but poorly managed or configured APIs are a serious attack point. Hackers take advantage of such vulnerabilities and break security measures, steal confidential information, or interfere with services. The necessary measure to counter these risks is to ensure a strong API management and monitoring.

IV. AI-ENABLES THREAT DETECTION TECHNIQUES IN CLOUD ENVIRONMENTS

The rise in the use of technology in most industries has resulted in more emerging cyber threats and attacks, thus, cybersecurity has become a critical issue [25]. The conventional methods of cybersecurity are ineffective in identifying and responding to new types of cyberattacks since their frequency and sophistication have been on the rise [26]. ML and AI are now known to be useful in the context of overcoming these issues as they could potentially improve the functionality of the already in place cybersecurity systems and identify new threats that could not be indicated before [27][28]. The application of AI and ML to cybersecurity has garnered a lot of attention recently, and several studies have investigated this topic. A breakdown of the many securities operations' use of ML and AI is shown in Figure 2.

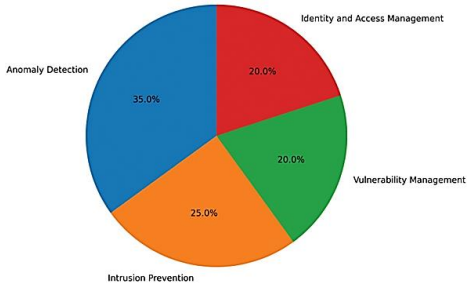

Figure 2 : AI/ML in Security Automation

A. Machine Learning Approaches in Threat Detection

Classification is the bread and butter of supervised learning (and IDS in particular), yet manually labelling data is a laborious and costly ordeal [29]. Clustering, SVM, and KNN are the mainstays of classical ML models used for threat detection.

a) Support Vector Machine (SVM):

Support vector machines can be trained in part by finding the hyperplane in the n-dimensional space of features that maximises margin separation [30]. A minimal number of support vectors regulate the separation hyperplane, allowing SVMs to achieve satisfactory results even with small-scale training data. To the contrary, noise around the hyperplane is a certain way to deceive support vector machines. SVMs truly shine when dealing with linear problems. When dealing with data that is not linear, kernel functions are often used. Implementing a kernel function, which maps the original space to a new space, allows for the splitting of the initial nonlinear data. Keras tricks are commonly used by SVMs and other ML techniques.

b) K-Nearest Neighbour:

The manifold hypothesis forms the basis of KNN's central idea. There is a strong indication that a sample is representative of a class if the majority of its neighbours are also members of that class. As a result, the top k nearest neighbours are the only ones that matter for the categorisation outcome. When it comes to KNN models, the parameter k is king [31]. Overfitting is more likely to occur in a more complicated model when k is less. When k is large, on the other hand, the model becomes less complex and its fitting ability weakens.

c) Clustering:

Clustering relies on similarity theory, which states that data that are very similar should be clustered together, whereas those that are less similar should be clustered apart. Clustering is an unsupervised learning technique that differs from classification. Clustering methods do not necessitate labelled data or prior knowledge, hence the data set needs to be minimal. Clustering methods can be useful for attack detection, although they do need referring to external sources of data.

B. Deep Learning Strategies in Threat Detection

Deep learning models are assemblies of different types of deep networks. This class includes deep neural networks, autoencoders, and convolutional neural networks.

- Autoencoder: A pair of components that make up an autoencoder are the encoder and the decoder. The decoder takes the encoder-extracted features and applies them to the raw data in order to recreate the data. The training process involves a gradual reduction of the divergence between the encoder's input and the decoder's output. The features extracted by the encoder should faithfully represent the data's essence if the decoder can reconstruct the data from them [32]. Keep in mind that no supervised information is needed at any point throughout the process.
- Deep Neural Network: Create multi-layer DNNs with a layer-wise pretraining and fine-tuning approach. Learn the parameters using unlabelled data first in the unsupervised feature learning step of DNN training. Supervised learning then involves training the network with tagged data. Most of DNNs' impressive performance comes from their unsupervised feature learning phase.
- Convolutional Neural Network: CNNs have achieved remarkable success in computer vision because they are designed to emulate the HVS. Alternating convolutional and pooling layers make up a CNN. The features are extracted by means of convolutional layers, and their generalisability is improved by means of pooling layers. Since CNNs can only handle 2D data, the input data must be translated into matrices before they can be trained to detect attacks.

C. Reinforcement Learning

One advanced machine learning technique that enables systems to evolve and adapt dynamically through environmental interaction is RL. The RL-based models can also be utilised to teach autonomous agents to keep an eye out for cyber dangers and react instantly within the context of IoT security. Compared to supervised and unsupervised learning, RL does not use a set of decisions; it constantly increases its decision-making skills using trial and error. IDS that is built on RL has the capability of proactively scaling up security policy, preventing malicious actions, and reducing the impact of attacks on the basis of real-time examination.

V. LITERATURE REVIEW

This section examines literature on AI-enabled threat detection for secure cloud infrastructures. Table III describes the existing benchmarking studies on threat detection for secure cloud infrastructures using AI, focusing on contribution, models and methods, dataset, performance parameters, and notes.

B and Meenakshi (2025) assessed four ML models for zero trust anomaly detection: XGBoost 95.23% of the time, RF 96.48% of the time, and AdaBoost 77.39% of the time when used in conjunction with KNN. RF and "XGBoost" outperform KNN and AdaBoost when analyzing AUC scores that approach 1.00 and 0.99. The outcomes of the work indicate that the security of the passwords is weak, which proves the need to implement biometric solutions and other authentication factors to secure the system [33].

Igwe (2025) The accuracy of detecting security misconfigurations is proven to be 92.4% (experimental validation), deployment latency is reduced by 45%, and manual security interventions were lowered by 78%. The framework was able to process 3250 deployment scenarios with an average response time of 3.1 seconds. This methodology, designed generically to work in regulated enterprise settings, reduces the amount of manual error, has fast secure deployment and is adherent to the principles of the Zero Trust. They describe elements of architecture, automation, and compatibility with other services such as GuardDuty and AWS Inspector and prove that AI-managed infrastructure security is not only possible but becoming essential in future consumer ecosystems [34].

Chaudhary et al. (2024) using a wide range of test datasets to achieve notable enhancements in detection accuracy, FP and FN rates, and AUC values. In instance, the proposed approach significantly beats the state-of-the-art system, with a detection accuracy of 98.5% and a decrease in FN and FP rates to 2.0% and1.2%, respectively. Moreover, the proposed methodology is always more effective than the existing system based on various test sets, meaning that it is effective in improving the accuracy of cyber threat detection in cloud environments [35].

Tocci, Zhou and Zhang (2023) A system for detecting intrusions in UAVs is developed using reinforcement learning. To train the model, employ a Deep-Q Learning strategy and generate training data from the CICIDS2017 dataset. The Vitis-AI toolkit from Xilinx allows for the realistic training of a UAV-sized FPGA, which expedites the procedure. The agent is able to differentiate between benign traffic, DDoS assaults, and port scan attacks with ease, thanks to its accuracy rate of over 90% and inference speed of 51.3 FPS on an AMD Ryzen 5600x CPU. The Xilinx Zynq UltraScale+ ZCU102 FPGA saw a 100-fold performance increase thanks to Vitis-AI, which allowed the neural network to achieve 5886.85 FPS [36].

Mehmood et al. (2023) This article uses ML algorithms to categorise insider assaults. Several files from the CERT dataset are combined to create a customised dataset. The dataset is analysed using four ML algorithms: LightGBM, XGBoost, RF, and

Adaboost. When comparing overall performance, LightGBM came out on top. However, when it comes to protecting against internal attacks (such Behavioural Biometrics attacks), two algorithms that could be better than the others are RF or AdaBoost. Therefore, by integrating multiple machine learning algorithms, a more accurate classification of internal threats can be achieved. Following XGBoost at 88.27%, LightGBM at 97%, RF at 86%, and AdaBoost at 88% are the suggested algorithms in order of accuracy [37].

Opara, Wimmer and Rebman (2022) The goal of this research is to demonstrate how well auto-ML can identify cyber security risks using the resources available in free tier accounts on three different cloud services: Microsoft Azure, Google Cloud, and IBM Cloud. They scored the instruments based on how well they optimised speed and accuracy. This report compares and contrasts the benefits of the various platforms' outputs. Three platforms exceeded 70% accuracy on average, with IBM Cloud Platform delivering the best results [38].

The Table 3 provide s the summary of the comparison of the recent studies using focus, methods, data, performance and notes

Table 3 : Summary of AI Approaches for Cyber Threat Detection in Zero-Trust and Cloud Environments

Reference	Focus	Method Used	Dataset	Performance	Research Gaps
B & Meenakshi (2025)	Evaluated ML models for Zero-Trust anomaly detection	AdaBoost, RF, XGBoost+KNN	Not specified	RF: 96.48%, XGBoost: 95.23%, KNN: 77.39%, AdaBoost: 67.84%; AUC ~1.00 & 0.99 for RF/XGBoost	Limited hybrid models; dataset diversity; advanced authentication integration lacking
Igwe (2025)	Detecting security misconfigurations in Zero-Trust environments	AI-based validation framework	3,250 deployment scenarios	92.4% accuracy, 45% latency reduction, 78% fewer manual interventions, 3.1s response	Real-time threat detection not addressed; generalization beyond regulated environments unclear
Chaudhary et al. (2024)	Enhanced threat detection in cloud systems	Proposed detection model	Several test datasets	98.5% accuracy vs 89.7% baseline; FN: 2.0%, FP: 1.2%, Higher AUC values	Zero-trust scenarios not tested; model explainability missing; scalability unclear
Tocci, Zhou & Zhang (2023)	UAV intrusion detection using RL	Deep-Q Learning on FPGA	CICIDS2017	>90% accuracy; 51.3 FPS on CPU; 5886.85 FPS on FPGA (~100× speedup)	Focus on UAVs; adaptation to general cloud workloads not studied
Mehmood et al. (2023)	Insider attack classification	RF, AdaBoost, XGBoost, LightGBM	Custom CERT-based dataset	LightGBM: 97%, RF: 86%, AdaBoost: 88%, XGBoost: 88.27%	Real-time cloud deployment missing; zero-trust integration lacking; ensemble potential underexplored
Opara, Wimmer & Rebman (2022)	AutoML threat detection on cloud platforms	Azure AutoML, Google AutoML, IBM AutoML	Azure, Google, IBM free tiers	All >70% accuracy; IBM strongest overall	Focused on tool comparison; zero-trust evaluation missing; adaptive attacks not tested

VI. CONCLUSION AND FUTURE WORK

One of the most important ways that AI is helping to strengthen Zero Trust Architectures in today's cloud-based landscapes is through threat detection. The complexity and ever-changing nature of cloud systems make it increasingly difficult to combat sophisticated assaults using the same perimeter-focused security measures. By continuously authenticating users, imposing least-privilege access, and evaluating rules in real-time, Zero Trust Architecture provides a solid security foundation.

On the other hand, models driven by AI enable a higher detection rate, more flexibility, and automatic responses. ML, DL, and reinforcement learning techniques significantly improve cloud and zero-trust system intrusion detection, anomaly detection, and adaptive policy enforcement, according to the reviewed research. The difficulty to integrate across heterogeneous multi-cloud environments, high computational costs, a lack of high-quality labelled data, and an absence of model explanations are all ongoing problems. In order to implement zero-trust in real-time, future research should center on developing AI models that are both lightweight and explainable. This research should particularly target resource-constrained and edge-cloud scenarios. Moreover, the federated learning process and privacy-conserving systems represent the prospective solutions to prevent the issue of information sharing and associated regulatory challenges. Standard sets of data, benchmarks will also be necessary to measure the performance objectively and to replicate it. Overcoming these issues will also improve the synergy of AI and Zero Trust, so that resilient, scalable, and intelligent cloud security architectures become possible.

VII. REFERENCES

[1] A. Meshram, "Hybrid Cloud Strategy for Mission-Critical Financial Software Applications," Int. J. Adv. Res. Comput. Commun. Eng., vol. 14, no. 12, p. 136, 2025, doi: 10.17148/IJARCCE.2025.1412136.

[2] S. Srinivasan, R. Sundaram, K. Narukulla, S. Thangavel, and S. B. Venkata Naga, "Cloud-Native Microservices Architectures: Performance, Security, and Cost Optimization Strategies," Int. J. Emerg. Trends Comput. Sci. Inf. Technol., vol. 4, no. 1, pp. 16–24, 2023, doi: 10.63282/3050-9246.ijetcsit-v4i1p103.

[3] M. S. Mahajan, "Zero Trust Cloud Security and AI for Secure Multi-Cloud Architecture," vol. 11, no. 4, pp. 750–755, 2024, doi: 10.17148/IARJSET.2024.114110.

[4] S. R. Kurakula, "Cloud-native microservices in financial services: Architecting for scalability and flexibility," World J. Adv. Res. Rev., vol. 26, no. 2, pp. 1435–1442, May 2025, doi: 10.30574/wjarr.2025.26.2.1690.

[5] V. Prajapati, "Enhancing Threat Intelligence and Cyber Defense through Big Data Analytics: A Review Study," J. Glob. Res. Math. Arch., vol. 12, no. 4, 2025.

[6] P. Chandrashekar and M. Kari, "Design Machine Learning-Based Zero-Trust Intrusion Identification Models for Securing Cloud Computing System," Int. J. Res. Anal. Rev., vol. 11, no. 4, pp. 901–907, 2024.

[7] M. Mangla, "AI-Driven Zero Trust Architecture: A Scalable Framework for Threat Detection and Adaptive Access Control," IJST, vol. 2, no. 3, 2023, doi: 10.56127/ijst.v2i3.22.

[8] R. Palwe, "Onboarding for AI features: Reducing friction at the first use," Int. J. Comput. Artif. Intell., vol. 6, no. 2, pp. 393–400, Jul. 2025, doi: 10.33545/27076571.2025.v6.i2e.227.

[9] M. Shore, S. Zeadally, and A. Keshariya, "Zero Trust: The What, How, Why, and When," Computer (Long. Beach. Calif)., vol. 54, no. 11, pp. 26–35, 2021, doi: 10.1109/MC.2021.3090018.

[10] S. Narang and A. Gogineni, "Zero-Trust Security in Intrusion Detection Networks: An AI-Powered Threat Detection in Cloud Environment," Int. J. Sci. Res. Mod. Technol., vol. 4, no. 5, pp. 60–70, Jun. 2025, doi: 10.38124/ijsrmt.v4i5.542.

[11] S. Ameer, L. Praharaj, R. Sandhu, S. Bhatt, and M. Gupta, "ZTA-IoT: A Novel Architecture for Zero-Trust in IoT Systems and an Ensuing Usage Control Model," ACM Trans. Priv. Secur., vol. 27, no. 3, Aug. 2024, doi: 10.1145/3671147.

[12] C. Zanasi, S. Russo, and M. Colajanni, "Flexible zero trust architecture for the cybersecurity of industrial IoT infrastructures," Ad Hoc Networks, vol. 156, p. 103414, Apr. 2024, doi: 10.1016/j.adhoc.2024.103414.

[13] S. Ahmadi, "Zero Trust Architecture in Cloud Networks: Application, Challenges and Future Opportunities," J. Eng. Res. Reports, vol. 26, pp. 215–228, 2024, doi: 10.9734/JERR/2024/v26i21083.

[14] V. Shah, "Securing the Cloud of Things : A Comprehensive Analytics of Architecture , Use Cases , and Privacy Risks," ESP J. Eng. Technol. Adv., vol. 3, no. 4, pp. 158–165, 2023, doi: 10.56472/25832646/JETA-V3I8P118.

[15] S. Amrale, "Proactive Resource Utilization Prediction for Scalable Cloud Systems with Machine Learning," Int. J. Res. Anal. Rev. (IJRAR, vol. 10, no. 4, pp. 758–764, 2023, doi: 10.56472/25832646/JETA-V3I8P119.

[16] V. Varma, "Secure Cloud Computing with Machine Learning and Data Analytics for Business Optimization," ESP J. Eng. Technol. Adv., vol. 4, no. 3, pp. 181–188, 2024, doi: 10.56472/25832646/JETA-V4I3P119.

[17] S. K. Chintagunta and S. Amrale, "Enhancing Cloud Database Security Through Intelligent Threat Detection and Risk Mitigation," Tech. Int. J. Eng. Res., vol. 9, no. 10, pp. 49–55, 2022, doi: 10.56975/tijer.v9i10.159996.

[18] N. Mohamed, "Current trends in AI and ML for cybersecurity: A state-of-the-art survey," Cogent Eng., vol. 10, no. 2, pp. 1–30, 2023, doi: 10.1080/23311916.2023.2272358.

[19] V. M. L. G. Nerella, "Architecting secure, automated multi-cloud database platforms strategies for scalable compliance," Int. J. Intell. Syst. Appl. Eng., vol. 9, no. 1, pp. 128–138, 2021.

[20] M. H. Hnini and Z. Bensakif, "Exploring The Cloud Security Landscape: Challenges, Solutions, And Insights From Academic Inquiry," Ensa," ENSA, vol. January, pp. 1–21, 2025.

[21] H. P. Kapadia, "Zero Trust Architecture In Banking Web Applications," vol. 14, no. 2, pp. 112–118, 2024.

[22] D. Patel, "Zero Trust and DevSecOps in Cloud-Native Environments with Security Frameworks and Best Practices," Int. J. Adv. Res. Sci. Commun. Technol., vol. 3, no. 3, pp. 454–464, Jan. 2023, doi: 10.48175/IJARSCT-11900D.

[23] S. B. Karri, C. M. Penugonda, S. Karanam, M. Tajammul, S. Rayankula, and P. Vankadara, "Enhancing Cloud-Native Applications: A Comparative Study of Java-To-Go Micro Services Migration," Int. Trans. Electr. Eng. Comput. Sci., vol. 4, no. 1, pp. 1–12, Apr. 2025, doi: 10.62760/iteecs.4.1.2025.127.

[24] A. Parupalli and H. Kali, "An In-Depth Review of Cost Optimization Tactics in Multi-Cloud Frameworks," Int. J. Adv. Res. Sci. Commun. Technol., vol. 3, no. 5, pp. 1043–1052, Jun. 2023, doi: 10.48175/IJARSCT-11937Q.

[25] N. K. Prajapati, "Federated Learning for Privacy-Preserving Cybersecurity: A Review on Secure Threat Detection," Int. J. Adv. Res. Sci. Commun. Technol., vol. 5, no. 4, pp. 520–528, Apr. 2025, doi: 10.48175/IJARSCT-25168.

[26] N. Mohamed, "Current trends in AI and ML for cybersecurity: A state-of-the-art survey," Cogent Eng., vol. 10, no. 2, Dec. 2023, doi: 10.1080/23311916.2023.2272358.

[27] S. Kumara, "AI-Driven Threat Identification and Response: Implications for Secure and Scalable Telecom Infrastructure," Int. J. Adv. Res. Sci. Commun. Technol., vol. 5, no. 4, p. 559, Dec. 2025, doi: 10.48175/IJARSCT-30567.

[28] R. Dattangire, R. Vaidya, D. Biradar, and A. Joon, "Exploring the Tangible Impact of Artificial Intelligence and Machine Learning: Bridging the Gap between Hype and Reality," in 2024 1st International Conference on Advanced Computing and Emerging Technologies (ACET), IEEE, 2024, pp. 1–6. doi: 10.1109/ACET61898.2024.10730334.

[29] H. Liu and B. Lang, "Machine Learning and Deep Learning Methods for Intrusion Detection Systems: A Survey," Appl. Sci., vol. 9, no. 20, p. 4396, Oct. 2019, doi: 10.3390/app9204396.

[30] G. Maddali, "Enhancing Database Architectures with Artificial Intelligence (AI)," Int. J. Sci. Res. Sci. Technol., vol. 12, no. 3, pp. 296–308, May 2025, doi: 10.32628/IJSRST2512331.

[31] A. R. Bilipelli, "AI-Driven Intrusion Detection Systems for Large- Scale Cybersecurity Networks Data Analysis : A Comparative Study," TIJER – Int. Res. J., vol. 11, no. 12, pp. 922–928, 2024.

[32] G. Sarraf and V. Pal, "Adaptive Deep Learning for Identification of Real-Time Anomaly in Zero-Trust Cloud Networks," vol. 4, no. 3, pp. 209–218, 2024, doi: 10.56472/25832646/JETA-V4I3P122.

[33] R. B and C. Meenakshi, "Zero Trust Network and Cloud Security Architecture: A New Wave of Access Control Techniques," in 2025 3rd International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI), 2025, pp. 516–519. doi: 10.1109/ICoICI65217.2025.11253860.

[34] H. A. Igwe, "AI-Driven Framework for Automating Infrastructure Provisioning and Compliance Validation in Cloud-Native Environments," in 2025 IEEE 14th International Conference on Consumer Electronics - Berlin (ICCE-Berlin), 2025, pp. 158–162. doi: 10.1109/ICCE-Berlin67488.2025.11277463.

[35] D. Chaudhary, S. K. Verma, V. Mohan Shrimal, R. Madala, R. Baliyan, and S. M, "AI-Based Methods to Detect and Counter Cyber Threats in Cloud Environments to Strengthen Cloud Security," in 2024 International Conference on Electrical Electronics and Computing Technologies (ICEECT), 2024, pp. 1–6. doi: 10.1109/ICEECT61758.2024.10739173.

[36] D. Tocci, R. Zhou, and K. Zhang, "FPGA Accelerated Decentralized Reinforcement Learning for Anomaly Detection in UAV Networks," in 2023 IEEE 16th International Symposium on Embedded Multicore/Many-core Systems-on-Chip (MCSoC), 2023, pp. 248–253. doi: 10.1109/MCSoC60832.2023.00044.

[37] M. Mehmood, R. Amin, M. M. A. Muslam, J. Xie, and H. Aldabbas, "Privilege Escalation Attack Detection and Mitigation in Cloud Using Machine Learning," IEEE Access, vol. 11, pp. 46561–46576, 2023, doi: 10.1109/ACCESS.2023.3273895.

[38] E. Opara, H. Wimmer, and C. M. Rebman, "Auto-ML Cyber Security Data Analysis Using Google, Azure and IBM Cloud Platforms," in 2022 International Conference on Electrical, Computer and Energy Technologies (ICECET), 2022, pp. 1–10. doi: 10.1109/ICECET55527.2022.9872782