International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 09 September 2024
Page No: 2377 - 2384
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2024.0326

Zero Trust in the Cloud: A Comprehensive Review of Data Breach and Network Attack Prevention

Shagufta Shakeel[1], Sushil Kumar Saroj[2], Nida Shakeel[3]

[1,2]Department of Computer Science and Engineering, MMMUT, Gorakhpur, UP, 273001, India

[3]Department of Information Technology and Computer Application, MMMUT, Gorakhpur. UP, 273001, India

Emails: *2023023107@mmmut.ac.in[1], sushil.mnnit10@gmail.com[2], nidashakeel251@gmail.com[3]*

Abstract

Over the past three decades, the world of computation has evolved from centralized to distributed systems, returning to virtual centralization in Cloud Computing. The location of data and processes significantly impacts computation, with cloud computing allowing vendors to provide services and data maintenance, leaving the client unaware of the processes running or data storage. This raises concerns about data security in cloud computing. The increasing frequency of cross-border access has made traditional perimeter-based network security models insufficient. The rise of new threats and attacks in the digital world necessitates reliable and secure methods for information processing, data storage, and network transport. Zero Trust (ZT) is a developing network safety model that focuses on clients, resources, and assets, using zero-trust concepts to design modern frameworks and work processes. Since zero-trust architecture is still a relatively young field of study, a lot of papers have been published on it in the previous few years. This paper lists and evaluates a few relevant research publications about blockchain technology and the Zero Trust Architecture. The emphasis is on documents that use the zero-trust security mechanism and blockchain-based zero-trust systems. This research aims to contribute to the ongoing discussion on effective ways to protect advanced frameworks in the interconnected world, helping professionals and network safety experts. The paper provides an in-depth analysis of the zero-trust model, its concept, and applications, and proposes suggestions for organizations embracing this methodology. By examining recent research, the advantages, disadvantages, and potential uses of zero-trust security are determined by examining the significant parts of the zero-trust structure and their coordination across various domains.

Keywords: *Blockchain; Cloud Computing; Cloud Security; Trust Models; Zero Trust Architecture.*

1. Introduction

In the modern context of digital transformation, cloud computing has become an essential element for enhancing organizational efficiency and stimulating innovation. This shift has allowed for remarkable scalability, agility, and cost-effectiveness, empowering organizations to optimize their operations, hasten their time-to-market, and improve customer interactions. (F. Tang, C. Ma and K. Cheng et al., 2023;). The name cloud computing was inspired by the cloud symbol often used to represent the Internet in flow charts and diagrams. A distinct migration to the clouds has been taking place over recent years with end users, ‘‘bit by bit’’ maintaining a growing number of personal data, including bookmarks, photographs, music files, and much more, on remote servers accessible via a network. Cloud computing is empowered by virtualization technology, which dates back to 1967, but it was only available on mainframe systems for decades. [3-4] numerous computing concepts, such as distributed and grid computing, are expanded upon by cloud computing. Both the industrial and academic domains employ cloud computing these days. By making virtual resources available online, cloud computing helps its users. New methods are emerging as the field of cloud computing expands. The growing cloud computing environment presents cloud developers with more security issues. Because users save their data on the cloud, insufficient security may cause users to lose faith in the cloud. To overcome the difficulty of establishing trust based on a network location, Kindervag [17] proposed the

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 09 September 2024
Page No: 2377 - 2384
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2024.0326

concept of Zero Trust (ZT) in 2010. ZT is based on three main ideas: 1) Security devices no longer have an interface marked as trustworthy or untrusted. 2) There is no longer a network that is trustworthy or untrusted. 3) Users are no longer classified as trustworthy or untrustworthy. Building on the idea of ZT, Google began work on the BeyondCorp project in 2011. NIST defined ZT in 2020. Zero Trust (ZT) is a security approach that focuses on data and service protection but can be extended to encompass all enterprise assets and subjects. It means that people should not blindly trust anyone or anything in the realm of computers and data. ZT is not only about ensuring that everything is secure within a network but also considering that there may be danger everywhere. It was developed to prevent competent hackers from sneaking into networks using existing security measures. ZT security involves constantly verifying who or what is trying to access data, whether it's human logging into a system or software connecting to the internet. It aims to defend our digital environment from cyberattacks by being extremely cautious and granting access to only those who can credibly demonstrate their worth. ZT is a key idea in modern cloud security because it represents a significant shift in how we protect our digital assets. Instead of automatically trusting anyone or anything, we double-check and verify everything. This tactic helps prevent cyberattacks by making it more difficult for hackers to harm even after successfully breaking past one layer of defense.

Figure 1 Policies Offered by Zero Trust Architecture

Figure 1 illustrates the policies offered by Zero Trust Architecture. To provide high-level security for preventing data breaches, cyber threats, and network attacks, zero trust architecture enforces policies related to fingerprint verification, multifactor authentication, user devices, network infrastructure, web and emails, data services, network applications, and network devices. ZT is a crucial part of maintaining the safety of our online environment in a world where cyber risks are constantly evolving. It's like having a strong castle around our virtual kingdom. The article describes how the paradigm for cloud security has evolved, from one that was primarily trust-based to one that is more robustly trust-secure. It exposes the flaws in traditional approaches and offers the concept of many security layers that work like locked doors with keycard access. A comprehensive overview of zero-trust security and useful guidance for enterprises navigating the constantly shifting landscape of modern cyber threats are provided by the paper, along with case studies and insights into implementation challenges.

1.1. Motivation

The necessity of exploring and comprehending the applications, and possibilities offered by the Zero Trust paradigm is the driving force for this study. Adaptable and resilient security solutions are crucial as more and more enterprises embrace digital transformation and new technologies. Zero Trust claims to improve network security and lessen a variety of cyber threats by switching from a trust-based strategy to continuous verification and stringent access restrictions. To protect companies from modern cyber risks, we want to analyze Zero Trust's cutting-edge ideas, useful applications, and applicability through this research. We want to provide insightful analyses to network administrators, IT specialists, and cybersecurity experts who are trying to strengthen their defenses by discovering their applications across sectors and evaluating the implementation's obstacles.

1.2. Paper Organization

Here is a summary of the reminder for this paper assignment. The research that has already been done on network attacks cloud security, and data breaches is reviewed in Section 2. We illustrate the zero-trust

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 09 September 2024
Page No: 2377 - 2384
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2024.0326

architecture's guiding concept and essential element in Section 3. In Section 5, we provide a final overview of our plan and talk about the course of our upcoming research.

2. Related Work

Zero Trust has attracted a lot of interest in cloud security, which has resulted in a large amount of research examining its foundations, uses, and efficacy. This section provides a concise summary of related research done in Zero Trust, emphasizing important discoveries and contributions made by earlier investigations. In the subject of network security, several articles and research papers have advanced and deepened our understanding of the zero-trust paradigm. F. Tang, C. Ma, and K. Cheng et al. [1] explained that this study concentrates on zero-trust network authentication technologies. Furthermore, a privacy-preserving authentication technique for zero-trust architecture is built using Traceable Universal Designated Verifier Signature (TUDVS) technology. Moreover, the efficiency of the suggested approach is examined and its security is demonstrated. M.A. Azad, S. Abdullah, J. Arshad, H. Lallie, and Y.H. Ahmed et. al. [2] described that the zero-trust model, its guiding principles, and its implementation are all thoroughly and in-depth examined by the writers, who also offer suggestions for businesses considering this course of action. They also concisely explain the concerns with the zero-trust model's security and privacy for users and devices. A. Damaraju et. al. [3] first discusses the benefits, implementation approach, and guiding principles of zero-trust architecture for securing corporate assets and limiting cyber threats. Additionally, this paper offers helpful advice for enterprises looking to implement ZTA and improve their cyber defense posture in a dynamic threat landscape by combining empirical data with an expert viewpoint. S.R. Pokhrel, G. Li, R. Doss, and S. Nepal et. al. [4] explained that the categorize ZTA operationalization approaches into three different categories for the first time in this paper: centralized ZTA operationalization (cZTA), federated ZTA operationalization (fZTA), and decentralized ZTA operationalization (dZTA). Using FL and distributed ledger's decentralized computing capabilities, along with ZTA's concept, the authors developed a novel operationalization of the ZTA paradigm. F. Wang, G. Li, Y. Wang, W. Rafigue, M.R. Khosravi, G. Liu, Y. Liu, and L. Qi et. al. [5] described an accurate traffic flow prediction method based on location-sensitive hashing (LSH) that preserves privacy was employed by the authors in this work. After conducting many tests on an actual traffic dataset, the authors finally show that their suggested work is feasible in terms of efficiency and forecast accuracy while maintaining the privacy of sensor data. T. Stephen and A. Abbas et. al. [6] clarifies the prospects and practical difficulties associated with implementing ZTA in the context of the pandemic response. The results show that although ZTA has the potential to support privacy and security measures, some critical issues need to be resolved for its integration to be successful. The report also emphasizes how crucial it is for administrators, doctors, and IT specialists to work together to successfully adopt and maintain ZTA frameworks. Healthcare organizations can contribute to more secure and resilient healthcare ecosystems during and after crises by adopting ZTA principles, which will also help them become more robust against cyber-attacks, protect patient data, and guarantee the integrity of digital health services. T. Vang and M.L. Lind et. al. [7] describe that it is appropriate to examine cloud adoption in a zero-trust setting using the extended TAM-TOE paradigm. The model clarifies and highlights the several variables that might be utilized to forecast the uptake of cloud computing. Compatibility and perceived ease of use significantly predicted perceptions about the usefulness of cloud computing; trading partner support, perceived ease of use, and perceived usefulness significantly predicted cloud adoption intention in a zero-trust environment; and complexity, top management support, training, and education significantly predicted perceptions about the ease of use of cloud computing. S. Sarkar, G. Choudhary, S.K. Shandilya, A. Hussain, and H. Kim et. al. [8] compare the cutting-edge feature sets that are unique to each requirement that is employed in zero-trust cloud network research models. The features are thus divided into three primary categories based on nine parameters: frameworks, proofs-of-concept, and zero-trust-based cloud network models. The study also addresses domain-specific problems

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 09 September 2024
Page No: 2377 - 2384
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2024.0326

that plague contemporary cloud computing networks, utilizing intelligent security orchestration, automation, and response in addition to selecting and implementing features that will be essential for networks of the future. The difficulties with cloud platforms and the prerequisites for switching to zero-trust architecture are also covered in the paper. Lastly, several avenues for future study are explored, including the integration of new technologies into the ZTA to create reliable enterprise networks based on trust that are hosted in the cloud. W. Yeoh, M. Liu, M. Shore, and F. Jiang et. al. [9] examined the CSFs for putting zero-trust cybersecurity into practice by running a three-round Delphi study to get the opinion of a panel of twelve cybersecurity specialists. Eight factors make up our multi-dimensional CSFs framework: identity, endpoint, workload and application, data, network, infrastructure, visibility and analytics, and automation and orchestration. We created a framework for maturity assessments based on the CSFs that allows organizations to assess their level of zero trust maturity. This study provides a practical guiding framework for businesses and advances the theoretical understanding of how to implement zero trust from many angles. F. Federici, D. Martintoni, and V. Senni et. al. [10] described in this paper the architecture that enables multi-level authorization to offer fine-grained access control, improved scalability, and maintainability is the secure solution that goes beyond the conventional perimeter-based security method. The deployment of the suggested solution is also covered, including the security of a complex IIoT infrastructure's network and edge domains utilizing open-source technology. The article concludes by outlining a model-based, risk-driven methodology that will aid in the transition of current infrastructures to the solution architecture. Two pertinent scenarios for the aerospace sector are used as a point of reference to validate the strategy. P. Phiayura and S. Teerakanok et. al. [11] presents a thorough framework for the ZTA migration. This study's methodology consists of an analysis and synthesis of published research on ZTA migration. The results of current knowledge build a procedure that is motivated by the ZTA migration. The report also discusses the shortcomings in current ZTA migration strategies and migration challenges. To create quicker procedures, a thorough zero-trust migration architecture is created. The suggested framework can be applied as a model of reference for a smooth transition to ZTA. P. Divya and A.S. Sherin et. al. [12-14] explain a zero-trust network is a security technique that requires users to be continuously authorized, authenticated, and validated before granting access to network, data, and applications. This approach uses advanced technologies like multi-factor authentication, next-generation endpoint security, and identity & access management to maintain strict security. A.I. Weinberg and K. Cohen et. al. [15] explore AI's potential to enhance real-time decision-making in quantum computing (ZT) through Machine Learning algorithms. It demonstrates that a chaos theory-based strategy can reduce cyberattacks when combined with eXtended Detection and Response. The report also addresses challenges in ZT migration and automation. A. Deshpande et. al. [16] intends to investigate the general incentives, as well as the advantages and disadvantages, for businesses that have either implemented or are currently assessing various solutions, such as ZTNA, to quickly allow their employees to work from home safely and effectively. A synopsis of the zero-trust architectural paradigm is shown in Table 1. It also provides a summary and key contributions of several writers.

3. Zero Trust Architecture

A lot of businesses are switching to cloud-based services and systems for a variety of purposes, including data hosting and computing device use. Although cloud-based systems have numerous advantages, such as flexibility and scalability, they can also cause security flaws in the IT infrastructure of a company. In addition to becoming a crucial part of network operation, cloud-based systems are also becoming a more common attack surface in zero-trust security models. Account hijacking, data breaches from external or internal actors, misconfigurations, zero-day vulnerabilities, and malware are a few possible attack vectors against cloud-based systems. ZTA implementation makes sure that to utilize network resources, users, devices, and applications must always be authenticated and granted permission. It also mandates that regulations for network usage and access control be put into place

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 09 September 2024
Page No: 2377 - 2384
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2024.0326

according to the user's identification, the device's state, and other contextual factors. To achieve more resilient and dynamic security, we will examine many potential zero-trust security solutions in various organizational contexts in this section.

Table 1 Summary of Zero Trust Architecture Paradigm

Paper Title	Key Findings and Contributions
Augmenting Zero Trust Architecture to Endpoints Using Blockchain: A State-of-The-Art Review	The authors explore the integration of ZTA with blockchain-based intrusion detection and prevention, highlighting its potential to enhance detection methods, identify unresolved issues, and explore potential solutions and future possibilities.
Security of Zero Trust Networks in Cloud Computing: A Comparative Review	This study compares zero-trust cloud network models, frameworks, and proofs-of-concept to identify security flaws in contemporary cloud computing networks, enabling future academics to focus on these issues.
Zero trust cybersecurity: Critical success factors and A maturity assessment framework	This study uses Delphi to identify Critical Success Factors (CSFs) for zero trust implementation, providing guidance for organizations to optimize cyber security resource allocation through maturity assessment and evaluation of current implementations.
The Usage of Clouds in Zero-Trust Security Strategy: An Evolving Paradigm	This research explores various zero-trust security solutions, their advantages, and challenges in cloud implementation. It provides insights for organizations considering adopting this approach, aiming to help them choose the most suitable solution for their needs.
Zero Trust Implementation in the Emerging Technologies Era: Survey	The article provides recommendations for enterprises transitioning to a secure ZT model, offering best practices for smooth adoption and strengthening cybersecurity defenses.
Zero Trust Security Paradigm: A Comprehensive Survey and Research Analysis	This study explores how businesses can utilize and adapt to a changing threat landscape, providing cybersecurity specialists with practical insights to safeguard modern digital infrastructures.

3.1. Conceptualization of Zero Trust Architecture

The main concept is before accepting anyone or any device into your network, check them all. Rather than assuming someone is secure, you should properly check their identity and the state of their equipment when they join your network. Limit who is granted access, second. Just like not everyone in the club gets VIP access, users and devices should only have access to the specific resources they need to do their work, nothing more. That way, even calculating intruders cannot enter. To put it plainly, zero trust security is the idea that you shouldn't blindly trust anybody or anything and that, like a vigilant club bouncer, you should only give individuals the keys to what you need. Operating on the premise of mistrust by default, "zero trust" is a cybersecurity approach that demands continuous verification of all individuals obtaining access to network resources was the idea behind zero trust. It secures digital assets with robust authentication, ongoing monitoring, and strict access control, and it can identify threats from both internal and external sources. This method breaks with traditional security paradigms by prioritizing stringent procedures and creating a fortress-like environment where every entry is thoroughly examined. It is essential for defending against modern cyber threats and data breaches. Further, zero-trust cybersecurity improves security by making continual authentication necessary and reducing hackers' ability to roam across networks [16-17]. Restricting permissions strengthens

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 09 September 2024
Page No: 2377 - 2384
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2024.0326

protection against potential threats and lessens unauthorized access to sensitive data. The approach creates a win-win situation for enhanced security and improved network operations by implementing rigorous access controls and monitoring, which also boosts overall operational efficiency.

3.2. Component of Zero Trust Architecture

Zero Trust operates on the tenet that devices must first be verified before being granted access to vital data, information, or network resources within the company. Appropriate policy definitions, user and device characterization, and profiling can help achieve this. With the help of this definition, we would be able to decide on access control and implement regulations according to established guidelines. Three logical elements are there for Zero Trust Architecture (ZTA) to overcome this. A key element of the Zero Trust Architecture (ZTA) is the Policy Decision Point (PDP), which is in charge of deciding on access control and authorization by the rules established for people, networks, devices, processes, and IP traffic types. Real-time and dynamic decision-making about access control is done while taking into account pertinent device or user attributes. PDP is in charge of carrying out and upholding the policies (rules, relevant data, user behavior, device type, and risk assessment variables). Based on the established policy rules, the PDP also determines what degree of access privileges should be given to a certain user, device, or application. The Policy Enforcement Point (PEP), which is in charge of enforcing the access control choices made by the PDP, is contacted by the PDP once it decides on policy enforcement. The PDP ought to be set up in a ZT as a centralized element that gets access requests from different people, devices, apps, and network resources, among other sources. For the sake of compliance and auditing, the PDP also keeps a record of all access requests and decisions. Low-level policies and high-level policies are the two categories into which policies may be divided. High-level rules specify how to implement and enforce low-level policies, whereas low-level policies are usually implemented at a granular level specifying which people, devices, or applications are authorized to utilize certain resources under what circumstances. The PDP's choices about access control must be put into effect by the Policy Enforcement Point. The PEP enforces the decision sent by the PDP and may take the form of a hardware component, software, or server-side operation. Because it reduces the amount of time a user must wait to access a certain resource, the best place for PEP is close to the device and the user who needs access. As the network's resources and devices grow over time, the PEP system must be scalable to accommodate the expanding network of resources and devices. By overseeing the link between resources and the person requesting access, the Policy Administrator serves as the gatekeeper. To decide whether to approve or reject a session, the PA closely collaborates with the policy decision point. The PA is also in charge of providing users with the credentials or authentication tokens they need to access business resources. To implement control policies at the network and application levels, the PA works closely with the PEP and is also in charge of policy enforcement. The PA and PDP are often implemented at the same level.

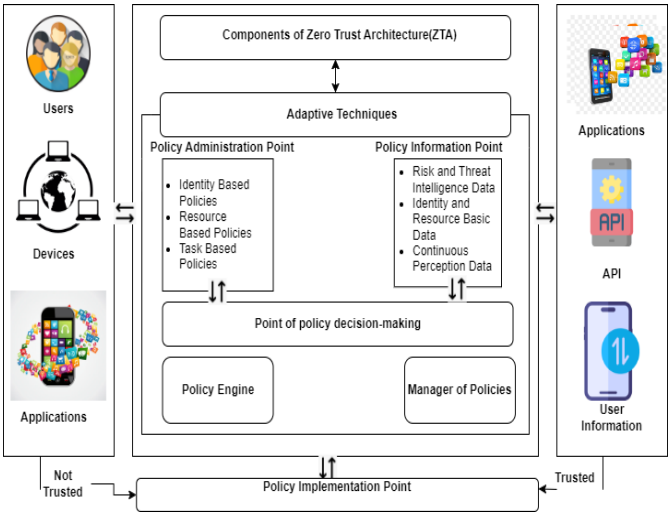

Figure 2 Architectural Paradigm of Zero Trust Architecture

All network interactions, including those between users, various devices, and apps, as well as those involving related resources like data, APIs, and apps, are covered by the logical framework of zero trust security and have been elaborated in Figure 2. The components of PE and PA make up the PDP. The trust algorithm, a critical decision-making process, is carried out by the PE component, which is referred to

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 09 September 2024
Page No: 2377 - 2384
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2024.0326

as the "brain" of the zero-trust architecture. Based on data from PIP and PAP, including behavioral analysis, threat intelligence, network traffic, and access controls, it continually assesses how trustworthy each network member is. Authorization policy management is done continually by the PA component. The PEP is responsible for putting these regulations into practice and serves as a communication channel between users, devices, apps, and the resources they need.

3.2.1. Cloud-Based Zero Trust Architecture

The ZTA components of the cloud-based system may be set up and controlled online. By moving implementation to a cloud-based service, the cloud-based ZTA offers scalability, resilience, security, and affordability. With this configuration, access restrictions and regulations that are enforced at the edge point following cloud access may be defined, allowing PDF capability to be enabled in the cloud. ZTA allows for the usage of Platform as a Service (PaaS) and Software as a Service (SaaS) as the Policy Enforcement Point (PEP) and Policy Decision Function (PDF). PaaS and SaaS can offer the resources necessary to set up and enforce access control restrictions in this configuration. For policy and access control, cloud-based zero-trust systems can also use systems like Google, Azure, or Amazon Web Services.

3.2.2. Blockchain-Based Zero Trust Architecture

Distributing ZTA functionality throughout the network is another possible use for blockchain technology. Smart contracts and distributed ledger technology can be used to implement PDPs and PEPs in a blockchain-based ZTA. Smart contracts installed on network nodes can be used to implement PEPs in a ZTA based on blockchain technology. The PEP smart contract can utilize the access PDP smart contract to authenticate the identity of the person or device attempting to access a resource and determine whether or not they are authorized users. The PEP smart contract enforces access control policies based on the PDP smart contract's policy check. The blockchain maintains a tamper-proof record of all transactions, increasing security and privacy for users and devices. This method reduces the single point of attack. Despite the complexity of processing blockchain transactions, a blockchain-based implementation of PEP and PDP can offer companies enhanced security and decentralized decision-making.

Conclusion

The study concludes by highlighting the significance of Zero Trust in contemporary cybersecurity, especially in cloud contexts. It provides both theoretical insights and useful implementation instructions, advocating for using ZTA as a crucial defense mechanism against increasing cyber threats. According to the paper, implementing a zero-trust strategy will be crucial to safeguarding digital assets as businesses increasingly turn to cloud-based systems. This will provide robust and dynamic security in the face of constantly changing cyber threats.

References

[1]. F. Tang, C. Ma, K. Cheng, (2023), Privacy-preserving authentication scheme based on zero trust architecture, Digital Communications, and Networks, doi: https://doi.org/10.1016/j.dcan.2023.01.02.

[2]. Azad, Abdullah, Arshad, Lallie, and Ahmed. (2024). Verify and trust: A multidimensional survey of zero-trust security in the age of IoT. Internet of Things, 2-27, doi: 10.1016/j.iot.2024.101227.

[3]. Damaraju. (2024). Implementing Zero Trust Architecture in Modern Cyber Defense Strategies. Unique Endeavor in Business & Social Sciences, 3(1), 173-188.

[4]. Phokrel, Doss, and Nepal. (2023). Towards Decentralized Operationalization of Zero Trust Architecture. 1-11.

[5]. Wang, Li, Wang, Rafique, Khosravi, Liu, Liu, Qi. (2022). Privacy-aware Trafic Flow Prediction based on Multi-party Sensor Data with Zero Trust in Smart City, ResearchGate, 2-19, doi: 10.1145/3511904.

[6]. Stephen, Abbas. (2024). Zero Trust Architecture for Securing Digital Health Technologies: Insights from Healthcare Workers in Pandemic Times. ResearchGate. doi: 10.13140/RG.2.2.34742.31048.

[7]. Vang, Lind. (2024). Factors Influencing

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 09 September 2024
Page No: 2377 - 2384
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2024.0326

Cloud Computing Adoption in a Zero-Trust Environment. Advances in Machine Learning and Artificial Intelligence. 5(1), 1-18.

[8]. Sarkar, Chaudhary, Shandilya, Hussain, and Kim. (2022). Security of Zero Trust Networks in Cloud Computing: A Comparative Review. Sustainability. doi: 10.3390/su141811213.

[9]. Yeoh, P., Saini, N., Gulzar, Y., Turaev, S., Kaur, A., Nisa, K. U., & Hamid, Y. (2024). Zero trust cybersecurity: Critical success factors and A maturity assessment framework. Computer and Security. 1-13. doi:10.1016/j.cose.2023.103412.

[10]. Federici, Martintoni, and Senni. (2023). A Zero-Trust Architecture for Remote Access in Industrial IoT Infrastructures. Electronics, 12(566). doi: 10.3390/electronics12030566.

[11]. Phiayura, teerakanok. (2023). A Comprehensive Framework for Migrating to Zero Trust Architecture. IEEEAccess, 1-27. doi: 10.1109/ACCESS.2023.3248622.

[12]. Divya, A. (2022). A Zero Trust Framework Security to Prevent Data Breaches and Mitigate the Cloud Network Attacks, International Journal for Research in Applied Science & Engineering Technology (IJRASET), 10, 3530-3538.

[13]. Shakeel, Dwivedi. (2022). Performance Analysis of Supervised Machine Learning Algorithms for Detection of Cyberbullying in Twitter. 5th Springer International Conference on Intelligent Sustainable Systems (ICISS). 195-199. doi: 10.1007/978-981-19-2894-9_29.

[14]. Shakeel, Dwivedi. (2023). A Survey on Detection of Cyberbullying in Social Media using Machine Learning Techniques, 4th Springer International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV). 334-346.

[15]. Weinberg, Cohen. (2024). Zero Trust Implementation in the Emerging Technologies Era: Survey. arXiv, 2-15.

[16]. Deshpande. (2021). A Study on Rapid Adoption of Zero Trust Network Architectures by Global Organizations Due to COVID-19 Pandemic. New Visions in Science and Technology, 1, 27-33.

[17]. J. Kindervag, S. Balaouras, and L. Coit, (2010) No More Chewy Centers: Introducing The Zero Trust Model Of Information Security. For Security & Risk Professionals, 1-13.