Journal of Artificial Intelligence in Governance and Public Policy

Volume 1, No 1, January 2026
Available Online at: jaigpp.org

JAIGPP
Journal of Artificial Intelligence in Governance and Public Policy

Zero-Trust Security Enforcement through AI-Powered Anomaly Detection in Cloud Systems

Dr. Puneet Garg
Associate Professor
Department of CSE-AI
KIET Group of Institutions
Delhi NCR, Ghaziabad
puneet.garg@kiet.edu

***Abstract*—The adoption of cloud computing has increased compared to a quick pace, and the sophistication of cyber threats have made the conventional perimeter-based security model to be inadequate. Based on the idea of never trust, always verify, Zero Trust Architecture (ZTA) has proved to be an effective model of securing the cloud environment in modern times through ongoing authentication, minimal privileges, micro-segmentation, and real-time monitoring. This paper examines the central concepts, rational aspects, and design features of Zero Trust in clouds, and the ways it can be compliant with the NIST guidelines. In addition, the article compares and contrasts the more conventional statistical, rule-based, and signature-based approaches to anomaly detection with AI-driven methods that use machine learning and deep learning models such as supervised, semi-supervised, and unsupervised models, autoencoders, convolutional neural networks (CNNs), and recurrent neural networks (RNNs). Incorporation of artificial intelligence in Zero Trust can boost adaptative threat detection, behaviour analytics and automated responses mechanism. Also, the paper focuses on how this applies to cloud systems, remote work forces, IoT, microservices, and SASE environments, and outlines difficulties in implementation, including technical complexity, organizational resistance, financial limitations, and regulatory alignment. The results report the presence of an AI-based anomaly detector and Zero Trust principles as a dynamic, contextual, and resilient security system that able to respond to the changing threat in cloud-based infrastructures.**

Keywords—Zero Trust Security, AI-Powered Anomaly Detection, Identity and Access Management (IAM), Behavioral Analytics, and Security Automation.

I. Introduction

The concept of "cloud computing" (CC) [1] has emerged as a novel model for enabling and providing services through the Internet. Cloud computing has evolved significantly in recent years in response to widespread budget cuts and rising computing costs associated with data storage, analysis, and presentation. Access to end-user resources, such as data storage and computing power, on demand, without direct client-side specialization, is known as CC [2]. The term "distributed computing" has a variety of meanings depending on who ask [3][4]. Clients can access both public and private data over a unified platform in distributed computing over the Internet [5][6]. Client and association vulnerabilities are only two of the many security issues with CC [7] that slow down the computing model's quick adoption. The term "cloud infrastructure" can refer to either a local area network (LAN) or a more generalized network that is built on the internet of things (IoT) [8]. Included in the infrastructure are servers, storage, underlying systems, processing in real-time, and operations [9].

Current methods of user identification, authentication, and access management are not cloud-friendly. Some major security concerns include data storage outside of the system, reduced user control, and interconnected models and architectures. Data protection is the top priority when it comes to privacy and security in the cloud. There is a rise in cybercrimes impacting people, businesses, and governments if this is breached [10], since it exposes users' personal information. One of the most crucial aspects of cloud computing's success is its security [11]. In 2011, the data's placement was recognised as a potential security risk. They spoke about data security issues [12]. Researchers also paid close attention to trust as a consideration because of the strong correlation between trust and the credibility of cloud service providers. Even in the cloud, systems that store data are vulnerable to the same kinds of threats that affect more conventional systems [13]. Discussed and emphasized as crucial to the safety of cloud computing [14] and the data stored therein is the virtual machine's security.

Zero-Trust Architecture (ZTA) is now a network defines paradigm shift, based on the principles of never trust, always verify, and always authenticate, micro-segmentation, and the enforcement of context-based access control. Although it has strong conceptual elements, real-world implementations tend to rely on fixed policies and rule-based trust scoring, which are poorly responsive to changing behaviour patterns and real-time abnormalities [15]. At the same time, the potential of artificial intelligence (AI) [16] technologies in dynamic threat modelling, behavioral analytics, and anomaly detection [17] is impressive in the context of security. The introduction of these AI-based detection features into Zero-Trust ecosystems is one potential path to overcoming the failures of current APT mitigation policies.

Cloud network environments that monitor and help diverse nodes in the network require a trust-based authorization method, as is evident from the present threat landscape [18]. The entity in question must obtain approval from the network management authority before executing any activity that could compromise mission-critical data or services [19]. Existing technologies like intrusion detection systems (IDS), real-time resource management (RTM), resource segmentation (RS), and behaviour tracking can be set up to do this, giving network security teams insight, granular control, and access to endpoint devices. In contrast, an intrusion detection system (IDS) when misused can detect intrusions by searching a database of signatures. It doesn't trigger false alarms, but a fresh assault with a different signature can bypass it [20]. A number of limitations impact IDS and thus the efficacy of intrusion detection systems; they include, but are not limited to, large data volumes, the need for immediate detection, concerns about data integrity, and other similar issues. Recently, AI techniques such as ML [21][22] and DL [23][24] algorithms have been employed to handle security concerns and improve data management.

Cloud computing [25][26] reduces the need for local servers, ensuring security and reliability. However, risk evaluation is complex due to high resource usage, uneven standards, and limited transparency [27][28]. The Zero Trust Architecture Enhancement is proposed to improve cloud-based security by integrating adaptive safety precautions with trust evaluations. The review enhances cloud security adaptability by enhancing knowledge of successful trust management strategies that incorporate safeguards against dynamic threat environments.

A. Structure of the Paper

This paper is organized as follows: Section II presents Zero Trust Security Architecture. The section III discusses about AI-based anomaly detection. Section IV entails AI-based applications, challenges, and future trends. The uses, difficulties, and potential developments of AI are discussed in Section IV. The literature review is presented in Section V, and the study is concluded with future directions in Section VI.

II. Zero-Trust Security Architecture in Cloud Environments

Zero Trust Architecture (ZTA) is a shift in thinking of the past security descriptions that are based on perimeter security. Instead of considering the fact that the entities within the network are somehow trustworthy [29], ZTA is based on the principle that all users, devices, and systems cannot be trusted by default either within the organizational boundary or outside [30]. This never trust, always verify model requires unceasing authentication, access control and finer security policies according to context, identity and conduct.

A. Core Principles of Zero Trust Architecture

The widespread adoption of cloud computing has led to the complexity of cybersecurity threats necessitating the adoption of advanced security solutions like ZTA [31]. ZTA adheres to the principle of "never trust, always verify" when it comes to all access requests, particularly in relation to the safety of cloud environments such as Microsoft Azure. In contrast to conventional perimeter-based security measures, ZTA employs continuous authentication of users, devices, and requests, hence granting access only when absolutely necessary. Using the cloud as an example, this section delves into the benefits and how to put ZTA into practice:

1) Verify Identity and Context

This is accomplished by taking precautions to verify the identity of users, devices, and apps before granting them access to any resources. Verification extends beyond conventional username and password validation to encompass multi-factor authentication (MFA), biometric verification and situational factors, including the location of the user, the health of the device and their behavioral patterns.

2) Least Privilege Access

System and user access should be limited to that which is absolutely necessary for the performance of their tasks in accordance with the principle of least privilege. This reduces the possibility of unintentional or intentional abuse of privileges. Access rights are also subtle in a Zero Trust architecture and become dynamically apportioned depending on the needs of the users, as well as their functions. This strategy reduces the potential attack surface since, even if a hacker gains access to a user's account, they only able to use the resources required to carry out their job, limiting the potential damage.

3) Micro-Segmentation

The network is divided into smaller parts using micro-segmentation in order to minimize its lateral mobility. All the segments have security policies and access controls. This segmentation is applicable to both the data and applications, which form a chain of safe areas in the network. Organizations can facilitate the effects of security incidents by containing and mitigating threats to the network by limiting potential threats to restricted segments and eliminating unauthorized user access between segments.

4) Continuous Monitoring and Analytics

Zero Trust Architecture relies on analytics and continuous monitoring. A key component of this approach is the continuous monitoring of the network, user activity, and network performance. This allows for the real-time detection of any anomalies or potential security concerns. The application of sophisticated analytics and machine learning algorithms to identify trends and outliers is regarded as standard practice [32]. Through a proactive, real-time perspective of the network, organizations are able to quickly react to any emerging threats, enable security policies accordingly, and make certain that their defences keep pace with the changing threat environment.

B. Logical Components of the Model

The framework of the building's architecture is great, and so are the relationships inside it. An American institution, the National Institute of Standards and Technology, served as inspiration for this design. The policy enrolment point and the policy administrator are communicated with via the policy engine, which is the major portion. Fig. 1 displays the relative components, and this is further upon below:

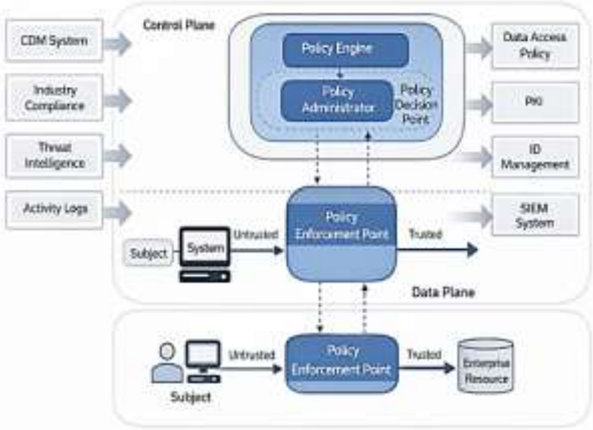

Fig. 1. Logical Components of Zero Trust Model

1) *Policy Engine*

The model's policy engine plays a crucial role in determining the long-term and ultimate decision to grant access to a device or network. PE design takes into account external elements like CDM systems, threat intelligence, and activity logs as trust algorithms to authorize, deactivate, or provide access to resources, in addition to the organization's internal and external working policies. The policy administrator component is connected with the PE. A decision is made and recorded by the policy engine, which can be either authorized or refused. The policy administrator then takes action based on this decision.

2) *Policy Administrator*

The policy administrator mainly acts as an executor, monitoring the flow of information from the policy engine and controlling the communication paths based on that information. In practice, the PA verifies the identity of users using the token or credential that clients use to access enterprise resources.

3) *Policy Enrolment Point*

The policy engine makes decisions, and this component executes those decisions by enabling, monitoring, and terminating agent-client traffic. It acts as a conduit between users and the system resources.

C. *Elements of Zero-Trust Security Architecture*

The zero-trust paradigm, like any other security framework, relies on other frameworks and variables to ensure its successful acceptance and implementation. Despite the fact that model deployment is very dependent on a number of factors, Ngo-Lam (2020) isolated three crucial architectural components. These factors are significant in assessment of the model, based on review of the literature; they are detailed below.

1) *No False sense of security*

Employees' passing initial security checks is insufficient proof of trust or security breaches; instead, they should be held responsible for their honesty and the conviction that they would always abide by security regulations [33], thus validating trust. Nevertheless, the Zero Trust model de-mystifies this principle; the architecture of the model secures against the threats of insiders which might have gone undetected.

2) *Multi-Factor Authentication*

As the name implies, multi-factor authentication is a combination of two or more security factors that aim to verify a user's identity. The concept is to authenticate the user and credentials of the system. An MFA system, in its most basic form, is one that asks for more than one form of identification when logging into an application or system. If one fails, the intended physical location, computational equipment, network, or database is not authorized [34].

3) *Micro-Segmentation*

The concept of micro-segmentation aims to grant users the least privilege and restrict access across the entire organization's network. The idea behind it is that users should only have access to the parts of the company network that are relevant to their jobs, and that correct authorization should be used for this. It protects the weaknesses at the lateral level and protects against the unauthorized access to the assets within the premises.

4) *Model Requirements*

The NIST (2020) policy mandates a specific set of guidelines for the design and procedural execution of zero trust architecture. Although some organizations have user-based procedures, it employs the methodology outlined in the NIST 2020 policy. Access control, monitoring, and granting are the three areas where these seven procedural concepts are covered.

III. AI-Powered Anomaly Detection In Cloud Systems

Detection of anomalies is another essential part of cybersecurity, especially the one amid cloud computing. The security landscape is undergoing a sea change as more and more organizations migrate their data and apps to the cloud [35]. The chapter is a review of the available literature on the topic of anomaly detection [36] methods with reference to the problem of using such methods in the cloud security setting. The chapter consists of several parts: the description of the conventional methods of anomaly detection [37], the discussion of AI-based methods, the analysis of the problems encountered in the field, and the discussion of the latest achievements in the given sphere.

A. *Machine Learning for Anomaly Detection*

Machine learning (ML) methods [38][39] are being used more and more as a way to find odd activities. With ML, it aims to "automate the process of knowledge acquisition from examples." To construct a model that differentiates between normal and abnormal categories, this method is employed [40]. Anomaly detection can be broadly classified into three groups according to the training data function utilized to construct the model [41]. Each of the three main categories comprise:

1) *Supervised Anomaly Detection*

This class uses tagged instances to differentiate between normal and aberrant training data. Constructing a prediction model for the normal class and another for the anomalous class is the basic idea behind this model. Nevertheless, there are two problems that arise with this technique. To begin with, there are significantly fewer outliers in the training set than there are in the usual situations. Furthermore, it is especially difficult to find accurate and representative labels for the anomaly class.

2) *Semi-supervised Anomaly Detection*

The training here consists of the usual class scenarios. For that reason, anomaly is the label given to anything out of the ordinary. It is assumed in semi-supervised methods that the training data only contains labelled instances of the normal class. They are more prevalent than supervised approaches since they do not require anomalous class labelling.

3) *Unsupervised Anomaly Detection*

The techniques in this instance do not require training datasets. Accordingly, those techniques suggest that typical cases predominate over outliers in test datasets [42]. On the other hand, this method has a significant false alarm rate if the assumption is incorrect.

B. *Deep Learning-Based Anomaly Detection*

The capacity of DL [43] to handle complicated data structures and identify complex patterns has made it a popular subfield of machine learning in the area of anomaly identification [44]. Techniques such as:

1) *Autoencoders*

These are neural networks that are used to re-create input data. Autoencoders are able to attract attention to anomalies by measuring the reconstruction error, and this is used to detect data points that do not fit the learned patterns. This is especially effective in high dimensional data environments that are common in cloud applications.

2) *Convolutional Neural Networks*

CNNs were initially created to process images, though they can be used in cloud security when working with time-series data [45]. CNNs have the potential to detect anomalous patterns within network traffic or user behaviour by extracting spatial hierarchies, which allows them to be useful in identifying these patterns.

3) *Recurrent Neural Networks (RNNs)*

RNN works with sequential data, but are especially effectively applied to time-series data in real-time. They have the capability to remember what happened in the past time steps hence suitable in identifying abnormalities within user behaviour over time.

C. *Traditional Approaches to Anomaly Detection*

Conventional security is based on Statistical Methods, Rule-Based Systems and Signatures to detect known threats based on baselines and preset patterns, though they usually cannot contend with the vendor of dynamic cloud environments and zero-day attacks. The various traditional approaches used for Anomaly Detection are explained below:

- **Statistical Methods:** The conventional methods of anomaly detection have generally been based on statistical methods of detecting a deviation to expected behaviour. Such techniques usually include the creation of a normal activity base and raising red flags when there are data values that are not within this range. The common statistical techniques are:
- **Z-Score Analysis:** The procedure involves calculating the standard deviations of each data point from the mean. A data point is considered an outlier if its Z-score is higher than a particular limit.

1) *Box Plot Analysis*

Box plots visually display the information about the distribution of data points, and it is possible to identify outliers i.e. the value that would be above the whiskers of the box plot.

2) *Rule-Based Systems*

Rule-based systems are those that deal with the establishment of pre-established rules that govern what is normal behaviour. Such rules may be either straightforward (e.g., when traffic has exceeded X requests per minute, it is anomalous) or complicated, and have many conditions. Whereas rule-based systems may be useful in cases of known threats, they are restricted in the way they are unable to respond to novel and unexpected threats vectors. Answering the question of how to uphold the rules is the primary challenge of having rule-based systems. The cloud environment is dynamic and organizations need to keep on updating their rules with regards to user behaviour and system processes. This overhead may be considerable especially when the environment to be maintained is large and has various applications.

3) *Signature-Based Detection*

Signature-based Detection is a method of identifying threats through searching known patterns or malicious activity signatures. This is a technique popular among intrusion detection systems (IDS) [46] and antivirus software. Though signature-based detection works well on known threats, it is poorly placed to deal with zero-day attacks or new forms of malware that do not have known signatures.

IV. AI-Based Applications, Challenges and Future Trends of Zero Trust Architecture

The complexity and velocity of cyber threats in today's technologies necessitate more adaptable and efficient countermeasures. To counter new types of assaults and dangers, traditional security paradigms need to be rethought. Rising security risks and big, complex, hybrid networks have made controlling access to vital data resources and services an insurmountable task. Zero Trust Architecture (ZTA), founded on the principle of "never trust, always verify," has thus been proposed as an appropriate solution. The Zero Trust architecture provides a dynamic defense mechanism that can actively monitor and change the security mechanisms in operation [47]. It is orchestrated by AI technologies like as machine learning, AI-enabled anomaly detection, and behavioral analysis.

A. *AI-Powered Applications in Zero Trust Architecture*

The benefits that AI can provide through the automation of threat identification and management have led to its increasing application in cybersecurity [47]. This technology allows systems to anticipate and avoid potential dangers, leading to far faster response times. Up until around halfway through 2022, the most popular AI applications in threat intelligence platforms were those that aimed to detect anomalies, phishing attempts, and malware. See Fig. 2 and read on for an explanation of certain AI uses:

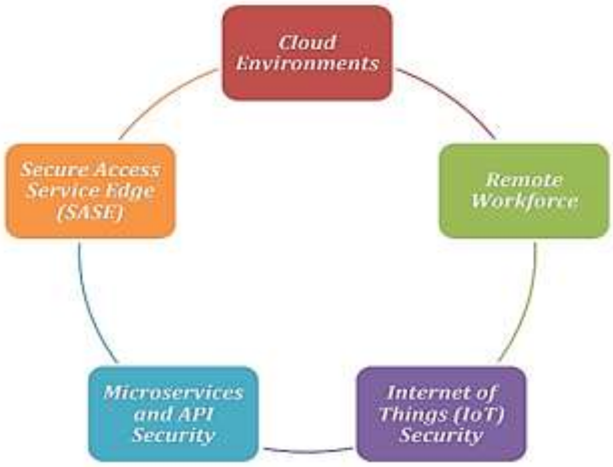
Cloud Environments
Secure Access Service Edge (SASE)
Remote Workforce
Microservices and API Security
Internet of Things (IoT) Security

Fig. 2. Applications of Zero Trust Applications

1) *Cloud Environments*

Cloud services and Zero Trust have grown in popularity, and for good reason: they provide a solid basis for safeguarding assets and data kept on cloud servers. Implementing access restrictions and continuous verification, Zero Trust provides greater control over cloud resources and mitigates security vulnerabilities associated with the cloud.

2) *Remote Workforce*

Zero Trust is also helpful for protecting company resources when employees use non-traditional ways to access them. An unauthorized intrusion is less likely to occur when there is such a divergence in conduct with the distant devices and networks.

3) Microservices and API Security

APIs and microservices are now essential elements in application architecture. The Zero Trust Principle ensures that only authorized businesses can access APIs, and it allows microservices to securely exchange data with one another.

4) Internet of Things (IoT) Security

The Internet of Things (IoT) has grown in scope, and zero trust is essential for protecting IoT devices [48]. With zero trust, the risk of cyberattacks on the IoT is reduced, and unauthorized entities cannot use IoT devices because of the tight control over permissions and constant authentication of IoT devices [49][50]. To do this, they may use analytics and AI to rank the potential risks posed by the activity of IoT devices.

5) Secure Access Service Edge (SASE)

Zero Trust and the SASE architecture function well together since they both incorporate networking and cloud security. By implementing Zero Trust effectively, organizations may strengthen network security, keep up with changing threats, and shield vital assets from sophisticated cyberattacks [51][52]. Zero Trust should be applied to different fields enabling the organization to build a robust security architecture that safeguards information and assets and encourages trust in online operations.

B. Challenges in Implementing Zero Trust

The Zero Trust paradigm leaves organizations with a continuum of challenges that have to be addressed in a careful way and mitigated strategically. The advantages of Zero Trust are indisputable; nevertheless, these obstacles are an inseparable part of making the implementation successful and making optimal use of its potential. This sub-section clarifies the complexities involved in the implementation of Zero Trust and provides some ideas on how to deal with such complexities.

1) Cultural Barriers and Organizational Resistance

A cultural change has to take place in the organization when moving to Zero Trust as traditional security models are being used. Those employees who are used to using a perimeter-based model of trust might be opposed to constant verification and least privilege access policies of Zero Trust. The process of overcoming this resistance requires the following effective strategies of managing the change process, the extensive training, and the open communications that helps to create the common sense of the paradigm shift.

2) Technical Complexity and Integration

The implementation of Zero Trust in the infrastructure of an organization may be complex and consumptive of resources. The use of legacy systems, an unequal technology, and varying platforms can be an obstacle to compatibility that should be carefully planned and implemented in stages. The ability to connect different elements, but maintain interconnectivity with the other components and yet maintain the seamless functionality is central in achieving the holistic benefits of Zero Trust.

3) Balancing Security and Usability

Finding the right balance between the high level of security and usability is a delicate issue in the implementation of Zero trust. The continuous authentication and access restriction can cause the possible user frustration and efficiency loss. The solution to this hurdle would include the creation of user-friendly interfaces, simplifying the authentication process and workflow optimization to make sure that the security improvements do not affect the productivity of the user.

4) Financial Considerations

Zero Trust implementation has financial implications such as investments in technology, manpower, and maintenance. Organizations have to invest in the upgrades of the security infrastructure, training, and monitoring tools. A careful evaluation of the costs and benefits and a careful allocation of resources becomes essential to bring the equilibrium between these financial obligations and the expected benefits and mitigation of the risk.

5) Data Privacy and Regulatory Compliance

Zero Trust intrinsically requires unceasing verification and access controls, which impact the issue of data privacy and, to that end, should be consistent with regulatory standards. The ability to comply with the data protection standards, including GDPR or HIPAA, and introduce the effective protection measures implies a sophisticated perception of the legal standards and careful data management.

C. Envisioning the Future of Zero Trust

With the infiltration of the Zero Trust concept into the cybersecurity circles, its implementation is expected to be cross-industrial and take a central position in network security policies. Enterprises not adopt Zero Trust as an act of response but as a proactive position that section of their risk management systems. The future of adaptive security as a natural quality of online intercourse is a prospective reality the merger of Zero Trust and cognitive computing creates. The natural capability of Zero Trust to know context and purpose, combined with the use of AI, to make decisions leads to the creation of a security fabric that automatically adapts to threats. To sum up, the prospects and future of Zero Trust are connected with change potential. Its ability to secure security landscapes, coexist with the new technologies and envision a dynamic cybersecurity ecosystem attests to the fact that Zero Trust is a pioneer in network protection. By adopting the concept of Zero Trust and moving the path, which can be traced to its postulates, organizations can find it easy to sail through the dynamic cyber landscape with robustness, speed, and uncompromising credibility.

V. Literature Review

This section reveals equivalent investigations on Anomaly Detection in Zero-Trust Security displaying their effects on learning, decision making, and efficiency of operation in diverse fields.

S. Ghimire (2026) presented a conceptual architecture that combines AI with Zero Trust principles to support continuous monitoring and risk assessment of PLCs in food processing environments. The proposed approach uses passive behavioral observation and network-level monitoring to track controller activity over time and enable adaptive trust decisions based on observed risk. By improving visibility without requiring changes to controller hardware or control logic, the architecture helps preserve safety and availability [53].

A. Qazi and S. Arshad (2025) presented a Zero Trust Architecture (ZTA)-based security framework for Oracle ERP

Cloud to counter the emerging cybersecurity threats. The framework integrates compliance security, Identity and Access Management (IAM), micro-segmentation and real time monitoring to prevent unauthorized access. This model is aligned with frameworks as NIST 800-207 for ZTA. Moreover, it compares Oracle components that serve crucial areas compliance security, user protection, password authentication, and data security in Oracle ERP Cloud [54].

F. Wei et al. (2024) proposed a security architecture for power monitoring system based on Zero Trust, which combines the power monitoring system with the three major technologies of Zero Trust SDP+IAM+MSG to form a comprehensive security protection program and provide multi-level security protection. The architecture effectively improves the overall security of the power system, which can cope with modern complex security challenges and protect critical power infrastructure from various network threats and attacks [55].

R. Singh et al. (2023) proposed that the 6G network's intelligent orchestration and management are essential components. Consequently, the 6G paradigm that is being considered heavily relies on machine learning and artificial intelligence. Unfortunately, there are pros and cons to combining 6G with AI/ML, as AI has the potential to both enhance and undermine privacy and security. Future network automation, proactive threat detection, and intelligent mitigation strategies are necessary to create autonomous networks in 6G. Because of this, the paper delves further into the 6G-based projects that are now underway and the reasons why 6G technology is essential [56].

F. A. Qazi (2022) examined zero trust as it pertains to network architecture security as opposed to conventional perimeter security. Also included is a synopsis of various software solutions that can be used to establish zero trust network access (ZTNA) for distant users to securely access apps and services. Additionally, the author discusses a synopsis of the qualitative study titled "Insecure Application Programming Interface in Zero Trust Networks" in this section. The research confirmed that zero trust is becoming more popular for network security and warding off cybercriminals. Also, most companies don't know that APIs exist in zero trust environments, which makes them vulnerable, according to the study [57].

According to Table I, Zero-Trust Security Enforcement is a summary of AI-Powered Anomaly Detection in Cloud Systems including applications, zero-trust components, monitoring approach, contributions and challenges

TABLE I. COMPARATIVE ANALYSIS OF ANOMALY DETECTION IN ZERO-TRUST SECURITY

Author(s) & Year	Application Domain	Zero Trust Components	Monitoring Approach	Key Contributions	Limitations
S. Ghimire (2026)	PLCs in food processing (Industrial Control Systems)	AI-integrated Zero Trust, adaptive trust evaluation	Passive behavioral observation, network-level continuous monitoring	Proposed AI-driven adaptive trust architecture for PLCs without modifying hardware/control logic; enhances visibility while preserving safety and availability	Conceptual model; lacks empirical validation and real-world deployment results
A. Qazi & S. Arshad (2025)	Oracle ERP Cloud (Enterprise Cloud Systems)	IAM, micro-segmentation, compliance security, real-time monitoring (aligned with NIST 800-207)	Real-time monitoring of user access and transactions	ZTA-based framework tailored for Oracle ERP Cloud; integrates compliance and identity security mechanisms	Focuses more on access control than advanced anomaly detection techniques
F. Wei et al. (2024)	Power monitoring systems (Critical Infrastructure)	SDP + IAM + MSG under Zero Trust framework	Multi-layered security monitoring across network and system levels	Developed multi-level Zero Trust security architecture for protecting power infrastructure from cyber threats	Limited discussion on AI-based anomaly detection or adaptive trust scoring
R. Singh et al. (2023)	6G Networks (Next-generation communication systems)	AI/ML-enabled intelligent orchestration (Zero Trust-aligned concepts)	AI-driven proactive threat detection and network automation	Highlighted importance of AI in proactive threat detection and autonomous 6G network security	Not specifically focused on Zero Trust architecture implementation
F. A. Qazi (2022)	Network Architecture & ZTNA (Remote Access Systems)	Zero Trust Network Access (ZTNA), secure access solutions	Application-level and API-level security analysis	Reviewed ZTNA solutions and identified insecurity of APIs in Zero Trust environments	Primarily qualitative review; lacks quantitative anomaly detection models

VI. CONCLUSION AND FUTURE WORK

Zero Trust Security, when fortified with AI-powered with AI-driven anomaly detection added to it, Zero Trust Security is a radical concept in cloud security, which offers uninterrupted authentication of users, devices, and applications to minimize the attack surface and overcome dynamic cyber threats. This paper has discussed the development and use of ZTA in the cloud platform and explained why AI-based anomaly detection is the most important component in enhancing the current cybersecurity systems. Zero Trust removes lateral movement by reducing attack surfaces through continuous authentication, least-privilege access, micro-segmentation, and real-time monitoring by moving away from the perimeter-based defenses and adopting a never trust, always verify model. The combination of machine learning and deep learning methods leads to the increased ability to detect abnormal behavior, identify new threats, and dynamically adapt security policies. Although conventional detection solutions can still be beneficial in the presence of known threats, AI-based solutions offer the intelligence and scalability needed in complicated and dynamically changing cloud environments. Although there are difficulties in the way of technical complexity, organizational resistance, cost reduction, and regulatory compliance, the integration of Zero Trust and AI offers a robust and flexible, and future-oriented security paradigm. After all, adapting AI-enhanced Zero Trust Architecture could allow organizations to proactively address the risks and protect the critical assets, as well as retain the trust in more distributed and cloud-based digital infrastructures.

Further studies will also be based on creating adaptive AI-based trust scoring models to evaluate risks in real-time in multi-cloud setting. The focus will be put on federated learning (privacy-preserving anomaly detection), explainable AI (transparent decision-making), and automated policy orchestration (better scalability, interoperability, and regulatory compliance in dynamic Zero Trust frameworks).

REFERENCES

[1] S. Garg, "Predictive Analytics and Auto Remediation using Artificial Inteligence and Machine learning in Cloud Computing Operations," *Int. J. Innov. Res. Eng. Multidiscip. Phys. Sci.*, vol. 7, no. 2, 2019.

[2] G. Maddali, "Intelligent Resource Allocation in Cloud Environment via ML- Based Optimization Methods," in *2025 IEEE 2nd International Conference on Information Technology, Electronics and Intelligent Communication Systems (ICITEICS)*, IEEE, Aug. 2025, pp. 1–8. doi: 10.1109/ICITEICS64870.2025.11341444.

[3] G. Maddali, "An Efficient Bio-Inspired Optimization Framework for Scalable Task Scheduling in Cloud Computing Environments," *Int. J. Curr. Eng. Technol.*, vol. 15, no. 3, pp. 229–238, 2025.

[4] V. K. Sharma, "Cloud Computing IoT: 5G Focused IoT with Cloud Solutions," *Int. J. AI, BigData, Comput. Manag. Stud.*, vol. 6, no. 3, 2025, doi: 10.63282/3050-9416.IJAIBDCMS-V6I3P103.

[5] U. A. Butt *et al.*, "A review of machine learning algorithms for cloud computing security," *Electronics (Switzerland)*. 2020. doi: 10.3390/electronics9091379.

[6] L. Wang *et al.*, "Cloud computing: A perspective study," in *New Generation Computing*, 2010. doi: 10.1007/s00354-008-0081-5.

[7] R. Tandon and D. Patel, "Evolution of Microservices Patterns for Designing HyperScalable Cloud-Native Architectures," *ESP J. Eng. Technol. Adv.*, vol. 1, no. 1, pp. 288–297, 2021, doi: 10.56472/25832646/JETA-V1I1P131.

[8] S. Garg, "Next-Gen Smart City Operations with AIOps & IoT : A Comprehensive look at Optimizing Urban Infrastructure," *J. Adv. Dev. Res.*, vol. 12, no. 1, 2021.

[9] R. Patel, "Advancements in Renewable Energy Utilization for Sustainable Cloud Data Centers : A Survey of Emerging Approaches," *Int. J. Curr. Eng. Technol.*, vol. 13, no. 5, pp. 447–454, 2023.

[10] S. B. Shah, B. Boddu, N. Prajapati, and S. A. Pahune, "AI-Powered Advanced Intrusion Detection for Securing Cloud Environments Against Network Attacks," in *2025 Global Conference in Emerging Technology (GINOTECH)*, IEEE, May 2025, pp. 1–7. doi: 10.1109/GINOTECH63460.2025.11076673.

[11] A. Syed, "Best Practices for Application Security," in *Supply Chain Software Security*, Berkeley, CA: Apress, 2024, pp. 127–170. doi: 10.1007/979-8-8688-0799-2_4.

[12] K. M. R. Seetharaman and P. Yadav, "A Machine Learning Framework for Detecting and Mitigation of Cyber Threats in IoT Environments," in *2025 3rd International Conference on Inventive Computing and Informatics (ICICI)*, IEEE, Jun. 2025, pp. 1112–1119. doi: 10.1109/ICICI65870.2025.11069697.

[13] W. Ahmad, A. Rasool, A. R. Javed, T. Baker, and Z. Jalil, "Cyber Security in IoT-Based Cloud Computing: A Comprehensive Survey," *Electronics*, vol. 11, no. 1, p. 16, Dec. 2021, doi: 10.3390/electronics11010016.

[14] N. K. Prajapati, "Quantum Computing and Its Impact on Cryptographic Security," *Int. J. Innov. Sci. Res. Technol.*, vol. 10, no. 5, pp. 1–13, 2025.

[15] A. Imashev, "AI-Driven Zero-Trust Security Framework for Detecting Advanced Persistent Threats in Cloud Environments," *ICONIC Res. Eng. JOURNALS*, vol. 9, no. 5, pp. 477–491, 2025.

[16] S. Garg, "AI/ML Driven Proactive Performance Monitoring, Resource Allocation and Effective Cost Management in SAAS Operations," *Int. J. Core Eng. Manag.*, vol. 6, no. 6, pp. 263–273, 2019.

[17] R. Tandon, J. Thomas, K. V. Vedi, and S. Gupta, "Prediction and Anomaly Detection Methods Based on Artificial Intelligence Techniques in Supply Chain Management," in *2025 International Conference on Information, Implementation, and Innovation in Technology (I2ITCON)*, IEEE, Jul. 2025, pp. 1–7. doi: 10.1109/I2ITCON65200.2025.11210612.

[18] A. Syed, "AI-Powered Threat Detection and Mitigation," in *Supply Chain Software Security*, Berkeley, CA: Apress, 2024, pp. 249–287. doi: 10.1007/979-8-8688-0799-2_6.

[19] S. Sarkar, G. Choudhary, S. K. Shandilya, A. Hussain, and H. Kim, "Security of Zero Trust Networks in Cloud Computing: A Comparative Review," *Sustainability*, vol. 14, no. 18, p. 11213, Sep. 2022, doi: 10.3390/su141811213.

[20] H. Attou *et al.*, "Towards an Intelligent Intrusion Detection System to Detect Malicious Activities in Cloud Computing," *Appl. Sci.*, vol. 13, no. 17, p. 9588, Aug. 2023, doi: 10.3390/app13179588.

[21] S. B. Shah, "Advanced Machine Learning Models for Anti-Money Laundering (AML): Improving Detection Accuracy and Efficiency," in *2025 1st International Conference on Secure IoT, Assured and Trusted Computing (SATC)*, IEEE, Feb. 2025, pp. 1–5. doi: 10.1109/SATC65530.2025.11137255.

[22] J. E. Kofi, "Data-Driven Cloud Workload Optimization Using Machine Learning Modeling for Proactive Resource Management," *Int. J. Emerg. Res. Eng. Technol.*, vol. 6, no. 4, pp. 27–37, 2025, doi: 10.63282/3050-922X.IJERET-V6I4P104.

[23] G. C. Madhu, S. Sivakumar, S. S. H. Raju, M. Sonia, K. Chakradhar, and S. Gupta, "Improving SCADA Cyber security: A Deep Learning Technique for Anomaly Detection," in *2025 IEEE International Conference on Emerging Technologies and Applications (MPSec ICETA)*, 2025, pp. 1–6. doi: 10.1109/MPSecICETA64837.2025.11118388.

[24] A. Syed and M. I. Ahmad, "Advanced Data Collection Techniques in Cloud Security: A Multi-Modal Deep Learning Autoencoder Approach," *ArXiv*, pp. 13, Nov, 2025, doi: 10.20944/preprints202510.0767.v1.

[25] N. K. Prajapati, "Cloud-based serverless architectures: Trends, challenges and opportunities for modern applications," *World J. Adv. Eng. Technol. Sci.*, vol. 16, no. 1, pp. 427–435, Jul. 2025, doi: 10.30574/wjaets.2025.16.1.1225.

[26] Chitiz Tayal, "Designing Hybrid ETL Pipelines for Multi-Cloud Integration," *Int. J. Emerg. Trends Comput. Sci. Inf. Technol.*, vol. 4, no. 4, pp. 129–134, 2023, doi: 10.63282/3050-9246.IJETCSIT-V4I4P114.

[27] N. Aniya and K. Ashokkumar, "Improving Trust Assessment Through ZTA Adaptation in Cloud Computing Environment," in *2025 IEEE 7th International Conference on Computing, Communication and Automation (ICCCA)*, IEEE, Nov. 2025, pp. 1–6. doi: 10.1109/ICCCA66364.2025.11325679.

[28] D. Patel and R. Tandon, "Cryptographic Trust Models and Zero-Knowledge Proofs for Secure Cloud Access Control and Authentication," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 2, no. 1, pp. 749–758, Dec. 2022, doi: 10.48175/IJARSCT-7744D.

[29] G. Maddali, "Zero Trust Security Architectures for Large-Scale Cloud Workloads," *SSRN Electron. J.*, vol. 5, no. 2, pp. 960–965, 2025, doi: 10.2139/ssrn.5365222.

[30] G. Martinović, I. Ivković, D. Verber, and T. Bačun, "Effect of Data Preparation on Machine Learning Models for Diabetes Prediction," in *OTO 2025*, MDPI, Jan. 2026, p. 13. doi: 10.3390/engproc2026125013.

[31] 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, 2023.

[32] R. K. Rajendran, T. Mohana Priya, S. Goundar, K. R. Madhavi, J. Avanija, and B. R. Avula, "Zero Trust Architecture in Cloud Security," in *Convergence of Cybersecurity and Cloud Computing*, 2025, pp. 515–530. doi: 10.4018/979-8-3693-6859-6.ch024.

[33] G. Lakshmikanthan, S. S. Nair, J. Partha Sarathy, S. Singh, S. Santiago, and B. Jegajothi, "Mitigating IoT Botnet Attacks: Machine Learning Techniques for Securing Connected Devices," in *2024 International Conference on Emerging Research in Computational Science (ICERCS)*, IEEE, Dec. 2024, pp. 1–6. doi: 10.1109/ICERCS63125.2024.10895253.

[34] 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.

[35] S. P. Kalava, "Building Trust in AI: Ethical Principles for Transparent Autonomous Systems," *J. Artif. Intell. Mach. Learn. Sata Sci.*, vol. 2,

no. 2, 2024.

[36] V. K. Sharma, "AI-Based Anomaly Detection for 5G Core and RAN Components," *Int. J. Sci. Res. Eng. Manag.*, vol. 6, no. 1, pp. 1–6, 2022.

[37] M. Reddiar and K. Seetharaman, "Advanced Artificial Intelligence Methods for Intrusion Identification to Increase Cybersecurity in Insights of IoT Applications," in *16th International IEEE Conference on Computing, Communication and Networking Technologies (ICCCNT)*, 2025.

[38] S. B. Shah, "Advancing Financial Security with Scalable AI: Explainable Machine Learning Models for Transaction Fraud Detection," in *2025 4th International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE)*, 2025, pp. 1–7. doi: 10.1109/ICDCECE65353.2025.11034838.

[39] S. Singh, S. A. Pahune, P. Chatterjee, and R. Sura, "Advanced Machine Learning Methods for Churn Prediction and Classification in Telecom Sector," in *2025 IEEE 6th India Council International Subsections Conference (INDISCON)*, 2025, pp. 1–7. doi: 10.1109/INDISCON66021.2025.11252233.

[40] R. Dattangire, D. Biradar, R. Burle, L. Dewangan, and A. Joon, "Machine Learning Approaches to Safeguarding Health Insurance Against Fraudulent Claims," in *Advances in Data-Driven Computing and Intelligent Systems*, 2026, pp. 341–353.

[41] D. Patel, "The Role of Amazon Web Services in Modern Cloud Architecture: Key Strategies for Scalable Deployment and Integration," *Asian J. Comput. Sci. Eng.*, vol. 9, no. 4, 2024, doi: 10.22377/ajcse.v9i04.215.

[42] A. B. Nassif, M. A. Talib, Q. Nasir, and F. M. Dakalbab, "Machine Learning for Anomaly Detection: A Systematic Review," *IEEE Access*. 2021. doi: 10.1109/ACCESS.2021.3083060.

[43] R. P. Mahajan and N. Jain, "Deep Learning Techniques for Identification of Parkinson's Disease based on MRI Data: Novel Diagnostic Framework," in *2025 International Conference on Intelligent Computing and Knowledge Extraction (ICICKE)*, Jun. 2025, pp. 1–7. doi: 10.1109/ICICKE65317.2025.11136577.

[44] R. Patel, "Automated Threat Detection and Risk Mitigation for ICS (Industrial Control Systems) Employing Deep Learning in Cybersecurity Defence," *Int. J. Curr. Eng. Technol.*, vol. 13, no. 06, pp. 584–591, Dec. 2023, doi: 10.14741/ijcet/v.13.6.11.

[45] S. Singh, "Advancing Network Security in 5G: Leveraging the 5G-NIDD Dataset for Intrusion Detection and Mitigation," in *2025 IEEE 12th International Conference on Cyber Security and Cloud Computing (CSCloud)*, IEEE, Nov. 2025, pp. 1–6. doi: 10.1109/CSCloud66326.2025.00055.

[46] D. Patel, "Leveraging Blockchain and AI Framework for Enhancing Intrusion Prevention and Detection in Cybersecurity," *Tech. Int. J. Eng. Res.*, vol. 10, no. 6, 2023, doi: 10.56975/tijer.v10i6.158517.

[47] S. P. Kalava, "AI-Powered Development: How Artificial Intelligence is Shaping Software Productivity," *J. Artif. Intell. Cloud Comput.*, vol. 3, no. 2, pp. 1–4, Apr. 2024, doi: 10.47363/JAICC/2024(3)E148.

[48] K. M. R. Seetharaman, "Incorporating the Internet of Things (IoT) for Smart Cities: Applications, Challenges, and Emerging Trends," *Asian J. Comput. Sci. Eng.*, vol. 8, no. 1, pp. 8–14, 2023.

[49] R. Patel, "Optimizing Communication Protocols in Industrial IoT Edge Networks: A Review of State-of-the-Art Techniques," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 4, no. 19, pp. 1–12, 2023.

[50] R. Patel, "Artificial Intelligence-Powered Optimization of Industrial IoT Networks Using Python-Based Machine Learning," *J. Eng. Technol. Adv.*, vol. 3, no. 4, pp. 138–148, 2023, doi: 10.56472/25832646/JETA-V3I8P116.

[51] R. Patel, "Security Challenges in Industrial Communication Networks: A Survey on Ethernet/IP, Controlnet, and Devicenet," *Int. J. Recent Technol. Sci. Manag.*, vol. 7, no. 8, pp. 54–63, 2022.

[52] S. Arora and A. Tewari, "Zero trust architecture in IAM with AI integration," *IJSRA*, vol. 08, no. 02, pp. 737–745, 2023.

[53] S. Ghimire, "AI-Assisted Zero Trust Architecture for Continuous Risk Assessment of Programmable Logic Controllers in Food Processing Infrastructure," in *2026 IEEE 5th International Conference on AI in Cybersecurity (ICAIC)*, IEEE, Feb. 2026, pp. 1–5. doi: 10.1109/ICAIC67076.2026.11395864.

[54] A. Qazi and S. Arshad, "Implementation of Enhanced Security Measures in Oracle ERP Cloud with Zero Trust Architecture (ZTA)," in *2025 International Conference on Communication Technologies (ComTech)*, IEEE, Apr. 2025, pp. 1–6. doi: 10.1109/ComTech65062.2025.11034488.

[55] F. Wei *et al.*, "Research on the Security of Electric Power Monitoring System Based on Zero Trust Architecture," in *2024 7th International Conference on Mechatronics and Computer Technology Engineering (MCTE)*, IEEE, Aug. 2024, pp. 890–894. doi: 10.1109/MCTE62870.2024.11118024.

[56] R. Singh, G. Srivastav, R. Kashyap, and S. Vats, "Study on Zero-Trust Architecture, Application Area Challenges of 6G Technology in Future," in *2023 International Conference on Disruptive Technologies (ICDT)*, IEEE, May 2023, pp. 375–380. doi: 10.1109/ICDT57929.2023.10150745.

[57] F. A. Qazi, "Study of Zero Trust Architecture for Applications and Network Security," in *IEEE 19th International Conference on Smart Communities: Improving Quality of Life Using ICT, IoT and AI, HONET 2022*, 2022. doi: 10.1109/HONET56683.2022.10019186.