**Edelweiss Applied Science and Technology**
*ISSN: 2576-8484*
*Vol. 9, No. 2, 1726-1736*
*2025*
*Publisher: Learning Gate*
*DOI: 10.55214/25768484.v9i2.4888*


# Implementing zero-trust architecture and quantifying the impact on system reliability and data protection in big data cloud infrastructures

Arun Pandiyan Peruma[1*], Viralkumar Ahire[2]
[1]Dept. of Information Technology and Management Illinois Institute of Technology, United States; apandiyan@hawk.iit.edu (A.P.P.)
[2]Cloud and IT Infrastructure Expert United States of America, United States; viral.ahire@gmail.com (V.A.)

**Abstract:** The exponential growth of big data and the increasing complexity of cloud infrastructures have heightened the demand for robust security frameworks. This study presents the implementation process and analyzes the effect of zero-trust architecture (ZTA) on system reliability and data protection in big-data cloud environments. The methodology involves a comprehensive research approach, encompassing a review of existing research papers and the execution of a narrative review and content analysis to identify critical issues related to ZTA, system reliability, and data protection. The findings indicate that ZTA, with its robust access control mechanisms, can enhance data protection in a practical and tangible manner, thereby contributing to the enhancement of operational efficiency. This implies that organizations that embrace ZTA can fortify their data protection strategies and experience substantial real-world improvements in system reliability. A continuous monitoring system aids in the detection of anomalies and maintenance records, leading to reduced downtimes and improved system reliability. This study underscores the crucial role of strategic planning, resource management, and awareness training in the seamless integration of ZTA into organizational functionality for superior outcomes.

***Keywords:*** *Big data, Cloud infrastructure, Endpoint and network security, Identity and access management, Incident response, System reliability, Zero-trust architecture (ZTA).*

## 1. Introduction

### *1.1. Overview of Zero-trust Architecture*

Zero-trust Architecture (ZTA) is a paradigm-shifting security model, embodying the principle of 'never trust, always verify.' This revolutionary approach to infrastructure security necessitates continuous user verification within a Zero-trust Access framework, enhancing the ability to understand and address security needs [1]. ZTA's foundation lies in the recognition that threats can originate both internally and externally, underscoring the importance of verifying every user for appropriate access management and security. ZTA operates on a set of core principles, each designed to provide sustainable solutions for security and access control needs. The principles that bolster the functionality of ZTA include:

#### *1.1.1. Use Least Privilege Access*

The principle of least privilege dictates that users should only be granted the minimum level of access necessary to perform their job functions. This principle aligns with the concept of just-in-time access, which ensures that users have the permissions required to carry out their tasks at any time.


**History:** Received: 16 December 2024; Revised: 20 January 2025; Accepted: 24 January 2025; Published: 19 February 2025
* Correspondence: apandiyan@hawk.iit.edu

*1.1.2. Verify Explicitly*

This principle enables authentication and authorization at all points, examining user identity, service, device health, and workload [2].

*1.1.3. Assume Breach*

This principle illustrates that the system has to operate based on the belief that a breach can occur at any given moment. This implies that initiatives are taken to ensure critical security management on the network, beginning with segmented network access and the application of encryption for data both in transit and at rest.

Zero-trust architecture (ZTA) provides a robust and adaptive security framework that continuously verifies and monitors access to minimize risks and enhance the overall security posture of an organization. By integrating multiple security components and enforcing stringent access controls, ZTA effectively mitigates modern cyber threats and ensures the integrity, confidentiality, and availability of critical resources. The critical elements of the ZTA architecture include [3]:

*1.1.4. Identity and Access Management*

This provides centralized control for authorization and authentication activities. The component ensures that user privileges are constantly addressed to enhance functionality.

*1.1.5. Micro-Segmentation*

This component ensures that the network is segmented into isolated and independent segments, which helps limit the scope of damages in case of an attack.

*1.1.6. Endpoint Security*

This is a crucial security component that helps connect networks through security provisions at all levels [4]. The component demands regular monitoring and updates to enable sustainable results in detailing and managing the demanded appeal to handle consistent needs.

*1.1.7. Network Security*

ZTA relies on robust network security controls, such as firewalls, intrusion prevention systems, and network segmentation, to limit lateral movement within the network and detect and respond to potential threats.

*1.1.8. Security Analytics and Automation*

This component enables the use of data analytics and real-time monitoring to ensure that threats are identified as they occur [5]. The automation also assists with the management of response actions aimed at targeting and providing integral management of the needed security requirements.

*1.1.9. Data Security*

A core principle of ZTA is protecting data at rest, in transit, and in use. This involves implementing encryption, data loss prevention (DLP) solutions, and strict access controls based on data sensitivity and classification.

*1.1.10. Continuous Monitoring and Incident Response*

This component works within the framework of ensuring that every action is monitored and that functionalities on the ZTA system are automated [6]. The incident response provides notification on events and an automated response to each activity, depicting an integral capacity to handle and achieve suitable handling of the desired components.

ZTA offers organizations significant benefits, including improved security, operational efficiency, and compliance with regulations. However, implementing ZTA presents several challenges, including

*Edelweiss Applied Science and Technology*
*ISSN: 2576-8484*
*Vol. 9, No. 2: 1726-1736, 2025*
*DOI: 10.55214/25768484.v9i2.4888*

ensuring the scalability and performance of security mechanisms without hindering data processing [7]. The complex and dynamic nature of data flows in big data environments requires meticulous mapping and the enforcement of consistent security policies [8]. Implementing ZTA within an organization requires investment in technology and training to provide the necessary resources.

The primary objective of this study is to map the best practices or framework for implementing ZTA in big-data cloud environments. This study aims to address the fundamental challenges and intricacies associated with deploying a zero-trust security paradigm in cloud environments, mainly focusing on the implications for system reliability and data protection. It endeavors to provide a detailed analysis of the theoretical underpinnings of zero-trust architecture, elucidating its core principles and the critical role it plays in safeguarding resources within a cloud infrastructure. Additionally, the study will address innovations and emerging trends in data protection, offering valuable insights into data analytics and protection on cloud platforms [9]. Overall, this study will contribute to the current body of research in this field, emphasizing the best approaches for implementing ZTA and enhancing our understanding of creating better security approaches.

## 2. Literature Review

### *2.1. Zero-trust Architecture*

Bertino [10] explains that Zero-trust Architecture (ZTA) is a crucial security mechanism in today's world. The author defines this architecture as a framework that enables continuous verification of every user without relying on trust for any single user within the network. Bertino [10] emphasizes the need for a deep understanding of networks to address individual development and achieve optimal results. Consequently, Bertino [10] points out that there are advancements in ZTA that ensure a high level of protection and security for networks by consistently verifying and monitoring user privileges. With the implementation of the zero-trust approach, organizations are paying more attention to managing their systems using a combination of techniques, each aimed at making valuable adjustments to the security architecture [10].

Syed, et al. [11] suggest that the implementation of a zero-trust architecture requires organizations to make significant changes to their security needs and organizational norms. They emphasize the importance of developing a culture that aligns with zero-trust architecture, which entails organizations changing their approach to prioritize the security of every aspect of the network system. According to Syed, et al. [11] zero trust requires the development of policies and practices that ensure networks can adapt effectively, enabling organizations to provide top-level security. By utilizing core components as described by Syed, et al. [11] zero-trust architecture enhances operations. It facilitates the attainment of the necessary level and form of security across various units and interactions. Implementing systems such as context-aware user authentication and zero trust can lead to significant improvements in an organization's understanding of its environment and security [11]. The authors concur that zero trust plays a crucial role in enhancing security and is instrumental in shaping the organizational environment.

Teerakanok, et al. [12] detail five critical components of the ZTA architecture. These components provide valuable insights into the operational levels and progression of ZTA to meet the evolving needs of all entities. The critical parts of the ZTA architecture, as introduced by Teerakanok, et al. [12] include the subject, policy enforcement point (PEP), resource, policy decision point (PDP), and supplements. They detail the necessary advancements within the framework to support and address the modeling of functionalities. The subject represents the user requesting access to the system [12]. The policy decision point serves as the primary decision maker for granting access to the system, leading to a comprehensive understanding and management of the entire engagement. Meanwhile, the policy enforcement point receives requests on behalf of the PDP, providing information on the engagement and managing communication as required. Teerakanok, et al. [12] state that the PDP consists of two main components, namely the policy engine and policy administrator, which help in executing functions

*Edelweiss Applied Science and Technology*
*ISSN: 2576-8484*
*Vol. 9, No. 2: 1726-1736, 2025*
*DOI: 10.55214/25768484.v9i2.4888*

and enhancing the management of engagements for a reliable outcome. Information supplements for the system will enhance the engagement process, leading to a complete cycle in the zero-trust framework.

Adahman, et al. [13] explains that using Zero-trust Architecture (ZTA) can establish better security practices through continuous monitoring. The evolving nature of security ensures that essential measures are utilized to track progress and make necessary adjustments [13]. Managing the security architecture at this level involves ZTA's involvement in monitoring and enabling early detection and management of threats. Adahman, et al. [13] highlights several security adjustments provided by ZTA, resulting in significant progress in establishing effective defense against threats and making critical decisions to achieve better outcomes. Therefore, Adahman, et al. [13] emphasizes the importance of understanding and implementing ZTA security models to create relevant systems and strategies, facilitating improved monitoring, addressing individual organization needs, and achieving desired security outcomes.

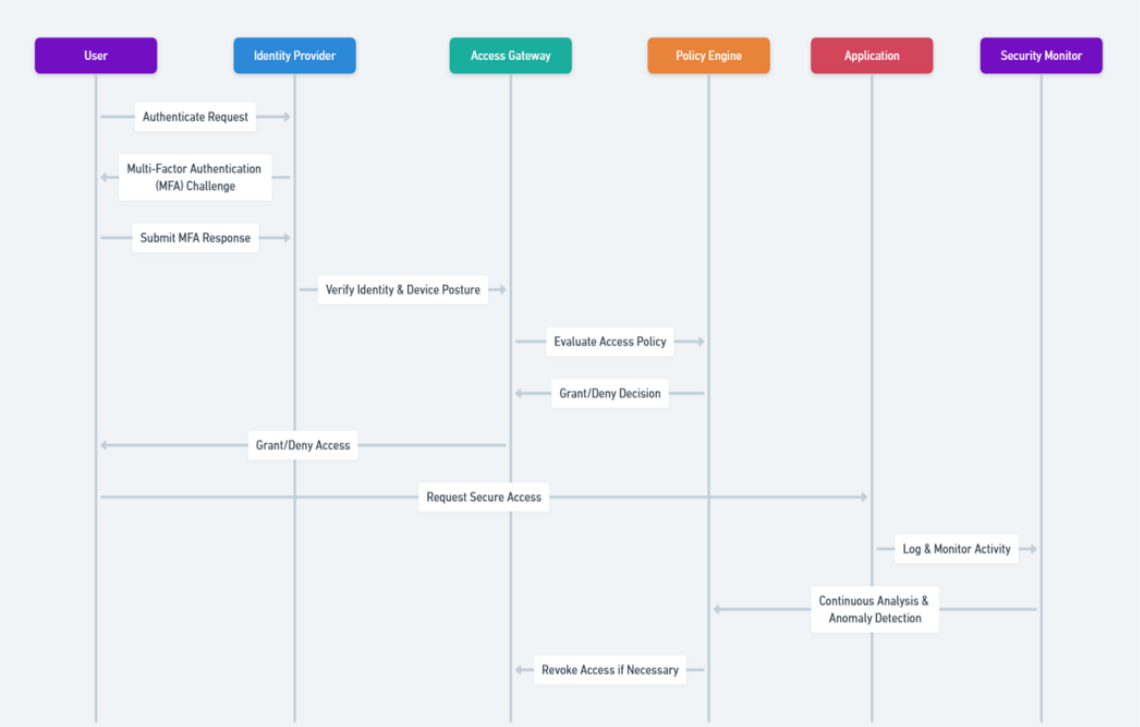


**Figure 1.**
Components of zero-trust architecture.

### *2.2. Big Data Cloud Infrastructure*

Demchenko, et al. [14] suggest that the use of cloud-based big data infrastructure allows for the seamless analysis of various datasets by combining cloud computing and big data. This enables the progressive modeling and management of datasets to provide better value and cater to multiple needs. The creation of big data infrastructure involves different components to ensure the effective management of data [15]. The data ingestion and data storage layers handle and manage data at various levels. The data processing and data analytics layer assists in managing data points. The data management and governance layer focuses on data quality and compliance with regulations. The workflow management layer automates procedures to achieve desired outcomes. The monitoring and logging layer analyzes the system and its functionalities. The user interface and visualization layer help end-users understand and work with the data effectively. Loreti and Ciampolini [16] also mention that a well-managed user interface provides visualizations and tabulations that encourage effective data

*Edelweiss Applied Science and Technology*
*ISSN: 2576-8484*
*Vol. 9, No. 2: 1726-1736, 2025*
*DOI: 10.55214/25768484.v9i2.4888*

management. Overall, these components work together to seamlessly integrate and function between cloud infrastructure and big data analytics [15].

Demchenko, et al. [17] identified key components necessary for a cloud-based big data infrastructure. They emphasized that the development of such an infrastructure requires components that can address various functions throughout the data lifecycle. Technologies addressing security, compliance, and other functionalities within these platforms enhance the ability to achieve significant outcomes in managing tasks across different channels [16]. The use of big data infrastructure enables the utilization of information and the extraction of value from cloud-based platforms, aiming to ensure consistent development and delivery of platforms to meet their value needs. Demchenko, et al. [17] highlighted the creation of automated service provision on cloud platforms, enabling further engagement and advancement in meeting critical demands for managing cloud data requirements. Dai, et al. [18] noted that the development of appropriate infrastructure and resource allocation on cloud platforms offers big data infrastructure the opportunity to achieve higher performance. The proper allocation framework and mechanism provide a critical understanding and modeling of big data to address individual concerns and needs. Dai, et al. [18] emphasized that resource allocation on a cloud platform is crucial when considering the speed and efficiency of systems aimed at meeting the core requirements of the system [17].

Sandhu [19] points out that in the current development of cloud-based big data infrastructure, a significant challenge of interoperability and data integration affects the possibility of most organizations achieving optimal outcomes. Managing tools and devices in both big data and cloud computing involves creating an incremental level of support for every consideration in appealing to organizational functions. The challenge is that some systems lack integration capacity, leading to a high chance of slow functionality and addressing various requirements Dai, et al. [18]. Sandhu [19]further indicates that specific tools would lead to latency and throughput challenges, demanding an increased level of participation in achieving the correct outcome when handling the infrastructure. Moreover, Ageed, et al. [20] state that these challenges have to be addressed well, with the indication that integration and interoperability challenges stand out as negative to functionality and capacity to achieve valuable outcomes within cloud platforms. Ageed, et al. [20] provide a remarkable insight into the management of the cloud-data infrastructure, appealing to the achievement of high throughput and low latency by enabling integration of the platforms for a critical address of major channels of identifying their needs and working within the best determination to achieve valuable outcomes [19].

### *2.3. System Reliability and Data Protection*

Yang, et al. [21] appreciated the development of cloud platforms for big data. However, the author indicated that the migration of data to cloud systems increases the risk for various organizations, leading to a demand to address and manage every underlying issue within these platforms [22]. The significant challenges and problems within cloud platforms include the need to address data leakage, privacy, and sensitive information disclosure. Therefore, Yang, et al. [21] provided the most remarkable advancement in targeting and dealing with data protection using critical encryption mechanisms to address significant challenges within cloud platforms. Additionally, developing systems with appropriate encryption and information protection presents an opportunity to refine the essential adjustments needed to meet the challenges of obtaining better results when utilizing data platforms.

Lo'ai and Saldamli [23] explain that additional measures are being taken to enhance data and privacy protection on cloud platforms. These measures aim to improve and achieve significant progress in adjusting to the requirements. They help to define the appropriate scope and level for developing sustainable models for different categories, ensuring better data handling practices. The use of peer-to-peer cloud computing requires an approach to manage data privacy, storage, and handling mechanisms [21]. This approach aims to protect data and enhance performance for essential data requirements, ensuring sustainable outcomes. Adjustments to the P2P cloud service platform are intended to provide

*Edelweiss Applied Science and Technology*
*ISSN: 2576-8484*
*Vol. 9, No. 2: 1726-1736, 2025*
*DOI: 10.55214/25768484.v9i2.4888*

sustainable improvements for every provision, aiming for better management and achieving the necessary value approach.

## 3. Methodology

### *3.1. Research Design*

This study leveraged a comprehensive review of past literature, which is a significant research method, to facilitate the discovery of crucial information on ZTA implementation. The review served as a robust platform for examining multiple studies, highlighting key themes and outcomes, and addressing the management of studies based on their capacity to tackle pertinent issues.

### *3.2. Data Collection Methods*

This study collected data by analyzing previously conducted studies. The data analysis ensured that information was collected from these previous research papers, accounting for every finding and looking into their key recommendations for managing the required variables of the study.

### *3.3. Data Analysis Techniques*

Content analysis was applied within the study, aiding the progressive understanding and handling of the research themes to achieve a desirable outcome. The analytical approach also provides a mechanism for identifying core issues related to the subject matter, offering an even deeper analysis of the research [21].

### *3.4. Ethical Considerations*

This study considers the ethical elements of reflexivity and bias management to assist with the modeling of critical issues in addressing previously conducted studies. Ethical considerations enabled the identification of biases and ensured that they did not apply to the current research.

### *3.5. Quality Assurance*

Quality assurance was performed during the study to help manage information effectively and achieve significant impact and results. Initially, the study assessed its quality, addressing all evolving requirements and improving the representation and handling of information.

## 4. Results

### *4.1. Research Study Selection*

This study selected fifteen previously conducted studies on ZTA architecture and implementation. It used a strict inclusion criterion to help designate key research papers that appeal to the area of research as appropriately needed. This approach included vital considerations, as dictated in Table 1.

**Table 1.**
Research study selection considerations.

| Condition | Evaluation |
|---|---|
| Publication date | Studies conducted within the last decade |
| Peer-review | Studies from journals, conference papers, and academic publications |
| Relevance | Discuss ZTA architecture in relation to big data and cloud environments. |
| Context | Discuss the implementation of ZTA architecture within the provided big-data cloud environment. |
| Empirical evidence | Provide evidence of their reports from case studies, experiments, or real-world implementations of the studies. |

### *4.2. Perceptions of Zero-trust Architecture*

The studies offered various insights into the components of ZTA within their respective organizations. The participants' perceptions indicated a clear understanding of the fundamental needs of organizations and the significance of ZTA in addressing these needs at every level. The use of ZTA

*Edelweiss Applied Science and Technology*
*ISSN: 2576-8484*
*Vol. 9, No. 2: 1726-1736, 2025*
*DOI: 10.55214/25768484.v9i2.4888*

resulted in different interpretations, which present a word cloud of keywords used by participants to convey their understanding and description of ZTA architecture. The participants demonstrated a strong awareness of the benefits and applications of ZTA architecture, providing accurate descriptions of the approach and emphasizing its relevance to their organization's big data platforms.

*4.3. Challenges in Implementing ZTA*

The studies have identified various challenges in implementing ZTA. These challenges highlight the key issues and limitations of using the system while attempting to enforce different regulations. Each challenge defines the scope and level of addressing ZTA, providing the capacity to address impending issues within the modeling and handling of infrastructure inclusion within the organization. Table 2 shows the challenges along with their frequency of occurrence, discussing each action and detailing the process by which every challenge affects the implementation of ZTA. These challenges include technical complexities, identity management, access control, cultural resistance from employees, continuous monitoring, interoperability, and the need for more awareness among employees. Table 2 indicates these challenges and their occurrence within the institution to emphasize engagement in handling specific appeals.

**Table 2.**
ZTA implementation challenges.

| Challenge | Description | Frequency |
|---|---|---|
| Cultural resistance | The difficulty of employees to adopt practices and competencies related to ZTA | Medium |
| Access control challenges | Challenges in ensuring the best definition of granular access control demands | High |
| Resource allocation | Limited financial capacity and employee skills to address ZTA needs | High |
| Interoperability | Experiencing a challenge in enabling seamless integration of individual tools and platforms. | Low |
| Awareness | Demand to ensure that customers have constant awareness and training sessions on the elements of ZTA | Medium |
| Identity management | Challenges in configuring and constantly managing the identity platforms and approaches by the institution. | Medium |
| Continuous monitoring | Configuring a system that enables a continued scope and level of addressing the challenges | Medium |
| Technical complexities | Difficulty in ensuring that the cloud-based systems can configure and work with available platforms in the organization. | High |

*4.4. Impact on System Reliability*

The adoption of Zero-trust Architecture (ZTA) has had a significant impact on addressing critical reliability issues. ZTA has dramatically improved system reliability, resulting in better downtime management and more efficient system handling. Essentially, the use of ZTA ensures that every request is thoroughly evaluated to determine the appropriate access, leading to more reliable system performance. Research has shown that organizations experience reduced downtime when using ZTA, resulting in sustainable value and benefits. The implementation of robust security measures has led to a decrease in unauthorized access attempts, contributing to improved system performance through efficient access control and resource management.

*4.5. Enhancement in Data Protection*

The implementation of Zero-trust Architecture (ZTA) practices and requirements has improved the system's capacity and scope for core development. ZTA aims to enhance and work within the provisional development of every necessary segment to ensure appropriate implementation within the framework. By focusing on cultural development and meeting ZTA requirements, data protection measures have significantly improved, ensuring the system's safety and leading to better performance. ZTA approaches have resulted in better data protection, fewer network breaches, and improved

*Edelweiss Applied Science and Technology*
*ISSN: 2576-8484*
*Vol. 9, No. 2: 1726-1736, 2025*
*DOI: 10.55214/25768484.v9i2.4888*

monitoring and response. This enhanced protection helps systems defend against attacks and improves their functionality.

*4.6. Implementation Techniques*

Studies have denoted the fundamental implementation techniques that have been applied over the years to assist in characterizing and ensuring that they can consistently address ZTA. These implementation techniques register an instrumental scope and level of depicting the sufficient management of the required needs in administering valuable additions to the ZTA framework and demands. Developing these implementation approaches ensures the critical development of the ZTA architecture. Core implementation requirements included the following measures:

*4.6.1. Identity Verification*

Studies have indicated that identity verification is conducted using multi-factor authentication (MFA) and role-based access control approaches (RBAC). These mechanisms enable strict management of identity verification within the system, granting an increasingly beneficial way to ensure their advancement at all times [24].

*4.6.2. Micro-Segmentation*

Segmentation of the networks was conducted in different ways, enhancing an appeal to structuring and ensuring instrumental development to target and achieve the suitable capacity to address the needs of an organization. Network segmentation ensures that the network can be divided into smaller segments to guard against potential attacks [25]. Additionally, application segmentation was carried out to enhance security across different applications, thereby improving security development and management.

*4.6.3. Continuous Monitoring*

The implementation of ZTA was significantly simplified with the development of real-time monitoring tools. These tools provided valuable insight into the network system for participants. The use of continuous monitoring, alerting, and response approaches has contributed significantly to the development and management of core advances in targeting and ensuring sustainable responses to the system's core needs. The demands of real-time monitoring have facilitated the development of a more secure system that is resistant to attacks, unlike traditional systems. Continuous monitoring also involved examining behavioral analytics to establish critical steps for identifying threats and anomalies within the network system. This framework has led to significant progress in detecting suspicious activities and their rates of occurrence within the network, allowing for timely alerts and the implementation of contingency measures to protect the system.

## 5. Discussion

The implementation of Zero-trust Architecture (ZTA) in big data cloud environments has significantly transformed data protection and system reliability. This approach has helped in providing a reliable framework for addressing organizational functions, facilitating their relevant development to achieve impactful outcomes consistently. The use of ZTA architecture primarily results in an improved understanding and awareness of ZTA, highlighting significant changes within organizations as they structure their knowledge and insight to manage and address their cloud operations and big data analytics [23]. The research indicates an enhanced perception of individuals when they utilize ZTA architecture, aiding their development and adaptation to help create exceptional results consistently.

Despite the growing adoption of ZTA architecture, various factors need to be addressed to effectively meet the evolving requirements for sustainable values. Technical complexity is a significant challenge, as organizations need to integrate systems to achieve optimal functionality seamlessly. Achieving seamless integration requires specific skills and tools, which may be cost-prohibitive [26].

*Edelweiss Applied Science and Technology*
*ISSN: 2576-8484*
*Vol. 9, No. 2: 1726-1736, 2025*
*DOI: 10.55214/25768484.v9i2.4888*

Cultural resistance to adopting new technological features within the organization is another crucial challenge. This resistance significantly impacts the ability to effectively address user needs at every stage of use and implementation. Organizations also need to manage resource allocation to ensure successful implementation and substantial progress in meeting the system's core requirements.

Implementing ZTA enhances system reliability by reducing downtime through continuous monitoring and real-time threat detection, which enable early identification and swift automated response to security incidents. The reduction in downtime ensures that organizations have better functionalities, achieving a remarkable scope for addressing their demands at all times [27]. Organizations that implement the ZTA architecture also ensure that appropriate steps are used to achieve maximum development and deploy and administer big data cloud infrastructures across every critical point of security engagements. Within these classifications, data protection is advanced, marking progressive handling and management of the ZTA architecture to achieve a sustainable appeal in handling organizational demands for efficient data management [28].

ZTA can be implemented by enabling access control and authorization techniques. The deployment of multi-factor authentication and role-based access control will allow organizations to administer their access regulations, manage the levels of access, and ensure that ZTA principles are upheld whenever confronting core identities and demands of achieving the required value of the research to achieve desired results [29]. Moreover, micro-segmentation and continuous monitoring will help ensure that ZTA requirements are met, directing an increased channel of delivering and achieving organizational security approaches. Furthermore, this approach will mark a depiction of the value of attaining organizational advancement toward managing security and alerts on any impending issues.

To enhance the implementation of the ZTA architecture, core steps must be procured to assist in channeling valuable outcomes and demands at all times. The first instance is developing a training and awareness program aimed at focusing on pertinent challenges and working towards maintaining the appropriate structure and elements of advancing system functionality [30]. The use of this approach ensures that employees in an organization are well-trained and informed about the core adjustments needed in the organization's everyday activities. Practicing strategic resource deployment will assist in addressing ZTA challenges and ensuring that organizations have the right resources to ensure measured adjustment within every distinctive angle of delivering value to the organization [31]. Employing relevant change management strategies is also crucial for detailing and appreciating the management of employee perceptions toward addressing core development in the context of the ZTA architecture. Therefore, these approaches are vital in depicting an increasingly beneficial path to handling ZTA implementation.

## 6. Conclusion

The implementation of Zero-Trust Architecture (ZTA) in big data cloud environments significantly enhances system reliability and data protection. ZTA introduces robust security measures such as strict access control, micro-segmentation, and continuous monitoring, which collectively reduce downtime and effectively address data breaches. One of the key conclusions drawn from this study is that the application of ZTA brings about a fundamental shift in the traditional security paradigm by enforcing strict access controls, continuous verification, and the principle of least privilege. The adoption of ZTA leads to a more secure, resilient infrastructure, as each access request is thoroughly evaluated, resulting in better system performance and operational efficiency. The study emphasizes the critical role of strategic planning, resource management, and awareness training in the seamless integration of ZTA into organizational functionality for superior outcomes. However, implementing ZTA can be challenging due to technical complexities and skillset requirements. The insights derived from this study serve as a valuable guide for organizations seeking to fortify their big data cloud environments against evolving security threats and elevate the reliability of their systems while upholding stringent data protection standards. As the landscape of cloud computing continues to grow, the integration of

*Edelweiss Applied Science and Technology*
*ISSN: 2576-8484*
*Vol. 9, No. 2: 1726-1736, 2025*
*DOI: 10.55214/25768484.v9i2.4888*

ZTA principles stands as a pivotal strategy in fortifying the security and resilience of modern digital infrastructures.

## Transparency:

The authors confirm that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.

## Copyright:



## References

[1] S. Ahmadi, "Zero trust architecture in cloud networks: Application, challenges and future opportunities," *Journal of Engineering Research and Reports*, vol. 26, no. 2, pp. 215-228, 2024. https://doi.org/10.9734/jerr/2024/v26i21083

[2] S. Mehraj and M. T. Banday, "Establishing a zero trust strategy in the cloud computing environment," presented at the International Conference on Computer Communication and Informatics, Jun 2020, https://ieeexplore.ieee.org/document/9104214, 2020.

[3] P. Srinivasan, "Zero-trust network architecture," Retrieved: http://hdl.handle.net/1828/15201, 2023.

[4] 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, 2022. https://doi.org/10.3390/su141811213

[5] L. Ferretti, F. Magnanini, M. Andreolini, and M. Colajanni, "Survivable zero trust for cloud computing environments," *Computers & Security*, vol. 110, p. 102419, 2021. https://dl.acm.org/doi/abs/10.1016/j.cose.2021.102419

[6] O. C. Edo, D. Ang, P. Billakota, and J. C. Ho, "A zero trust architecture for health information systems," health and technology," Retrieved: https://link.springer.com/article/10.1007/s12553-023-00809-4, 2023.

[7] E. S. Hosney, I. T. A. Halim, and A. H. Yousef, "An artificial intelligence approach for deploying zero-trust architecture (ZTA)," presented at the 2022 5th International Conference on Computing and Informatics (ICCI), pp. 343-350, March 2022, https://ieeexplore.ieee.org/abstract/document/9756117, 2022.

[8] K. N. Singh, R. K. Behera, and J. K. Mantri, "Big data ecosystem: Review on architectural evolution," *Emerging Technologies in Data Mining and Information Security: Proceedings of IEMIS*, vol. 2, pp. 335-345, 2019. https://doi.org/10.1007/978-981-13-1498-8_30

[9] Y. He, D. Huang, L. Chen, Y. Ni, and X. Ma, "A survey on zero-trust architecture: Challenges and future trends," wireless communications and mobile computing," Retrieved: https://dl.acm.org/doi/10.1155/2022/6476274, 2022.

[10] E. Bertino, "Zero trust architecture: Does it help?," *IEEE Security & Privacy*, vol. 19, no. 05, pp. 95-96, 2021. https://doi.org/10.1109/msec.2021.3091195

[11] N. F. Syed, S. W. Shah, A. Shaghaghi, A. Anwar, Z. Baig, and R. Doss, "Zero-trust architecture (ZTA): A comprehensive survey," IEEE access," Retrieved: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9773102, 2022.

[12] S. Teerakanok, T. Uehara, and A. Inomata, "Migrating to zero trust architecture: Reviews and challenges," *Security and Communication Networks*, vol. 2021, no. 1, p. 9947347, 2021. https://dl.acm.org/doi/abs/10.1155/2021/9947347

[13] Z. Adahman, A. W. Malik, and Z. Anwar, "An analysis of zero-trust architecture and its cost-effectiveness for organizational security," *Computers & Security*, vol. 122, p. 102911, 2022. https://doi.org/10.1016/j.cose.2022.102911

[14] Y. Demchenko, F. Turkmen, C. De Laat, C. Blanchet, and C. Loomis, "Cloud-based big data infrastructure: Architectural components and automated provisioning," presented at the International Conference on High-Performance Computing & Simulation (HPCS), pp. 628-636, July 2016, https://pure.rug.nl/ws/files/76818625/07568394.pdf, 2016.

[15] Arun Pandiyan Perumal and Pradeep Chintale, "Improving operational efficiency and productivity through the fusion of DevOps and SRE practices in multi-cloud operations," *International Journal of Cloud Computing and Database Management*, 2022. https://doi.org/10.33545/27075907.2022.v3.i2a.51

[16] D. Loreti and A. Ciampolini, "A hybrid cloud infrastructure for big data applications," presented at the IEEE 17th International Conference on High-Performance Computing and Communications, Aug 2015, https://ieeexplore.ieee.org/abstract/document/7336418, 2015.

[17] Y. Demchenko, F. Turkmen, C. de Laat, C. H. Hsu, C. Blanchet, and C. Loomis, "Cloud computing infrastructure for data-intensive applications big data analytics for sensor-network collected intelligence," Academic Press. https://www.sciencedirect.com/science/article/abs/pii/B9780128093931000027?via%3Dihub, 2017, pp. 21-62.

[18] W. Dai, L. Qiu, A. Wu, and M. Qiu, "Cloud infrastructure resource allocation for big data applications," *IEEE Transactions on Big Data*, vol. 4, no. 3, pp. 313-324, 2016. https://doi.org/10.1109/tbdata.2016.2597149

[19] A. K. Sandhu, "Big data with cloud computing: Discussions and challenges," *Big Data Mining and Analytics*, vol. 5, no. 1, pp. 32-40, 2021. https://doi.org/10.26599/bdma.2021.9020016

[20] Z. S. Ageed *et al.*, "Comprehensive survey of big data mining approaches in cloud systems," *Qubahan Academic Journal*, vol. 1, no. 2, pp. 29-38, 2021. https://doi.org/10.48161/qaj.v1n2a46

[21] P. Yang, N. Xiong, and J. Ren, "Data security and privacy protection for cloud storage: A survey," *LEEE Access*, vol. 8, pp. 131723-131740, 2020. https://doi.org/10.1109/access.2020.3009876

[22] S. Rodigari, D. O'Shea, P. McCarthy, M. McCarry, and S. McSweeney, "Performance analysis of zero-trust multi-cloud," presented at the IEEE International Conference on Cloud Computing (CLOUD), 2021, https://ieeexplore.ieee.org/document/9582229, 2021.

[23] A. T. Lo'ai and G. Saldamli, "Reconsidering big data security and privacy in cloud and mobile cloud systems," *Journal of King Saud University-Computer and Information Sciences*, vol. 33, no. 7, pp. 810-819, 2021. https://doi.org/10.1016/j.jksuci.2019.05.007

[24] I. Kovacevic, M. Stojkov, and M. Simic, "Authentication and Identity management based on zero-trust security model in micro-cloud environment," presented at the Conference on Information Technology and its Applications, Springer, Cham, Feb 2024, https://link.springer.com/chapter/10.1007/978-3-031-50755-7_45, 2024.

[25] H. Sedjelmaci and N. Ansari, "Zero trust architecture empowered attack detection framework to secure 6g edge computing," *IEEE Network*, vol. 38, no. 1, pp. 196-202, 2023. https://doi.org/10.1109/mnet.131.2200513

[26] J. N. Lester, Y. Cho, and C. R. Lochmiller, "Learning to do qualitative data analysis: A starting point," *Human Resource Development Review*, vol. 19, no. 1, pp. 94-106, 2020. https://doi.org/10.1177/1534484320903890

[27] S. Gaurav, X. Zhao, S. Narayana, and B. Rajkumar, "Integration of cloud, internet of things, and big data analytics," *Software Practice Experience*, vol. 49, no. 4, pp. 561-564, 2019. https://onlinelibrary.wiley.com/doi/10.1002/spe.2664

[28] P. Phiayura and S. Teerakanok, "A comprehensive framework for migrating to zero trust architecture," *LEEE Access*, vol. 11, pp. 19487-19511, 2023. https://doi.org/10.1109/access.2023.3248622

[29] V. N. S. S. Chimakurthi, "The challenge of achieving zero trust remote access in multi-cloud environment," *ABC Journal of Advanced Research*, vol. 9, no. 2, pp. 89-102, 2020. https://doi.org/10.18034/abcjar.v9i2.608

[30] K. Ramezanpour and J. Jagannath, "Intelligent zero trust architecture for 5G/6G networks: Principles, challenges, and the role of machine learning in the context of O-RAN," *Computer Networks*, vol. 217, p. 109358, 2022. https://dl.acm.org/doi/10.1016/j.comnet.2022.109358

[31] P. Parameswarappa, "Artificial intelligence based zero trust network," *IRJEAS*, vol. 10, no. 3, pp. 42–48, 2022. https://doi.org/10.55083/irjeas.2022.v10i03013