10.31341/jios.48.1.8
Open Access

UDC 004.75:004.056
Survey Paper

The Usage of Clouds in Zero-Trust Security Strategy: An Evolving Paradigm

Jyoti Bartakke *Jyotibartakke@hotmail.com*
Zeal Institute of Business Administration,
Computer Application Research, Nerhe, Pune, India

Rajeshkumar Kashyap *rajdlw@gmail.com*
Sadhu Vaswani Institute of Management
Studies For Girls, Pune

Abstract

Zero-trust security is a security model that assumes no entity is implicitly trusted, regardless of its origin or scope of access. This approach requires continuous verification of all users, devices, and applications before granting access to resources. Cloud computing is a model for delivering IT resources and applications as a service over the Internet. Cloud computing offers many benefits, including scalability, agility, and cost savings. However, cloud computing also introduces new security challenges. This paper proposes a survey-based research methodology to evaluate the usage of clouds in zero-trust security strategies. The paper identifies different zero-trust security solutions, their key features, and the benefits and challenges of implementing these solutions in the cloud. The paper will also discuss the costs and benefits of different zero-trust security solutions. The findings of this research will be valuable for organizations that are considering implementing a zero-trust security strategy in the cloud. The paper will provide guidance on how to choose the best zero-trust security solution for organizational needs and how to implement it effectively.

Keywords: Zero-trust security, Cloud computing security challenges, Trust management, Zero-trust security approach, Zero trust benefits, Zero-trust security challenges

1. Introduction

Cloud computing has become a popular choice due to its scalability, flexibility, and cost efficiency. However, it also presents security challenges that traditional models struggle to address. Data security is crucial in cloud computing, as data is accessible globally and dynamic environments make it difficult to monitor access. Building secure cloud computing requires building trust in the cloud service provider and reliance on their services. This paper proposes a conceptual framework for trust-based permission systems within the cloud computing framework, introducing the zero-trust model. This model grants access based on user identity, device, and context, eliminating assumptions about user or device trustworthiness. This approach offers a safer approach by not relying on conventional security paradigms. Access is granted only upon request, contingent on the user's identity, device, and context, ensuring enhanced security through the zero-trust model.

1.1. Importance of Building Trust in Cloud Environments

Trust is paramount in the realm of cloud computing. Establishing trust between cloud service providers (CSPs) and cloud customers (CS) is essential for fostering secure and reliable interactions. With the rise in cloud service usage, concerns about identity theft, data breaches, data integrity, and confidentiality have intensified. These challenges underscore the significance of robust trust management practices. Building trust involves not only ensuring the credibility of cloud service providers but also enabling cloud customers to have confidence in the services they use. Trust in cloud environments is pivotal for users to confidently store, process, and manage their data in the cloud.

2. Literature Review

Developing trust in cloud computing is challenging. Numerous investigators are currently working to develop a reliable and effective trust strategy for the paradigm of cloud computing. There are many trust structures, designs, and frameworks that have been proposed in order to build relationships between cloud customers (CS) and CSPs that are based on trust. This section covers the best work in the field.

[1] The authors conduct a comparative review of the security aspects of Zero Trust Networks (ZTN) in the context of cloud computing. The authors analyze and compare various security measures implemented in Zero Trust Networks, focusing on their application within cloud computing environments. The paper discusses different approaches and technologies related to Zero Trust Networks, evaluating their effectiveness, advantages, and potential challenges when applied in cloud computing scenarios. The authors might explore how Zero Trust Networks enhance security, mitigate risks, and provide a secure framework for cloud-based applications and data.

[2] This paper provides an in-depth overview of security issues related to cloud computing. The authors conducted a comprehensive survey, likely reviewing existing literature and research findings in the field.

[3] The authors propose a framework for securing electronic healthcare systems (EHSs) based on mutual trust. They argue that traditional access control frameworks are not sufficient to protect EHSs from modern threats and that a mutual trust-based approach is needed.

[4] In this paper, the authors likely present a novel approach or algorithm aimed at measuring and quantifying trust levels within cloud computing systems. Trust quantification in this context likely refers to assessing the reliability and credibility of various elements within cloud computing, such as services, resources, or entities.

[5] In this paper, the authors propose a novel method to assess the trustworthiness of users in cloud computing environments. The model is designed to evaluate user trust based on their behavior data, which may include various interactions, activities,

or transactions within the cloud system. By analyzing this behavioral data, the model likely aims to identify patterns and indicators that can be used to determine the level of trust associated with each user.

[6] the authors probably propose a system that assesses the trustworthiness of cloud services. The evaluation is likely based on evidence, which could include various data points and indicators related to the performance, reliability, and security of cloud services. Fuzzy logic, a mathematical framework dealing with uncertainty and imprecision, is likely used to handle the vagueness and uncertainty in the trust evaluation process.

[7] In this paper, the authors probably explore the complexities associated with establishing and managing trust in cloud computing environments. Trust management in this context typically involves addressing issues such as security, privacy, reliability, and data integrity. The paper might discuss challenges faced by users and organizations when it comes to trusting cloud service providers and the broader cloud ecosystem. Potential topics covered could include trust models, authentication mechanisms, data encryption, access control, and other security measures deployed in cloud environments to foster trust.

[8] In this book, the authors likely provide insights into the principles and practices of implementing a zero-trust security framework. Zero Trust emphasizes the need for strict identity verification and continuous authentication for anyone trying to access resources on a network, regardless of whether they are inside or outside the corporate perimeter. The book probably covers various aspects of network security, including encryption, access control, network segmentation, and continuous monitoring, all centered around the Zero Trust model.

[9] In this document, the author describes, the concept of Zero Trust Architecture (ZTA) is explained. Zero Trust is a security approach where organizations do not automatically trust any user or system, even if they are inside the corporate network. Instead, it emphasizes strict verification and least privilege access for everyone trying to access resources on the network, regardless of their location.

[10] The report defines zero trust as a security model that assumes that no entity is inherently trusted, whether inside or outside the organization's network. This approach requires continuous verification of all users, devices, and applications before granting access to resources.

[11] Introduced cloud research categorization. The authors argue that having a clear understanding of what is needed to deliver dependable software services helps to increase trust in the cloud. When it comes to resolving technical issues and fostering trust, it offers a range of transparency levels. The authors have also looked into the characteristics of operational trust in the cloud that incorporate versatility, flexibility, adaptability, dependability, and accessibility. In this article, the authors give a concise overview of the cloud infrastructure qualities that can be utilized to assess how secure cloud operations are.

[12] The paper provides a systematic literature review of the state-of-the-art trust evaluation mechanisms in cloud computing. The authors begin by defining trust and discussing the different types of trust that can exist in cloud computing. They then discuss the challenges of building trust in cloud environments, such as the lack of

visibility into cloud infrastructure, the dynamic nature of cloud environments, and the potential for insider threats.

[13] This paper offered a trust architecture that determines the security potency and trust value of cloud services. Cloud service users can successfully use the trusted model to choose a specific cloud service. The writer claims that cloud providers can assess a cloud service's strengths and weaknesses using the suggested trust model as a benchmark."

[14] Cloud security customers' resources, data, and apps were the subject of an investigation by authors. Additionally, the authors in this study are attempting to describe the trust problem and offer solutions for CSPs.

[15]Authors offered a contemporary trust framework that focuses on standards-based and certification-based security checks for cloud computing infrastructure services. The authors have also listed a number of essential elements for IAAS security. The trust framework that has been provided determines whether a cloud service is trustworthy based on a security analysis using standards and certification that the cloud provider has successfully completed.

[16] The author discussed how to group different cloud environment stages. The fuzzy centroid method of defuzzification is used by the authors to examine the measurement of trust value for CSPs and provide a more useful trust model as a result. Three criteria are also used by the authors to evaluate trust: accessibility, restructuring time, and dependability. As a result, this trust model improves the safety and reliability of cloud-based services. As an outcome, this model measures trust with fewer variables and is more realistic.

[17] stressed the importance of trust in the cloud environment. Because trust ensures the security of the cloud environment, the authors came to the opinion that it is a crucial component of cloud computing. Additionally, trust aids in the selection of trustworthy customers and services by both the user and the CSP. In order to assess trust based on various factors, the most recent trust models are also presented. This work gave a summary of the trust model based on cloud-based fuzzy logic

[18] The authors begin by discussing the importance of trust in cloud computing. They note that cloud users need to be able to trust their cloud providers to protect their data and applications and to provide reliable and secure services.

[19] In this paper, the authors probably explore the challenges and considerations involved in establishing a zero-trust security model within cloud computing contexts.

3. Methodology

This paper is a survey-based research paper. So, we use qualitative and quantitative research methodology that involves a comprehensive approach to understanding cloud security challenges and the implementation of the zero-trust security model.

3.1. Data Collection

We use a secondary data collection method. Gathering relevant data from academic sources and research papers on zero trust and cloud computing. industries that adopted cloud computing for their workloads that industries websites through information collection and also gathering information on traditional security challenges in cloud computing and practical implementations of cloud security strategies, with a focus on zero-trust models.

3.2. Data Analysis

Employing qualitative and quantitative analysis techniques to assess the effectiveness of the zero-trust model. Analyzing real-world case studies and scenarios to evaluate its impact on cloud security.

3.3. Implementation of Zero-Trust Model

Practical implementation of the zero-trust security model in simulated cloud environments, considering diverse use cases and potential challenges.

3.4. Evaluation Criteria

Develop specific criteria to evaluate the success of the zero-trust model in enhancing cloud security. These criteria include factors such as data confidentiality, user authentication efficiency, and mitigation of insider threats.

By adopting this comprehensive methodology, we aim to provide valuable insights into the practical implications of the zero-trust security model in cloud computing environments.

4. Security Challenges In Cloud Computing

The internal security issues that cloud-hosted networks face is covered in this section. The purpose of this section is to highlight the key architectural components of contemporary cloud networks that use traditional network security controls. External forces can cause attacks like ransomware, phishing, data breaches, and malware to affect systems because of vulnerabilities caused by the issues listed below. The existence of vulnerabilities related to virtualization, for instance, is an important factor in the ease with which ransomware can spread from a host operating system to its virtualization and eventually to different host operating systems. Attackers have the power to harm cloud service providers, customers, and IT systems. because of weak security measures and control issues. (1)

There are a number of security concerns with cloud computing that need to be addressed.

Technical problems, legal issues, and other risks are all related to organizational and policy risks. Here are a few current issues that need to be addressed.

4.1. Vulnerabilities in Shared Technology

By leveraging more resources, attackers have a single point of entry and can inflict damage that is disproportionate to the threat. Cloud management and hypervisor systems are two examples of shared technology.

4.2. Account of Service Traffic Hijacking

The benefit of cloud computing is having an Internet connection, but there is also a chance that an account will be affected. A service interruption could happen if a privileged account is destroyed.

4.3. A Danial of Service

Any denial-of-service attack on the cloud provider could have an impact on all principles. (2)

4.4. Weaked Insider

In a cloud scenario, a clever insider can come up with additional ways to attack and hide their tracks.

4.5. Internet Protocol

IP has a number of security holes that can be exploited, such as DNS poisoning, ARP spoofing, and IP spoofing.

4.6. Injection Vulnerabilities

Numerous cloud users may experience serious effects from vulnerabilities at the management layer. A committed insider can come up with additional strategies for attacks and cover-ups.

4.7. Vulnerabilities In the API and Browser

Any security breach in a cloud service provider's API or connect presents a serious risk when coupled with social engineering or web-based assaults.

4.8. Modifications To the Business Model

The business model of a cloud user can experience significant change as a result of using the cloud.

4.9. Abusive Use

There are a lot of cloud computing features that can be used for malicious attacks, like the ability to launch DDoS or zombie attacks with a trailing period.

4.10. Malicious Insider

An insider who is malicious is always a serious risk, but one who works for a cloud provider can harm multiple consumers significantly. (2)

5. Trusting the Cloud: A Traditional Approach

Trusting traditionally in cloud computing information is based on a combination of factors, including the position of the cloud service provider, the level of transparency, and the specific needs of the organization.

The cloud service provider's positions. Cloud service providers (CSP) with a good reputation are more likely to be trusted by their customers. This reputation can be based on factors such as the providers' experience, security certifications, and customer reviews.

The level of security offered by the cloud service provider. CSPs must offer security to save their customers' data. Several techniques, including data encryption, access control, and intrusion detection, can be used to succeed in this security. The level of transparency that the cloud service provider presents. To build trust with customers, cloud service providers must be open and honest about their security procedures and how they safeguard customer data.

The significance of developing cloud computing trust is made clear in this section. In the cloud-based approach, communication between the cloud service providers (CSP) and the customers is possible. without any previous encounters. Because of this, it is frequently difficult to predict the reliability of both the customers and the CSP due to a lack of prior knowledge and experience with both groups Therefore, having no prior transactions and not having sufficient details may cause distrust. Furthermore, cloud computing decision-making facilitation relies heavily on trust. When data processing and storage are separated across globally separated data centers and resources are distributed in the same way, trust problems become critical. consequently, effective. Successful trust management is implemented to enable CSPs and customers to fully trust one another and reap the benefits of cloud computing.

In a service-based framework like cloud computing, the trust model [3] is very helpful for making wise decisions regarding the selection of trustworthy entities. [4] These trust models essentially take into account behavioral observations, recommendations, and previous and current relationship experiences when selecting reliable cloud service providers (CSP) and (CS) cloud customers.[5] Cloud computing offers a highly abstracted, massively dispersed, extremely complex, opaque system. Because of this dispersed and service-based cloud computing design, customers of the cloud must reconsider criteria for selecting trustworthy entities that go above and beyond the usual ones for determining the quality of service. Trust models are different because they vary for different environments, frameworks, and applications.

Because of how things change over time, Trust Management was primarily created for a specific application. Due to the services offered by the cloud, traditional trust management processes are therefore wholly inapplicable to the cloud model [6].

6. Trust Management Challenges for Cloud Computing

6.1. Trust Feedback Legitimacy

It is challenging to assess the trustworthiness of user feedback. In order to boost the reputation of some nodes or harm other nodes, malicious users may spread false trust information on purpose. It can be difficult to track malicious feedback and give expert users credibility ("Cloud Armour Project"). Assessing trustworthiness in feedback would be made possible by the existence of an independent quality assurance body that could inform consumers about sources of trust.

6.2. Lack of transparency

The data in cloud data centers is dispersed across multiple geographical locations and different virtualization levels. The most well-known CSPs of today, such as Amazon EC2/S3 and Microsoft Azure, do not completely disclose how physical and virtual servers are used. Only service event logs and virtual hardware metrics for performance are currently accessible to clients. Client confidence in the cloud would increase with greater transparency.

6.3. Loss of visibility and control

In a cloud computing environment, where numerous remotely located computing resources are involved, millions of nodes and chains of services are heavily shared. Many different nations' laws govern these resources, some of which fall outside the CSPs. As a result, once the data leaves the perimeter of the service, the data owner or user no longer has control over it. This loss of asset control in cloud computing reduces confidence in the service and increases the possibility of data loss.

6.4. Accountability complexity

Cloud accountability demands complex real-time accountability and places a strong emphasis on data security. Some of the complexities in the area of accountability arise as a result of the cloud framework's unique structure. • OS logging versus file-centric logging • Scale, size, and scope of logging • Live and Dynamic Systems • Challenges incorporated as a result of virtualization. Accountability should cover both physical and virtual server events, not just those on virtual servers. The accountability of physical servers is complicated by a lack of connection between the physical and virtual servers. Although current tools offer OS-centric logging, file-centric logging would allow users to follow data from the time it is created until the moment it is destroyed. In the expanding cloud scenario, where detailed logging could wipe out the cloud storage holding logs, managing the scale of logging for efficient logging is crucial.

6.5. Weak trust chains

Because of the globalized nature of the cloud infrastructure, the trust chain within the cloud and the consumer may be weak at some points along the chain. Without sufficient verification of their reliability, a lot of new services, third parties, and providers could be added to the chain of on-demand services. Users should no longer be skeptical about the reliability of trust relationships because of the need for standardized monitoring and logging of the chain of relationships.

6.6. Lack of standardization and interoperability

Being a relatively new technology, cloud computing lacks interoperability and standards. Cloud adoption is hampered by inconsistent security standards that fail to address data privacy and trust issues. Currently, there aren't any standards for tracking data, evaluating trust, or auditing the object life cycle for data provenance. There isn't currently a standardized model for cloud management that could assess and track policies across various cloud offerings. (7)

7. Zero Trust Model In Cloud Computing

"Trust nothing verifies everything" is the main goal of zero trust security. This means that even if a customer or device is already connected to the network, they still need to be authenticated and given permission before granting access. The traditional security model, which demands that users and devices within the network be reliable, is changed by the zero-trust model. The traditional approach is less effective in a threat environment where internal networks are now easily accessible to attackers [1].

7.1. Zero trust model-based principles

Least privilege: Only the access necessary for users and devices to carry out their job-related duties should be granted.

Micro-segmentation: Only the resources required for a given purpose should be present in each of the network's small segments.

continuous monitoring: Any suspicious activity should be constantly looked out for on the network. (8)

A security structure called "zero trust" protects premises or cloud-based assets by preventing outsiders and unmanaged devices from accessing them, as well as by reducing all lateral movement. Data encryption, device verification, "identity and access management (IAM)", and "multi-factor authentication" (MFA) are among the technologies employed by zero trust. (9)

Features	Traditional model	Zero trust model
Approach	Trusts all users within the network	no user can be trusted, regardless of location
Cost	Less expensive to implement	More expensive to implement.
Authentication	Focus on user authentication	User and device both authentication
Security focus	Perimeter based security	Micro-segmentation and continuous monitoring
Response to threats	Incident response	Continuous monitoring and threat prevention

Table 1. Difference between the Traditional trust model and Zero trust model (10)

8. The Proposed Model Of Zero Trust

With the increasing issues of cloud infrastructure, modern security is recommended.

When putting new infrastructure into the cloud, security is the primary concern. The zero-trust security model for Cloud computing infrastructure is not compatible with the traditional security model. As a result, implementing the cloud requires zero trust. The zero-trust strategy uses strict access controls and keeps a record of all data used to improve cloud security. This is how the zero-trust architecture can better identify and stop external attackers while reducing security breaches brought on by insider attacks in the cloud infrastructure. The zero-trust cloud computing scheme also needed to successfully integrate and incorporate difficult practices, policies, and technology.

However, Figure 1 shows the basic concept behind zero-trust strategies.[19]

8.1. User identity is the first column.

Zero trust places a high value on the ongoing verification of trusted users. It is possible to restrict user access and privileges utilizing technologies such as multi-factor authentication and the concept of Identity Credentials, and Access Management (ICAM), as well as ongoing user credibility monitoring and validation technologies. Technologies like traditional web gateway solutions that secure and protect user interactions are also important.

8.2. Device security is the second column.

A fundamental aspect of a ZT approach is the safety and trustworthiness of devices. Data from some "system of record" solutions, like mobile phone device managers, can be helpful for determining how trustworthy a device is. Every access request should also undergo additional evaluations (such as checks for compromise states, software versions, protection statuses, encryption facilitation, etc.).

8.3. The third column is network security.

Some networks, operations, and tools are becoming more important than perimeter defenses. This is not the result of one technology or use case, but rather the result of a number of new services and technologies that allow users to communicate and work together in novel ways. Zero-trust networks truly make an effort to distinguish important data from other data by introducing perimeters in from the network edge. However, the edge is now much more clearly discernible. The traditional perimeter firewall approach of "castle and moat" is insufficient.

8.4. Workload and Application Security is the fourth column.

The adoption of zero trust depends on the security and effective management of the application's layer, computer containers, and machine virtualization. Making more accurate and thorough access decisions is possible with the help of an understanding of and management of the technology stack. Multi-factor authentication is increasingly crucial for providing applications in zero-trust environments with proper access control, as is to be expected.

8.5. Automaton: The fifth column

Security Automation and Orchestration is effortless and economical. ZT frequently employs security automation reaction tools, which employ workflows to automate operations across various products while preserving end-user control and participation Automated tools are used in security operation centers for analyzing user and entity behavior as well as security information and event management. These security tools are connected by security automation, which also helps with managing various security systems. Together, these tools can drastically cut costs, even response times, and human labor.

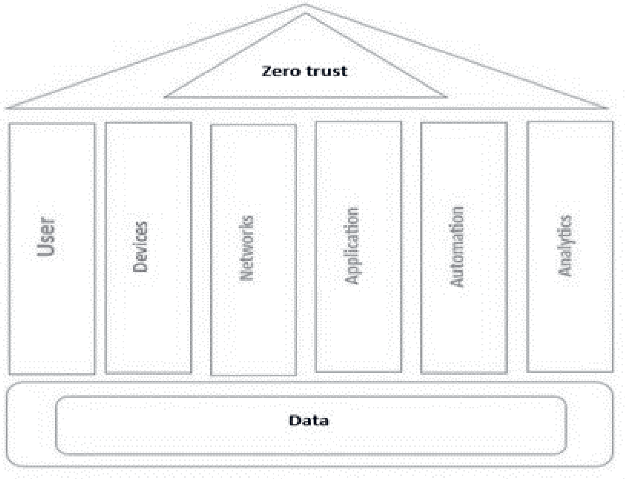

Figure 1. Six columns of the zero-trust security model [19]

8.6. Sixth column: Analytics

Security Analytics and Visibility

Thanks to the zero-trust use of resources such as data security management, advanced security, data analysis systems, security user behavior data analysis, and other analytics systems, security experts can see what is happening in real-time. Setting aside data analysis from cyber-related incidents can aid in the creation of security protocols before an actual attack occurs. (11)

9. Trust Building Is a Foundation

Zero Trust is a framework basis of trust "nothing verifies everything" and needs a flexible deployment model that steady evaluation and tracking first. Access is restricted to using dynamic, sensitive-to-context trust extensions in accordance with the threshold authorization regulations that have been established. The question of "How do we find how trustworthy something is?" is one that arises in this movement towards trust. Many security organizations have trouble coming up with an answer to this dilemma. Traditional programmers make the erroneous assumption that all information and transactions can be trusted. By assuming that all information and transactions are immediately untrue, Zero Trust changes the estimation of trust. How do we create enough trust is the new question. Even though some fundamental concepts and components are applicable to all deployments, there isn't a single strategy that all organizations can use. The organization's goals and requirements will determine the level of trust To manage the trustworthiness of every transaction, environments with zero trust interact with controls for devices, users, data, and apps.

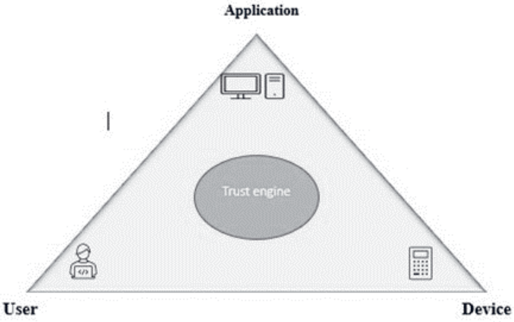

Figure 2. Zero Trust foundational Triangle [19]

"Trust Engine" is able to rapidly assess a user, device, or application's overall level of trust by establishing a "trust score" in a specific network. To determine a policy-based authorization decision, the trust engine assesses the trust score and applies it to each transaction request.

A user, device, or application's trust score reflects how reliable they are. Its value is produced by a variety of factors and circumstances. The trust score may also be affected by information such as past interactions, system knowledge, and access permissions granted or denied by the system.

The trust score of a user, application, or device shows how trustworthy they are. Its value is the result of many different things and circumstances. The trust score may also be affected by information about previous interactions, system knowledge, and access permissions granted or denied by the system.

The Trust Engine uses a "trust score" and the Zero Trust foundational triangle to determine each agent's level of trustworthiness before they join the network. The collection of information about the participants in a network request is referred to as an "Agent" or "Network Agent." A user, an application, and a device are typically included in this information. In order to provide the situational context in actual time, this combination of data is accessed upon request in actual time to provide contextual information and assist users in making the best authorization decisions possible. The customer, application, device, and trust score are combined to create an agent after the trust score has been identified. The request can then be granted by applying the policy to the agent after that [19].

10. Benefits of Cloud Computing In Zero Trust

There are various advantages to zero trust security for cloud computing, including.

10.1. More Powerful Security

Zero trust security is a safer approach than conventional security models because it does not rely on a single point of failure.

10.2. Better compliance with the law

Companies can adhere to compliance standards with the help of zero trust security.

10.3. Reduced cost

By doing away with the need for complicated security infrastructure, zero-trust security can assist organizations in saving money.

11. Challenges Of Implementing Zero Trust Security

Challenges with implementing zero-trust security, including.

11.1. Complexity

A sophisticated security strategy is zero trust security. To implement and manage it, a significant amount of time and money must be spent.

11.2. Cost

Zero security can be expensive to implement. The cost of implementing zero trust security will vary depending on the scope and complexity of the organization.

11.3. Cultural change

Zero trust security needs a change in culture. Employees need to be educated about the new security model and how to operate within it.

Organizations that are considering implementing zero trust security should start by assessing their current security posture. They should also create a strategy for putting into practice zero trust security that considers the issues covered in this paper's discussion.

12. Recommendation for Implementing Zero Trust Security

12.1. Start Small

Don't try to implement zero security across the entire organization all at once. Start by implementing it in a small, controlled environment.

12.2. Get by informing senior leadership.

Zero trust security needs an important investment of time and resources. It is important to get buy-in from senior leadership before starting the implementation process.

12.3. Educate employees

Employees need to be educated about the new security model and how to operate within it. Use of phased approach: implement zero trust security in phases.

Zero trust security is a new security strategy that may help organizations strengthen their security posture. However, it is important to be aware of the issues associated with implementing zero trust security. By following the recommendations that have been discussed in this paper, patients can increase their chances of success.

13. Discussion

One of the biggest trends in cybersecurity today is cloud computing, along with zero trust security. Agility, scalability, and affordability are just a few advantages that cloud computing has to offer. Data loss, data breaches, and unauthorized access are a few of the new security issues that are brought about by this.

Any user or device, no matter of their location or network, cannot be trusted, in the zero-trust security design. Because of this, all requests for access to resources must first be approved. Zero trust security uses a layered approach to security to help reduce the security risks in cloud computing.

It is believed that cloud computing security is a significant issue. Trust is crucial for cloud computing security. It makes it possible for CSPs and customers to locate dependable entities in a heterogeneous cloud infrastructure. Research on cloud computing trust is very active. This was the subject of numerous academic publications. Cloud computing and zero-trust security can be difficult to implement and manage. Organizations need to have a strong understanding of both technologies in order to design and implement an easy solution. The implementation and upkeep of cloud computing and zero-trust security can be costly. Organizations need to factor in the cost of software, hardware, and labor when considering cloud computing and zero-trust security. The security environment of the organization can be studied in great detail thanks to cloud computing and zero-trust security. The protection of this data from unauthorized access is the responsibility of organizations.

Zero trust, despite its difficulties, is a useful security framework that can aid organizations in strengthening their security posture. Organizations can minimize the security risks associated with cloud computing and enhance their overall security posture by carefully planning and implementing a zero-trust solution.

14. Conclusion

The current security difficulties of cloud computing were talked about in this paper. The cloud computing strategy is used by many businesses. As a result, they face numerous challenges. Following that, the difficulties of traditional cloud computing trust were discussed. This paper discussed the significance of zero-trust security in cloud computing. a difference between the traditional trust model and the zero-trust security model. To address these issues, we recommend utilizing the zero-trust model in cloud computing. Cloud computing comes with a lot of problems. Be that as it may, it likewise affects creating trust. Although many cloud service providers claim to provide robust security, the reality is that they face greater failure risks in their efforts to completely protect cloud presence accusers.

The advantages and drawbacks of implementing zero trust security in an organization are discussed in this paper.

The paper offers some suggestions for putting zero-trust security into place. It was difficult for organizations to monitor how users accessed and moved data within the cloud. A concept-based model for a zero-trust cloud computing strategy is proposed and discussed in this study. Both cloud service providers and end users benefit from its effective trust management benefits for cloud computing. Customers of CSPs will find it easier to select dependable providers in the cloud with the assistance of the proposal structure strategy. To provide cloud service providers and customers with security in their businesses, we proposed a zero-trust cloud computing model in this paper.

References

[1] Sarkar, S. et al. (2022) Security of zero trust networks in cloud computing: A comparative review, Welcome to DTU Research Database.: Sustainability. doi: 10.3390/su141811213.

[2] Ramachandra, G., Iftikhar, M. and Khan, F.A. (2017) ‘A comprehensive survey on security in cloud computing’, Procedia Computer Science, 110, pp. 465–472. doi: 10.1016/j.procs.2017.06.124.

[3] Singh, A. and Chatterjee, K. (2017) ‘A mutual trust-based access control framework for Securing Electronic Healthcare Systems’, 2017 14th IEEE India Council International Conference (INDICON) [Preprint]. doi:10.1109/indicon.2017.8487658.

[4] Li, X. et al. (2016) ‘A method for trust quantification in cloud computing environments’, International Journal of Distributed Sensor Networks, 12(2), p. 5052614. doi:10.1155/2016/5052614.

[5] Chen, Z., Tian, L. and Lin, C. (2018) ‘Trust evaluation model of cloud user based on behavior data’, International Journal of Distributed Sensor Networks, 14(5), p. 155014771877692. doi:10.1177/1550147718776924.

[6] Selvaraj, A. and Sundararajan, S. (2016) ‘Evidence-based trust evaluation system for Cloud Services using fuzzy logic’, International Journal of Fuzzy Systems, 19(2), pp. 329–337. doi:10.1007/s40815-016-0146-4.

[7] Khan, M.S., Warsi, M.R. and Islam, S. (2019) ‘Trust management issues in cloud computing ecosystems’, SSRN Electronic Journal [Preprint]. doi:10.2139/ssrn.3358749.

[8] Gilman, even and Barth, Doug. (2017) Zero Trust Networks Building Secure Systems in Untrusted Networks [Preprint].

[9] Rose, S. et al. (2020) Zero trust architecture. doi: 10.6028/nist.sp.800-207-draft2.

[10] ‘Zero Trust Cybersecurity Current Trends’ (2019) American Council for Technology-Industry Advisory Council (ACT-IAC) [Preprint].

[11] Abbadi, I.M. and Martin, A. (2011) ‘Trust in the cloud’, Information Security Technical Report, 16(3–4), pp. 108–114. doi: 10.1016/j.istr.2011.08.006.

[12] Chiregi, M. and Jafari Navimipour, N. (2018) ‘Cloud computing and trust evaluation: A systematic literature review of the state-of-the-art mechanisms’, Journal of Electrical Systems and Information Technology, 5(3), pp. 608–622. doi: 10.1016/j.jesit.2017.09.001.

[13] Shaikh, R. and Sasikumar, M. (2015) ‘Trust model for measuring security strength of Cloud Computing Service’, Procedia Computer Science, 45, pp. 380–389. doi: 10.1016/j.procs.2015.03.165.

[14] Horvath, A.S. and Agrawal, R. (2015) ‘Trust in cloud computing’, Southeast Con 2015 [Preprint]. doi:10.1109/secon.2015.7132885.

[15] Saxena, A.B. and Dawe, M. (2018) ‘Trust Framework for IAAS—a tool based on security checks through standards and certifications’, Information and Communication Technology for Intelligent Systems, pp. 369–376. doi:10.1007/978-981-13-1747-7_35.

[16] Prakash, P. et al. (2018) ‘Enhancement of cloud security and strength of service using trust model’, International Conference on Intelligent Data Communication Technologies and Internet of Things (ICICI) 2018, pp. 1345–1353. doi:10.1007/978-3-030-03146-6_157.

[17] Ritu, Randhawa, S. and Jain, S. (2017) ‘Trust models in Cloud computing: A review’, International Journal of Wireless and Microwave Technologies, 7(4), pp. 14–27. doi:10.5815/ijwmt.2017.04.02.

[18] P, Archana. and P, Meenu. (2014). Trust management in cloud computing: A survey.’, International Journal of Computer Applications, [Preprint]. doi: 108(18), 1-12.

[19] Mehraj, S. and Banday, M.T. (2020) ‘Establishing a Zero trust strategy in cloud computing environment’, 2020 International Conference on Computer Communication and Informatics (ICCCI) [Preprint]. doi:10.1109/iccci48352.2020.9104214.