International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(10s) 2026 pp. 1046-1055
https://doi.org/10.70917/ijcisim-2026-3695
Article

Survey of Allaying Vulnerabilities for Cloud based Security in Zero Trust Architecture

Maulik Dhamecha [1], Urvi Dhamecha [2], Aswathy R Nair [3], Hansa Vaghela [4], Ravi J. Khimani [5], Shyam Kotecha [6]

[1] Department of Computer Engineering, V.V.P. Engineering College, Rajkot, Gujarat. mvdhamecha@gmail.com
[2] Department of Computer Engineering, Marwadi University, Rajkot, Gujarat, urvidarji17@gmail.com
[3] Department of Computer Engineering, Marwadi University, Rajkot, Gujarat. arn.aswathy@gmail.com
[4] Department of Computer Engineering, Marwadi University, Rajkot, Gujarat. vaghelahansa315@gmail.com
[5] Computer Engineering, Government Engineering College, Rajkot, Gujarat. ravikhimani.gec@gmail.com
[6] Computer Engineering, Government Engineering College, Rajkot, Gujarat. shyamkotecha.gec@gmail.com

Abstract: Zero Trust Architecture is currently the primary security framework used in cloud-based systems. ZTA is a far cry from the old school perimeter security models which rely on strong identity verifications and monitoring in order to prevent security risks and vulnerabilities. This paper looks at the vulnerabilities that exist in Zero Trust models and solution approaches that would improve the security of the cloud. Some of the major security threats examined include insider threats, configuration risks, and Advanced Persistent Threats (APT). AI-driven and policy-based solutions are proposed to bolster Zero Trust frameworks.
Keywords: Zero Trust Architecture, Cloud Security, Identity Verification, Insider Threats, AI in Security, Policy-Based Security.

1. Introduction

Zero Trust Architecture (ZTA) has proven to be one of the most influential cybersecurity models that can help secure the cloud computing ecosystem today [1], [2]. Whereas traditional cybersecurity methodologies rely on the assumption that users and devices that operate inside the company's network infrastructure can be trusted, ZTA makes use of authentication, authorization, and continuous verification of every access request made [1]. The primary premise of ZTA model, which can be described as “never trust, always verify” concept, is that no user, device, application, or workload can be considered trustworthy by default regardless of whether it operates inside or outside of the company network infrastructure [1], [3]. Such cybersecurity strategy becomes particularly relevant as companies continue to digitally transform and migrate their services to the cloud environment [2], [4].

The emergence of cloud computing technology has completely revolutionized the implementation of information systems in today’s world [4]. There are many benefits offered by cloud computing technology, which includes scalability, flexibility, cost efficiency, and instant availability of resources [4]. The usage of cloud computing technology has led to new attack vectors for cyber criminals [5]. Modern organizations extensively use distributed computing technologies, remote employees, mobile devices, IoT devices, third-party vendors, and applications designed to be used in the cloud environment [5], [6]. All these things present many security issues to an organization that cannot be addressed using conventional perimeter-based security models [2], [5]. Therefore, there are now many cyberattacks like ransomware attacks, phishing attacks, identity theft, insider threats, supply chain attacks, and APTs [5], [6].

The traditional security model has been developed considering that everything residing within the corporate network perimeter is considered to be trustworthy, while the threats were mainly coming from outside [7]. The security tools such as firewall, virtual private network, and IDS have been deployed in order to secure the perimeter of the network [7]. But this kind of security model is no longer useful because of the increasing trend of using the cloud services and remote access technologies [2], [7]. When the attackers manage to penetrate into the network by compromising credentials, vulnerable applications, or any insider threat, they get free lateral movement [6], [7].

In order to overcome such drawbacks, the Zero Trust Architecture implements a security model which involves the verification of all users, devices, applications, and network transactions continuously [1], [3]. Unlike the traditional security system where the access to systems is provided by a single authentication process, the Zero Trust Architecture ensures that access control remains dynamic and dependent upon several factors like identity of users, health of devices, context, behavior, and risk evaluation [1], [3]. Some of the fundamental aspects of the Zero Trust Architecture include identity and access management, multi-factor authentication (MFA), least-privilege access, micro-segmentation, continuous monitoring, endpoint security, encryption, and policy-based authorization [1], [3], [8].

Today, identity has emerged as the new security perimeter in cloud computing environments [8]. In light of the above, governance and management of identity and access have become important aspects of Zero Trust deployment [8]. Solutions such as IAM, PAM, SSO, adaptive authentication, and behavioural analysis have become important for making sure that only trusted identities get access to organizational resources [8], [9]. Additionally, Zero Trust is capable of constantly monitoring the behaviour of the users and taking actions when unusual behaviour is identified or when sessions are compromised [9].

However, although ZTA offers various benefits, there exist some technical difficulties associated with the deployment of the framework [2], [10]. For example, many organizations use legacy technologies which were not originally developed to meet the requirements of contemporary authentication methods and advanced access control policies [10]. Implementing ZTA may require making considerable efforts in terms of deploying new security measures, reconfiguring the network, defining appropriate policies, and training staff members [10]. Furthermore, the process of ensuring continuous authentication and authorization may be costly due to the additional load on the network performance and increased complexity of managing policy administration [10].

A number of other weaknesses still persist in the Zero Trust environment [6], [9]. One such issue is insider threats since there is always the possibility that the user with authorized access may use it for malicious purposes [6]. Inadequate security policies, poor management of identities, unsecured APIs, compromised endpoints, software bugs, and lack of visibility in cloud environments can seriously undermine the effectiveness of Zero Trust deployments [6], [9]. The increasing use of technologies such as containers, microservices, serverless applications, and multi-cloud platforms is also adding to the security challenges [4], [9].

Zero Trust Architecture can be strengthened by the use of AI, ML, and automation technologies [11], [12]. Security analysis based on AI helps organizations handle huge amounts of security events, detect anomalies, and discover sophisticated attack vectors much more quickly and accurately than traditional rule-based systems do [11]. ML algorithms are capable of analysing user behaviour, network traffic, endpoint activity, and authentication patterns to find deviations from normal behaviour and detect threats [11], [12]. SOAR platforms also provide help in enhancing Zero Trust architecture since they allow responding to security events quickly and without any human intervention [12].

However, since cybersecurity risks are ever evolving and new technologies are being invented, Zero Trust Architecture has to be able to adapt to the latest changes as well [2], [12]. Future research will concentrate around AI-driven trust assessment, privacy-focused authentication, blockchain-enabled identity management, quantum-proof cryptography, autonomous policy enforcement, and intelligent threat prediction [12], [13]. These innovations can bring even more benefits to Zero Trust Architectures in the cloud environment [13].

2. Key Vulnerabilities in Zero Trust Architecture

Zero Trust Architecture (ZTA), despite its ability to bolster security measures by doing away with implicit trust and introducing continuous authentication and authorization, is also vulnerable to security issues [14], [15]. The success of ZTA greatly depends on correct implementation, monitoring, identity management, and policy enforcement [14]. Configuration errors, advanced cyber-attacks, insider threats, and operational challenges may negatively impact the implementation of Zero Trust architecture, especially in large scale cloud-based settings [16], [17]. In light of increasing hybrid and multi-cloud infrastructures among enterprises, the identification of such vulnerabilities becomes vital for creating secure architectures [18]. The following are some of the key vulnerabilities that hinder the implementation of ZTA.

2.1 Insider Threats

Insider threats continue to be among the major sources of security threats in Zero Trust networks due to the fact that insider threats emanate from people who have legitimate access to the organization's information assets [19]. The insiders can be employees, contractors, third parties, or business associates who either use their legitimate access to

gain some personal or financial advantage [19]. Intentional insider threats can include stealing of confidential information, manipulating sensitive information, sabotaging important systems, or leaking intellectual property information [19]. Unintentional insider threats can emanate from human error like falling prey to phishing scams [20].

Even though the concept of Zero Trust is built on strict identity verification and least privilege access control, there is no doubt that the users who are authorized to access sensitive information also possess legitimate permissions that can be misused in case if their accounts are hacked or in case they try to misuse their permissions [14], [19]. Thus, companies need to conduct behavioral monitoring, PAM, UEBA, and privileges reviews [21].

2.2 Misconfigurations

Misconfiguration is one of the major contributors to security threats in cloud computing environment [16]. The Zero Trust Architecture depends on accurate configuration of its security policies, identity rules, authentication systems, network segregation, and access controls [14]. Small configuration mistakes can lead to security vulnerabilities, which can be exploited by the attacker [16].

Misconfiguration issues can be seen in poorly configured firewalls, poor identity management policies, excessive user privileges, exposure of cloud storage to the public, disabling of security logging, and weak encryption mechanisms [16]. Large companies run their systems through various cloud providers who have different security tools and therefore it becomes hard to ensure proper configuration management [18]. It can create vulnerabilities which will bypass Zero Trust [16], [18].

Automated configuration checking, Infrastructure as Code (IaC), compliance monitoring, security auditing, and configuration management are key tools to mitigate such threats by automatically detecting and resolving policy violations [22].

2.3 Advanced Persistent Threats (APTs)

APT attacks are very sophisticated and targeted cyber attacks carried out by well-financed attackers, such as nation-states and cyber-criminal organizations [23]. Contrary to conventional cyber attacks which are focused on disrupting operations in the immediate, APTs seek to gain access and maintain a prolonged presence without being detected [23].

APT attack methods normally start with phishing, software exploitation, compromised credentials, or supply chain exploitation to get into the system initially [23]. Then after gaining access, they use techniques such as stealing credentials, privilege escalation, lateral movements, malware deployment, and data exfiltration [23]. Despite being in a zero trust environment, APT can still use the legitimate credentials and applications to go unnoticed [14], [23].

Detection of APTs involves monitoring, artificial intelligence driven anomaly detection, endpoint detection and response, traffic analysis, threat intelligence, and automated response [24]. The following are the capabilities that allow organizations to detect malicious activity patterns before the breach of important assets [24].

2.4 Lack of Visibility

Visibility of all users, devices, applications, workloads, and network traffic is critical in the implementation of the Zero Trust strategy [14], [21]. The absence of a central monitoring and logging system makes it difficult for organizations to identify any malicious actions taking place in real time [21]. Lack of visibility of cloud assets will only delay any identification of an attack that might be under way [21].

Most modern organizations maintain a complex infrastructure that is based on several cloud service providers and includes remote users, IoT devices, virtual machines, containers, and even edge computing services [18]. Keeping track of all processes taking place within such an environment is rather difficult [18]. In the absence of centralized dashboards and security analytics, security personnel may fail to notice any abnormalities within their networks [21].

In order to overcome this problem, companies need to use centralized Security Information and Event Management systems (SIEM), Security Orchestration, Automation and Response systems (SOAR), continuous endpoint monitoring, and cloud native security monitoring tools [21], [24].

2.5 API Security Issues

Application Programming Interfaces (APIs) are important aspects of today's cloud-based applications because they allow interaction between users, applications, cloud services, and third party applications [25]. On the other hand,

APIs have become one of the main attack vectors for hackers since they provide direct access to critical business assets [25].

Insecure API can lead to exposing of sensitive information, allowing an attacker to get unauthorized access to accounts, perform privilege escalation, or manipulate critical transactions [25]. The most common vulnerabilities associated with API are poor authentication, insecure API keys, excessive permissions, broken access control, inadequate input validation, insecure data transfer, and the absence of rate limiting [25]. Such vulnerabilities are usually exploited by attackers using API abuse, credential stuffing, and injection attacks [25].

Organizations need to develop secure APIs, utilize robust authentication based on OAuth 2.0 and Multi-factor authentication, secure the communication between APIs, constantly monitor APIs, and conduct vulnerability assessments to reduce risks associated with APIs [25].

2.6 Identity and Access Management (IAM) Flaws

Identity and Access Management (IAM) is the basis of Zero Trust Architecture since all decisions made to grant or deny access to resources are based on identity and authorization checks [14], [15]. Inefficient IAM implementation will make Zero Trust Security Controls less effective [15].

The common IAM weaknesses comprise weak passwords, lack of sufficient MFA, overprivileged, orphaned accounts, incorrect role assignment, and ineffective identity governance [15]. Hackers often take advantage of compromised credentials by stealing them through phishing attacks, credential stuffing, and password reuse [20].

It is important for organizations to use the least privilege principle, adaptive authentication, review user privileges regularly, automate identity lifecycle management, and monitor authentication actions in order to ensure that only authorized users can have access to the critical data [15], [21].

2.7 Inconsistent Policy Enforcement

The challenge of maintaining coherent security policies in hybrid/multi-cloud deployments is one of the hardest parts of implementing Zero Trust architecture [18]. Organizations implement applications in several clouds while at the same time they have infrastructure on-premise [18]. Every deployment may use different security technology, identity providers, access controls, and compliance [18].

These discrepancies may lead to policy contradictions and security weaknesses that can be exploited by malicious parties [18]. For instance, a user, who was denied access in one cloud, may inadvertently have too many permissions in another due to policy inconsistency [18].

In order to address the above-mentioned concerns, it is important for businesses to use centralized policy management systems, automated compliance checking systems, unified identity solutions, CSPM, and standardized security governance structures that ensure enforcement of policies uniformly throughout all environments [18], [22].

In conclusion, the identified weaknesses prove that the implementation of Zero Trust Architecture alone does not provide total cybersecurity of a business organization [14], [15]. The effective implementation of Zero Trust Architecture implies the need to constantly improve it and conduct intelligent monitoring along with identity governance, compliance validation, and threat detection [14], [21]. Using Artificial Intelligence, Machine Learning, behavioural analysis, security automation, and real-time monitoring makes it possible to detect new threats and reduce the attack surface in the context of cyberattacks [24].

Here is a comparative study that summarizes the above criteria based on their focus area, contribution, and relevance to Zero Trust Architecture (ZTA).

Table-1: Comparative Analysis of Related Works on Zero Trust and Cloud Security

Ref.	Focus Area	Key Contribution	Relevance to ZTA
[14]	Zero Trust Architecture	Introduced the NIST Zero Trust reference architecture and core principles such as continuous verification and least-privilege access.	Very High
[15]	ZTA deployment	Provided practical guidance for implementing Zero Trust in enterprise environments.	Very High

[16]	Cloud security guidance	Identified critical cloud security domains, including IAM, data protection, and governance.	High
[17]	Cloud attack survey	Reviewed major cyber-attacks and security challenges affecting cloud computing environments.	High
[18]	Hybrid and multi-cloud security	Discussed security best practices for managing distributed cloud infrastructures and policy consistency.	High
[19]	Insider threat mitigation	Presented strategies for detecting and mitigating malicious and unintentional insider threats.	High
[20]	Data breach analysis	Provided statistical analysis of real-world breach patterns, credential attacks, and phishing incidents.	Medium
[21]	SIEM and threat detection	Described best practices for centralized monitoring, log analysis, and threat detection.	High
[22]	IaC security	Explained secure Infrastructure as Code practices and automated configuration validation.	High
[23]	Advanced Persistent Threats	Reported current attacker tactics, techniques, and procedures (TTPs) observed in real incidents.	High
[24]	AI-driven cybersecurity	Highlighted the role of AI and ML in anomaly detection, predictive security, and automated response.	Very High

Key observations

- ZTA foundational references: [14] and [15] outline the architecture and deployment framework for Zero Trust.
- Security and governance in the Cloud: [16], [18], and [22] stress secure Cloud configuration, governance, and policy management in multi-cloud environment.
- Studies focusing on threats: [17], [19], [20], and [23] discuss cyber-attacks, insider threats, breaches, and APT techniques.
- Monitoring and intelligence: [21] and [24] deal with centralized monitoring, SIEM, intelligent threat detection using AI/ML and automated incident response capabilities.

3. Solution-Oriented Approaches to Strengthen ZTA

Effectiveness of Zero Trust Architecture (ZTA) does not only lie in the adoption of the "never trust, always verify" principle but also involves the deployment of a holistic approach towards security through deploying mechanisms tailored to the dynamic nature of cyber-attacks [26], [27]. As organizations move their applications and information to public, private, hybrid, and multi-cloud infrastructures, security measures must be continually refined to counteract new attack methodologies, advanced malware infections, insider attacks, and cloud-native vulnerabilities [28], [29]. For an effective ZTA deployment, a combination of intelligent security solutions, continuous monitoring, robust identity management, automated policy enforcement, and risk assessment are necessary [26], [30]. The following approaches are key in enhancing ZTA effectiveness.

3.1 AI-Driven Threat Detection

AI and ML are two technologies that play a critical role in enhancing Zero Trust security [31], [32]. Conventional security mechanisms based on rules do not work effectively to detect complex cyber-attacks that change quickly and use newly discovered loopholes [31]. Artificial intelligence-enabled security technologies analyze huge amounts of security logs, authentication attempts, network communications, device interactions, and user behavior looking for any suspicious actions [31], [32].

Machine learning technologies define normal behavioral models for users, devices, and applications [31]. Any discrepancy from the normal models in form of unusual login times, geographic positions, data transmissions, or privileges escalation is recognized as a potential security threat [31]. AI-based SIEM and UEBA technologies help organizations to discover insider threats, ransomware infections, stealing of credentials, and APT attacks in real-time manner [30], [31]. Additionally, AI improves accuracy of threat detection, speed of the process, and relieves cybersecurity experts from additional tasks [31].

3.2 Policy-Based Access Control (PBAC)

Dynamic and context-based authorization is enabled by Policy-Based Access Control (PBAC), which adds to the flexibility of Zero Trust Architecture [33]. As compared to the static access control framework, PBAC takes into account various contextual factors to allow access, such as user identity, device condition, user's location, sensitivity of the application, network condition, time of access, and risk level [33].

It is recommended for organizations to implement Policy-Based Access Control (PBAC) along with Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) for better authorization capabilities [33], [34]. In Role-Based Access Control (RBAC), permission is granted to a user on the basis of organizational roles, while in Attribute-Based Access Control (ABAC), intelligent decision is made using attributes of the user, resource, and environment [34]. This enables an organization to apply the principle of least privilege and adjust permissions accordingly as per the changing security posture [26], [34].

3.3 Multi-Factor Authentication (MFA)

Identity verification is a core pillar of the Zero Trust Architecture, where the implementation of Multi-Factor Authentication (MFA) ensures the protection against any kind of unauthorized access [26], [35]. The traditional password authentication method is no longer reliable due to the vulnerability of the passwords to phishing attacks, brute force attacks, credential stuffing, and social engineering [35].

The MFA process requires the users to authenticate their identities via two or more factors of identification before access is provided [35]. The factors of identification may include something the user knows (password or PIN code), something the user has (security token, smart card, or mobile authenticator), and something that the user is (fingerprint, facial or iris recognition) [35]. The modern adaptive MFA systems consider additional factors such as the device trustworthiness, user location, and behaviour [35].

3.4 Zero Trust Network Access (ZTNA)

Zero Trust Network Access (ZTNA) is a security model which supersedes traditional virtual private networks (VPNs) and offers a more secure and identity-based approach for access to a network [27], [36]. It ensures that not only do all requests for access get verified repeatedly but that the users have access to only those resources that they have been approved for [36].

ZTNA follows the concept of least privilege, micro-segmentation, and continuous verification during the entire user session [27], [36]. All access attempts are analyzed according to the identity of the user, the device posture, the sensitivity of the application, and the risk involved at that time [36]. In this way, ZTNA greatly reduces the opportunities available for lateral movement to attackers that manage to acquire user credentials [36]. ZTNA also allows for secure remote access for employees, contractors, and third-party vendors while securing the network infrastructure from being exposed [36].

3.5 Automated Compliance Monitoring

Continuous adherence to organizational security policies and compliance standards is crucial for the sustained success of Zero Trust strategies [26], [37]. Compliance checks done manually are usually inefficient, prone to errors, and incapable of keeping pace with dynamic cloud environments characterized by regular modifications to the infrastructure [37].

Automated compliance monitoring allows organizations to continuously assess their security configurations, access controls, identity policies, and cloud resources in accordance with selected compliance frameworks [37]. Security automation solutions send instant notifications each time any compliance violations or deviations from established security policies occur [37]. Automated tracking, logging, and reporting make compliance with regulations like ISO/IEC 27001, NIST Cybersecurity Framework, GDPR, HIPAA, and PCI-DSS much easier for organizations [37].

3.6 Enhanced API Security Measures

Application Programming Interfaces (APIs) act as the means of communication in current cloud-based applications and thus need to be secured [29]. As APIs expose the business logic and data to the outside world, hackers take advantage of such vulnerabilities and compromise the API in order to gain access or to manipulate the API in any manner [29].

It is recommended for businesses to have a secure API gateway where authentication, authorization, and filtering and validating of requests are done in a single place [29]. Encryption of data using Transport Layer Security (TLS), OAuth 2.0 authorization, JSON Web Tokens (JWT), rate limiting, and proper management of API keys are some of the practices that should be followed in all API implementation scenarios [29]. API penetration testing and vulnerability assessments can help in identifying the loopholes which hackers can utilize [29].

3.7 User Awareness and Security Training

The role of human error remains an important factor in the occurrence of cybersecurity events even as security technologies evolve [30]. Staff members often fall victim to phishing schemes, social engineering tricks, password stealing, and accidental data exposure [30]. Therefore, user awareness and cybersecurity education are integral parts of an effective Zero Trust policy [30].

It is necessary for organizations to organize periodic cybersecurity education sessions related to Zero Trust policies, password security, phishing detection, safe use of the Internet, security of sensitive data, and reporting of security incidents [30]. Phishing drills and cybersecurity drills allow staff to identify new techniques used by attackers while developing the proper response to cybersecurity events [30]. Such continuous training helps create a security-aware corporate culture where all employees contribute to asset protection [30].

3.8 Cloud Security Posture Management (CSPM)

With companies relying more on multi-cloud and hybrid cloud architectures, it gets increasingly difficult to ensure secure cloud configurations [28]. Cloud Security Posture Management tools constantly monitor the cloud environment in order to detect any potential misconfigurations of security parameters, non-compliance, too many permissions granted, open storage buckets, and insecure network configurations [28].

Cloud Security Posture Management solutions automatically compare deployed cloud assets with the best industry practices and regulatory requirements while providing suggestions on how to fix them [28]. Modern CSPM solutions also integrate with Infrastructure as Code, DevSecOps and cloud-native security offerings in order to provide continuous protection of security policies during the whole development process [28], [37].

In summary, achieving an enhanced Zero Trust Architecture calls for an approach that is holistic and continuous and does not involve using one security technology alone [26], [27]. The implementation of technologies such as Artificial Intelligence, Machine Learning, Policy Based Access Control, Multi Factor Authentication, Zero Trust Network Access, compliance automation, API security, effective user awareness initiatives and Cloud Security Posture Management helps organizations create highly resilient security ecosystems [26], [28], [31]. All these technologies work together to improve identity validation, reduce attack surfaces, improve threat detection abilities, enforce policies automatically and achieve continuous compliance in distributed cloud environments [26], [37]. With the changing nature of cyber attacks, organizations implementing these solution-driven technologies will be better suited to defend their critical infrastructure, maintain compliance and have a future-proofed Zero Trust Architecture [27], [31].

4. Future Directions and Recommendations

With the constant advancement in cloud computing technology, the Zero Trust Architecture (ZTA) must also keep pace with the advanced threats that may arise in future, evolving enterprise infrastructures, and new computing models [38], [39]. Though current zero trust architectures have been effective in increasing the security level of organizations through continuous authentication, least privilege principle and identity centric security, some technical and operational issues have yet to be solved [38]. Research work in the future must be done in order to develop intelligent, scalable and adaptive zero trust architecture that is based on new technologies and has excellent security, usability and compliance [39], [40].

AI-Augmented Zero Trust

AI and ML are set to make an enormous difference in terms of the future Zero Trust security model [41], [42]. Existing security systems respond to threats, but future Zero Trust security systems that have been enhanced by AI will need to concentrate on predictive cybersecurity that detects potential attacks even before any actual threat occurs [41]. An advanced AI system is able to analyse the activities of users, traffic, authentication events, endpoints, and threat intelligence feeds for the purpose of predicting attacks and initiating action accordingly [41], [42].

The use of AI technology in Security Orchestration, Automation and Response (SOAR) systems can greatly decrease the time needed for responding to security incidents and decrease human involvement in the process [41]. In

addition, the use of Explainable AI (XAI) should be considered when developing an AI-based cybersecurity system [42].

Adaptive Security Models

Traditional access control systems generally use static policies which may not be able to adapt quickly enough in response to changing security needs [43]. Adaptive security measures for future Zero Trust architectures should therefore use dynamically adjusted authentication and authorization policies according to current risk levels [43].

Risk-aware authentication processes should take into account various contextual elements such as user identity, health status of the device being used, geographical location, sensitivity of applications accessed, behavioral patterns, and threats [43]. As a result, if a user accesses sensitive information from an unusual location or a suspiciously compromised device, it can lead to additional authentication procedures or access constraints [43].

Cloud-Native Zero Trust Solutions

The fast adoption of cloud-native technologies, such as containers, Kubernetes, serverless computing, microservices, and edge computing, demands Zero Trust solutions that can effectively work in distributed cloud environments [44], [45]. Further research should be directed at creating cloud native Zero Trust systems that would work well in cloud environments without adding any unnecessary complexity [44].

Zero Trust solutions should include features like automated identity management, workload protection, authentication between services, micro-segmentation, and continuous monitoring in public, private, hybrid, and multi-cloud environments [38], [44]. Integrating Zero Trust with DevSecOps and IaC will allow for applying security controls within the software development process, making applications secure when deployed [45].

Standardization and Best Practices

Although the number of organizations that use Zero Trust Architecture continues to rise, different implementation approaches are utilized by organizations in their pursuit of adopting the architecture because there are no commonly recognized standards or deployment approaches [38], [46]. In the future, it is important for organizations to consider developing standards and implementation frameworks for Zero Trust Architecture [46].

It is critical for government organizations, international standard bodies, cloud providers, cyber security experts, and industry players to collaborate in order to establish standards for Zero Trust reference architectures [46]. These standards will cover identity and access management, policy enforcement, compliance, interoperability, and performance assessment [46], [47].

Enhanced API Security

With the rising reliance of cloud software on Application Programming Interfaces (APIs) in facilitating communication and integration of services, the importance of studying API security will persist as an area of research [48]. Intelligent solutions that provide API security through continuous monitoring of APIs, identifying suspicious requests, blocking unauthorized access, and protecting from automated attacks need to be included in future Zero Trust architectures [48].

Emerging technologies like artificial intelligence-based anomaly detection of APIs, automatic vulnerability detection, behavioral analysis, token-based authentication, and security API gateways need to be incorporated into Zero Trust architecture [41], [48]. Moreover, adoption of secure API development methods, continuous penetration testing, and runtime protections needs to be embraced [48].

Cross-Cloud Policy Consistency

In modern companies, the number of cloud platforms is constantly growing, and therefore, consistent enforcement of security policies becomes an urgent problem [39], [46]. Discrepancies between services offered by different cloud providers, their identity management systems, access management methods, and other security features become obstacles to proper Zero Trust implementation [39].

Further research should be concentrated on creating the framework for unified policy management, which will be able to enforce security policies consistently throughout hybrid and multi-cloud environments [39], [46]. Policy orchestration, compliance validation, CSPM, and consistent identity management are just several means to address configuration gaps [39], [46].

Finally, the success of the Zero Trust Architecture in the future depends on creating intelligent, adaptive, and cloud-native security solutions that can actively protect against cyber threats while managing more advanced and intricate digital systems [38], [39]. Artificial intelligence, adaptive risk-based authentication, implementation guidelines, API security, and cross-cloud policy management will make it possible for organizations to create effective and scalable ZTA environments that can address the increasing challenges in cybersecurity [41], [43], [46]. These research directions and new security tools will help build future-ready Zero Trust Architecture that can effectively protect cloud assets and provide compliance with regulations [38], [47].

5. Conclusion

The Zero Trust Architecture (ZTA) has emerged as an essential cybersecurity framework that offers secure cloud computing by shifting away from perimeter-based security to a model of "never trust, always verify." This study analyzed the major vulnerabilities associated with ZTA, including insider threats, misconfigurations, Advanced Persistent Threats (APTs), limited visibility, API security problems, IAM vulnerabilities, and policy enforcement inconsistencies. Additionally, solution-oriented concepts that included AI-based threat detections, Policy-Based Access Control (PBAC), Multi-Factor Authentication (MFA), Zero Trust Network Access (ZTNA), automation of compliance checking, Cloud Security Posture Management (CSPM), improved API security, and user awareness were analyzed. With the evolution of cloud computing, the inclusion of AI, adaptive security models, and continuous monitoring will further bolster the Zero Trust frameworks. Overall, implementing an adaptive and comprehensive Zero Trust framework is critical for enhancing cloud security and reducing cyber risks.

References

1. S. Rose, O. Borchert, S. Mitchell, and S. Connelly, Zero Trust Architecture, NIST Special Publication 800-207. Gaithersburg, MD, USA: National Institute of Standards and Technology, Aug. 2020.
2. G. Godhani and M. Dhamecha, “A Study on Movie Recommendation System Using Parallel MapReduce Technology,”, Vol.5, Issue 1, page no.375-378, IJEDR – 2017.
3. M. Dhamecha, A. Ganatra, and C. K. Bhensadadiya, “Comprehensive Study of Hierarchical Clustering Algorithm and Comparison with Different Clustering Algorithms,” CiiT Int. J., 2011.
4. P. Mell and T. Grance, The NIST Definition of Cloud Computing, NIST Special Publication 800-145. Gaithersburg, MD, USA: National Institute of Standards and Technology, Sep. 2011.
5. K. Parmar, N. Limbasiya, and M. Dhamecha, “Feature-based Composite Approach for Sarcasm Detection Using MapReduce,” in Proc. IEEE, 2018. DOI: 10.1109/ICCMC.2018.8488096
6. A. K. Jain and B. B. Gupta, “A survey of cyber-attacks and security challenges in cloud computing,” Journal of Network and Computer Applications, vol. 122, pp. 1–16, 2018.
7. W. Stallings and L. Brown, Computer Security: Principles and Practice, 4th ed. Boston, MA, USA: Pearson, 2018.
8. M. Dhamecha, “Improve K-Mean Clustering Algorithm in Large-Scale Data for Accuracy Improvement,” AISC, 2021. https://doi.org/10.1007/978-981-15-9516-5_5.
9. Gartner, Identity Is the New Security Perimeter. Stamford, CT, USA: Gartner Research, 2021.
10. M. Dhamecha, “An Efficient Comparison between Structured Analysis and Object-Oriented Analysis,” IJSRCSEIT, 2021. https://doi.org/10.32628/CSEIT217369.
11. B. B. Gupta, D. P. Agrawal, and S. Yamaguchi, “Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security”. Hershey, PA, USA: IGI Global, 2016.
12. M. Dhamecha, “Plant Recommendation System with the Use of Weather Forecasting,” CEUR Workshop Proc., 2021.
13. N. Dragoni, S. Dustdar, S. T. Larsen, and M. Mazzara, “Microservices: Yesterday, today, and tomorrow,” in Present and Ulterior Software Engineering, M. Mazzara and B. Meyer, Eds. Cham, Switzerland: Springer, 2017, pp. 195–216.
14. S. Rose, O. Borchert, S. Mitchell, and S. Connelly, Zero Trust Architecture, NIST Special Publication 800-207. Gaithersburg, MD, USA: National Institute of Standards and Technology, Aug. 2020.
15. Microsoft, Zero Trust Deployment Guide. Redmond, WA, USA: Microsoft, 2023.
16. Cloud Security Alliance, “Security Guidance for Critical Areas of Focus in Cloud Computing v4.0”. Seattle, WA, USA: Cloud Security Alliance, 2017.
17. A. K. Jain and B. B. Gupta, “A survey of cyber-attacks and security challenges in cloud computing,” Journal of Network and Computer Applications, vol. 122, pp. 1–16, 2018.
18. Gartner, “Hybrid and Multi-Cloud Security Best Practices”. Stamford, CT, USA: Gartner Research, 2022.
19. CERT Division, “Common Sense Guide to Mitigating Insider Threats”, 7th ed. Pittsburgh, PA, USA: Carnegie Mellon Univ., 2021.
20. Verizon 2026, “Data Breach Investigations Report”. New York, NY, USA: Verizon Enterprise, 2026.
21. IBM Security, “Security Information and Event Management and Threat Detection Best Practices”. Armonk, NY, USA: IBM Corp., 2024.
22. Amazon Web Services, “Infrastructure as Code Security Best Practices”. Seattle, WA, USA: AWS, 2024.
23. Mandiant, “M-Trends 2025: Special Report”. Reston, VA, USA: Mandiant, 2025.

24. IBM Security, “The Evolution of AI in Cybersecurity and Threat Detection”. Armonk, NY, USA: IBM Corp., 2024.
25. M. Dhamecha, “Optimize Ant Colony Algorithm with Relation of Efficiency and Performance for the Traveling Salesman Problem,” GRADIVA, 2021.
26. S. Rose, O. Borchert, S. Mitchell, and S. Connelly, Zero Trust Architecture, NIST Special Publication 800-207. Gaithersburg, MD, USA: National Institute of Standards and Technology, Aug. 2020.
27. Urvi Darji, Shruti Oza, Kruti P. Thakor “Design Of PFD With Charge Pump For DPLL In 0.18µm CMOS Technology”, NCAET (2012).
28. Gartner, “Cloud Security Posture Management and Multi-Cloud Governance”. Stamford, CT, USA: Gartner Research, 2023.
29. OWASP Foundation, “OWASP API Security Top 10 – 2023”. Wakefield, MA, USA: OWASP Foundation, 2023.
30. M. Dhamecha, “Fundamentals of ANN and Basic Algorithm of Neural Network in Data Analytics,” MOENIA, 2021.
31. IBM Security, “The Evolution of AI in Cybersecurity and Threat Detection”. Armonk, NY, USA: IBM Corp., 2024.
32. B. B. Gupta, D. P. Agrawal, and S. Yamaguchi, “Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security”. Hershey, PA, USA: IGI Global, 2016.
33. V. Vyas, M. Dhamecha and U. Dhamecha, “Cognitive Storage Techniques Using Popularity Heuristics in Big Data Frameworks” Communications on Applied Nonlinear Analysis, vol. 31, no. 8, pp. 1262–1276, 2024, doi: https://doi.org/10.52783/cana.v31.6392.
34. V. C. Hu, D. Ferraiolo, and D. Kuhn, “Guide to Attribute Based Access Control (ABAC) Definition and Considerations”, NIST Special Publication 800-162. Gaithersburg, MD, USA: National Institute of Standards and Technology, Jan. 2014.
35. M. Dhamecha, “Study of Search Engines with the Paradigm of Machine Learning,” SAMRIDDHI – J. Phys. Sci. Eng. Technol., 2022.
36. Gartner, “Zero Trust Network Access (ZTNA): Secure Access for Modern Enterprises”. Stamford, CT, USA: Gartner Research, 2024.
37. M. Dhamecha, “Literature Survey of Basic Methodologies in Cloud Computing,” SAMRIDDHI – J. Phys. Sci. Eng. Technol., 2022.
38. S. Rose, O. Borchert, S. Mitchell, and S. Connelly, Zero Trust Architecture, NIST Special Publication 800-207. Gaithersburg, MD, USA: National Institute of Standards and Technology, Aug. 2020.
39. Urvi Darji, Shruti Oza, Kruti P. Thakor “Low power and low jitter phase frequency detector for dpll using 0.18µm cmos technology”, ICIKR-ETS (2012).
40. International Organization for Standardization, ISO/IEC 27001:2022 Information Security Management Systems — Requirements. Geneva, Switzerland: ISO, 2022.
41. M. Dhamecha, “Fundamental Study of Chatbot with the Use of Artificial Intelligence,” SODHASAMHITA, 2022.
42. A. Adadi and M. Berrada, “Peeking inside the black-box: A survey on explainable artificial intelligence (XAI),” IEEE Access, vol. 6, pp. 52138–52160, 2018.
43. M. Dhamecha, “Literature Survey for Outlier Detection Methods in Data Analytics,” TANZ Res. J., vol. 9, no. 12, pp. 139–142, 2023, doi: 10.6084/doi.23.9.11.TANZ21837.
44. M. Dhamecha and U. Dhamecha, “Prediction of Air Quality Index Affected by Vehicle Emissions Using Machine Learning,” Int. J. Environ. Sci., vol. 11, no. 21, pp. 1566–1571, 2025, doi: 10.64252/r2d6a722.
45. G. Kim, J. Humble, P. Debois, and J. Willis, “The DevOps Handbook: How to Create World-Class Agility, Reliability, and Security in Technology Organizations”, 2nd ed. Portland, OR, USA: IT Revolution Press, 2021.
46. M. Dhamecha and U. Dhamecha, “Behavioral Detection of Ransomware and a Comprehensive Approach to Ransomware Prevention,” IEEE Commun. Standards Mag., vol. 11, no. 21, pp. 1–7, 2025, doi: 10.1109/MCOMSTD.2025.3616108.
47. V. Vyas, M. Dhamecha and U. Dhamecha, “Performance Evaluation of Hashgraph Algorithm in IoT: Execution Time and CPU Usage in DLT Systems” Advances in Nonlinear Variational Inequalities, vol. 27, no. 4, pp. 606–617, 2024, doi: https://doi.org/10.52783/anvi.v27.6397.
48. OWASP Foundation, “OWASP API Security Top 10 – 2023”. Wakefield, MA, USA: OWASP Foundation, 2023.