Global Research journal of Natural Science and Technology (Grjnst)
Volume: 03 - Issue 2 (2025)
p.ISSN: 2790-7643 e.ISSN: 2790-7651
www.grjnst.com

Beyond Perimeter Defenses: Implementing Zero-Trust Security Models for Cloud Computing in the Era of Advanced Cyber Threats

Muafia Intazar
MS, Computer Science, Department of Computer Science, NFC Institute of Engineering and Technology Multan
muafiaintizar@gmail.com
Tehzeeb Zohra
MS, Computer Science, Department of Computer Science, University: NFC Institute of Engineering and Technology Multan
tehzeebzohra@gmail.com
Nadia Mustaqim Ansari
Department of Electronic Engineering, Dawood University of Engineering and Technology, Karachi
nadia.ansari@duet.edu.pk
Rizwan Iqbal
Department of Telecommunication Engineering, Dawood University of Engineering and Technology, Karachi
rizwan.iqbal@duet.edu.pk
Hassam Gul
International Islamic University, Islamabad
hassamgulp@gmail.com

Abstract: *Cloud computing has significantly transformed IT structures whereby organizations can address their computational needs through flexible, adaptable, and cheaper platforms. However with the growing usage of cloud services, the traditional perimeter security model cannot effectively secure the critical organizational assets against threats such as advanced persistent threats, internal threats and malware. This paper focuses on how zero-trust security models can be used to address these emergent threats in a cloud computing context. Zero-trust, as a security model that is based on ''never trust, always verify,'' implies the constant verification of everyone both inside and outside the organization with the intent to access systems or applications. This paper aims to review the limitations of the classical models, the principles of zero-trust, and the opportunities it provides and faces: minimizing attack pathways, enhanced access, and better management of incidents. There are, however, challenges organizations face when implementing zero-trust frameworks, these*

include integration with old systems and technologies, limited resources, and organizational change. Considering the experiences of IT experts and cybersecurity professionals from different branches and types of companies, the study demonstrates the level of effectiveness and issues in implementing zero-trust, case within sectors like finance, healthcare, and e-commerce. The result indicates that while zero-trust models are effective, the approach's implementation suffers from sector restriction, the large organization and high risk sectors such as finance, health sector have better adoption results. This study also outlines strategies organizations can adopt and implement in order to embrace zero-trust security in cloud environments as well as some of the challenges linked with its implementation.

Keywords: *Perimeter Defenses, Zero-Trust Security Models, Implementing, Cloud Computing, Advanced Cyber Threats*

1. Introduction

1.1 Background

Cloud computing in IT has been on the rise in the recent past giving organizations a better way of storing, securing and accessing their information and data. Based on the study done by Mell & Grance (2011), the National Institute of Standards and Technology (NIST) defines cloud computing as a ‘‘model for enabling convenient, on-demand network access to a shared pool of configurable resources.’’ This has revolutionized how firms and governments run their Life by outsourcing computing services to external cloud service providers. Cloud computing has taken a central stage in today’s advancements because it has been proved to provide a broad range of benefits such as scalability and flexibility and utility cost structure. Therefore, organizations can easily grow or shrink the IT infrastructure to adapt to changing business demands while avoiding the costs associated with physical hardware.

Although the adoption has brought about several advantages, which has made the use of cloud services a reality in the current society, there is a growing concern of security threats. The cloud environment thus has fundamental differences from traditional on-premises IT, which has most to do with losing control of data as well as their applications as well as

infrastructures. Furthermore, cloud has numerous users and devices to accommodate and multiple cloud resources increase the threats that increase the weaknesses of using the traditional perimeter security model. In traditional security paradigms, threats are considered to be outside, and security is concentrated at the gateway and access control. However, due to the growing similarity between internal and external networks in the cloud, this model has become quite inefficient (Gartner, 2020).

Threat actors are continuously diversifying and adapting their tactics with APTs, insider threats, and sophisticated malware testing existing defenses (Krause, 2021). Such a change in threat has led to the development of the zero-trust security model to effectively address system security threats and especially for cloud services. Zero trust model, which is predicated on the "never trust, always verify" mantra, does not allow any entity, internal or external to a network, to be trusted by default Kindervag 2010. All the access requests must undergo authentication, authorization and monitoring until the security of an organization is not based on traditional perimeter but rather based on the identity. With the growth of cloud solutions and their maximum density, the application of zero-trust security models has become one of the critical approaches to protecting data and minimizing threats from sophisticated threats (Rose et al., 2019).

1.2 Rationale

Cloud computing is becoming popular and along with it, advanced cyber threats require the changes to a new paradigm for the protection of organizations. Older security paradigms such as the perimeter-based model, which worked very well in pre-cloud environments where data and applications were centralized and accessed through company-owned systems, are no longer sufficient in the cloud world where data and applications are located in various parts and accessed through multiple devices. The concept of zero-trust security models has to be examined because the current security paradigm is not suitable for the complexity of cloud environments. Zero-trust security is a better model to address the weaknesses of perimeter protection as well as allowing security measures to be applied ubiquitously, which include identity confirmation, permission control, and supervision.

In addition, with organizations moving more critical applications and sensitive data to the cloud, this has added a new dimension of threat. These models address such issues through the following zero-trust security principles: Reducing the attack surface and limiting the lateral movement of threats. As cyber threats evolve and get innovative, the zero trust security model is both proactive and much more effective for securing cloud environments especially in these days when organizations are adopting digital transformations which heavily rely on cloud computing (Cavoukian, 2020).

1.3 Problem Statement

Cloud computing adoption has continued to grow rapidly thus placing pressure on traditional approaches to computer security that depend mostly on perimeter control. The specific characteristics that cloud computing entails to security includes; Diffused infrastructure security: The cloud infrastructure is spread across different locations. Conventional security measure like firewalls and intrusion detection systems can no longer contain emerging threats such as APTs, insider threats, and sophisticated malware.

The issue can be defined in the constant shift to adopt a new approach when it comes to securing cloud environments since classical perimeter security no longer works. The zero-trust architecture is recognized as a potential solution to combat the threats, yet it is still experiencing low adoption and faces difficulties in implementation in cloud contexts. These are: dealing with the adoption and interconnection of traditional systems, implementing and maintaining secure access, as well as continuous monitoring in complex and constantly evolving cloud environments. This research aims to explore the use of zero-trust security models in cloud computing environments and the main challenge and benefits of using such model, and of course the performance of the model in protecting against modern-day security threats.

1.4 Aim

The purpose of this research is to understand how organisations can adopt or deploy zero-trust security models in cloud computing environments for threat protection. Based on this

analysis of the main concepts, issues as well as the advantages of zero-trust models, we endeavour to identify how such approaches can be effectively employed to protect cloud resources and information. This research will also evaluate the effectiveness and practicality of using zero-trust security models in cloud servicing infrastructures, based on their capacity to protect against the threats and risks that conventional perimeter security lacks the capacity to address.

1.5 Research Objectives

The specific objectives of this research are as follows:

1. **To examine the limitations of traditional perimeter-based security models in cloud environments**: This will involve analyzing the shortcomings of traditional security measures and how they fail to address the complexities of cloud computing.

2. **To investigate the principles of the zero-trust security model**: This objective aims to provide an in-depth understanding of the zero-trust framework, its core principles, and how it differs from traditional security models.

3. **To assess the challenges organizations face in implementing zero-trust security in cloud environments**: This objective will explore the barriers to adoption, such as integration with legacy systems, complexity, and user resistance.

4. **To evaluate the benefits of adopting zero-trust security models for cloud computing**: This includes analyzing how zero-trust models can reduce the attack surface, improve access control, and enhance incident response in cloud environments.

5. **To propose a roadmap for implementing zero-trust security in cloud computing environments**: Based on the findings, this research will provide practical recommendations and strategies for organizations looking to adopt zero-trust security

models.

1.6 Research Questions

The research will be guided by the following questions:

1. **What are the limitations of traditional perimeter-based security models in cloud computing?**
    - This question aims to explore the reasons why perimeter-based security models are inadequate for securing cloud environments.
2. **What are the core principles of the zero-trust security model, and how can they be applied to cloud computing?**
    - This question seeks to identify the fundamental principles of zero-trust security and examine how they can be implemented in cloud environments.
3. **What are the main challenges organizations face when implementing zero-trust security models in the cloud?**
    - This question will investigate the technical, organizational, and operational challenges faced by organizations in adopting zero-trust frameworks.
4. **What are the potential benefits of adopting zero-trust security models for cloud-based infrastructures?**
    - This question aims to evaluate the advantages of zero-trust security in reducing the risk of cyber attacks, minimizing lateral movement, and improving overall security.

5. **What strategies can organizations adopt to effectively implement zero-trust security models in their cloud environments?**

    - This question will explore practical solutions and strategies that can guide organizations in successfully implementing zero-trust frameworks in cloud computing environments.

2. Literature Review

Cybersecurity remains a dynamic environment due to changes in technology and technological themed threats. Specifically, the application of cloud computing has gained much attention from the cybersecurity research community since it is utilized in many organizations and markets. This paper aims to provide an overview of the literature on the adoption of zero trust security architecture, especially in cloud systems, to overcome the weakness of the traditional perimeter-based security approach and threats from new forms of sophisticated cyber threats.

2.1 Traditional Security Models and Their Limitations

Traditionally, network security has always focused on the boundaries of protection like firewalls, IDS and VPNs among others. These security measures work on the basis of a fairly simple concept of incorporating independent internal and external networks. Since the internal network of the organization is apprehended to be secure, the key security concerns revolve around protection from external threats bypassing the outer layer (Firestone, 2018). However, this approach has proven to be increasingly ineffective in the current scenarios that are characterized by the use of cloud platforms.

Patel and Pandya (2019) have noted that perimeter-based security is inadequate for cloud computing because it cannot effectively respond to the conditions engendered by cloud technology where internal and external divisions are not well defined. In a cloud computing environment the organizations do not fully control the environment and data is shared across

different locations and devices, and hence there is no visible border or 'perimeter' (Islam & Liu, 2017). Altogether, attackers are cunning enough to get around the perimeter solutions such as social engineering and spear-phishing and attack the hardcore security layer (Zhou & Rhee, 2020). Hence, perimeter security has failed to protect organizations from internal threats, east-west traffic, and security threats that directly attack the core of cloud networks.

2.2 The Emergence of the Zero-Trust Model

The zero-trust security model started to be developed due to the shortcomings of the perimeter-centric security paradigm. The zero-trust model was first coined by John Kindervag of Forrester research in 2010 and has limited trust to everything with nothing trusted at its fundamental philosophy (Kelley & Fraser, 2019). However, it focuses on constant authorization with constant checks and verification on every user, device, and application that accesses the resources. Zero-trust aims at restricting users' access to certain resources and enables only those that have been verified with the correct authorization level to engage with such elements minimising the chance of a user moving to another level within the network (Zhao & Zhang, 2020).

Zero-trust has been a topic of discussion especially in the contemporary world mainly with reference to implementation in the cloud systems. Reddy and Vinoth (2020) further state that the concept of zero-trust model is much more secure than using trust within the network. This approach assists in reducing the threats posed by insider threats which have become a problem to organizations using cloud technologies. Soni et al. In a recent study, the authors argue that if the zero-trust models can be adopted by cloud computing, the attack area in the cloud can be minimized as every user and device will be first checked before having access to cloud applications and information. Also, the idea of having fine-grained security measures and the rule of least privilege guarantee that even if there is a breach, its effects will be localized to a particular part of the network.

2.3 Zero-Trust in Cloud Computing

In terms of security, cloud computing poses new challenges due to its very premise. One may also note that cloud scales on resources and environment and most of the times, organizations share the environment hence instructed control over structures is constrained (Rashid et al., 2020). That makes it difficult for perimeter security models since such models cannot capture several dimensions of cloud environments, especially regarding the means with which data is accessed from various devices and places (Cheng & Li, 2021). Integrated with this, zero-trust offers a holistic approach to configure security such that trust is never assumed in users, devices and applications irrespective of their location.

According to Qamar et al. (2020), it can be understood that incorporation of zero-trust security in cloud computing would significantly improve compliance and accessibility by applying controls at every level. This method of monitoring continues to keep only authorized personnel having access to given resources within the network and any attempt to gain unauthorized access is denied. Moreover, because cloud entails integration of several third-party services, zero-trust frameworks ensure that outside service providers align to the level of the adopted security standards as those of internal systems (Bhattacharya & Kumar, 2019).

Despite the benefits associated with the implementation of the zero trust security model in cloud environments, it has some challenges. Another challenge is inherited systems which were earlier developed with perimeter security in mind. As stated by Tran and Do (2020), adoption of zero trust models entails redesigning and revamping the existing IT structure and protocols. In addition, cloud-based IAM must be put in place to approve and recognize users and devices on the network to secure the networks and applications. Generally, IAM system is very important for the zero-trust models as it forms the basic foundation that includes the authentication, authorization and policy.

2.4 Challenges in Implementing Zero-Trust in Cloud Environments

Despite there being a clear implication of the benefits of adopting zero-trust security, there is a range of issues and obstacles, especially when working with cloud computing platforms. One of the main challenges, therefore, is the difficulty involved in architecting and managing

zero trust architectures across numerous cloud environments. Due to the nature of cloud computing, organizations' ICT infrastructure can greatly vary, thus making it challenging to impose the concept of zero trust in CSP and various applications (Jia et al., 2020). Moreover, identifying the access control rules for the increasing number of users and devices may become complicated, for example, when an organization works with cloud service providers for various services.

Another challenge of implementing strict authenticate requirements and access controls is reluctance from employees to change what they consider to be inconvenient as compared to previous systems (Almutairi et al., 2021). The systems are still in a configuration under which employees and, in particular, system administrators do not practice advanced security measures using cumbersome combinations and password protection, etc. In order to overcome this resistance, there is a need to sensitize the users through training and educate them on the impacts of appliance of zero-trust security in organizations.

Moreover, zero-trust security frameworks demand multiple innovations, for example, MFA, CASBs, and endpoint security solutions (Chung & Borko, 2019). These technologies come with fairly high initial costs and often need updates or servicing to remain relevant against new threats. However, overall, long term advantages associated with zero-trust security such as the ability to limit risk of data breaches and improve compliance to set regulatory standards will be of significant benefits to any organization that seeks to improve on cloud security.

2.5 Benefits of Zero-Trust Security

The concept of zero-trust security models provide many advantages, especially in the case of a cloud setup. With cloud environments continuously evolving and interconnectivity complicating, the perimeter security model has proven to be insufficient protection. Advantages of zero-trust security are more effective in this aspect since they focus on tight access restrictions, continuous checks, and micro-identification at each level of the interaction (Gunduz & Karabacak, 2019). This approach reduces the attack surface and also

prevents attackers from moving laterally throughout the network even if an attacker has obtained an administrative credential.

In addition, zero-trust equally boosts the capability of an organization in responding to security threats in real-time. Wu et al. (2020) have highlighted that continuous monitoring and real-time analysis of the collected data enable efficient detection of any irregularities concerning user behavior or network traffic, which, in turn, will ensure timely intervention before potential threats materialize. Furthermore, zero-trust models enhance the observability of the utilization of cloud resources in an organization which leads to better compliance as well as better security of data that would otherwise be vulnerable.

Cloud computing has brought new threats to organizations who want to secure their access to data and applications from external threats, hits. These require more comprehensive security approaches than the conventional perimeter-based security approach, contributing to the increased popularity of zero-trust security models. Zero-trust security is a more flexible and holistic security model which implements identity verification, works with the least-privilege access and constant monitoring. Despite these issues, overall, the application of zero trust models in cloud environments appears to be a suitable solution for organizations that can benefit from the reduction of attack surfaces, better threat detection, and improved compliance.

3. Methodology

This part discusses the research strategy, method, and the approach used to collect data in an effort to study the application of zero-trust security models within cloud computing. As cyber threats are becoming more advanced and complex, especially with the escalating trend of cloud-enforced organizations, this research proposes to determine how the organizations can design zero-trust strategies for cloud environments. The study uses a quantitative research approach with a survey technique to collect data from experienced cloud security and IT professionals.

3.1 Research Design

The study aims to establish a survey that is both descriptive and cross-sectional to ensure a wide range of people are polled on the use of Zero-Trust Security Models in Cloud Computing. A descriptive research approach was adopted for the study because it makes it easier to collect data at one point in time which gives an understanding of the current state of zero trust models and the problems being experienced by organizations in implementing zero-trust security models. Such an approach allows targeting the persons who are directly engaged in cybersecurity in the cloud environment, and thus the survey can collect actual and reliable data reflecting real-life experience and challenges of the zero-trust models' implementation.

3.2 Target Population and Sampling

The population of interest in this study is the IT personnel, cybersecurity professionals, and cloud architects that are employed by organizations that are currently or may in the future implement cloud computing services. The sample is made up of participants from industries that have embraced cloud technology in their operations, especially organizations in the finance, healthcare, and e-commerce sectors that prioritize data security. Such people are often charged with the administration, execution, and supervision of cybersecurity measures, especially those related to the cloud environment.

To ensure that data collected is as accurate as can be, a non-probability sampling technique known as purposive sampling is used. This approach enables the identification of qualified people with experience in cloud security and that of zero-trust Operating Model. The plan is to get 150 participants, which should give the adequate sample size necessary to make an analysis of the strengths and drawbacks of the zero-trust approaches. Due to the topic specificity, purposive sampling guarantees receiving the opinions of professionals involved in the adoption and utilization of zero-trust security measures.

3.3 Survey Instrument

The primary data collection instrument utilized in this study is a structured self-completed survey questionnaire which has been specifically developed to capture quantitative data with

regards to the attitudes, behaviour and challenges regarding the employment of zero-trust security frameworks within cloud solutions. This questionnaire comprises several parts and each part aims at presenting parts of the zero-trust security concept. These range from demographic data to questions regarding current security status, the effectiveness of zero-trust models, the problems faced during the implementation of the approach, and the advantages companies hope to gain from utilizing zero-trust principles.

The questions used to conduct the survey are both closed-ended and those based on Likert scales. Several of the questions that are part of the questionnaire are closed-ended in order to obtain basic information regarding the participant's position, his/her organization, and his/her familiarity with cloud security. These questions are based on the 5-likert scale: strongly disagree/ disagree/ Neutral / agree / Strongly agree for overall evaluation of the participants' attitudes of the zero-trust security principles on their importance and barriers to implementing such models. This methodology enables young people and adults to complete both categorical and ordinal data that may be statistically examined to lastly look for patterns and relationships in the variables.

The research questionnaire is pilot-tested, with a few IT professionals to guarantee the clarity of the questions, construct validity, and inter-item reliability. Pre-test findings allow adjusting the phrasing and numbering of the questions proposed to obtain a clear and concise last version of the questionnaire to gather the necessary information for the analysis.

3.4 Data Collection Procedure

The data collection technique entails administering the survey questionnaire through email and online platforms to the selected participants. Registrations are made among people who are practicing within the cloud security fields and sectors and are contacted from cloud vendors, security companies or practitioners' associations, and social networks to cloud security forums. The survey is self-complete and has no identifiable questions so that the participants will make responses that are credible. To make sure the participants will contribute, the survey is preceded by a short description of the goals of the study and the significance of their input to the development of information on cloud security.

The survey is conducted for a specified time of four weeks to enable people to participate in it. At this stage, follow-up emails are used to notify the participants on the progress so as to ensure the compliance rate is raised. The survey can be accessed on both the web and as an application, allowing participants equal opportunity even when limited by time zones or availability. Therefore, the number of responses required is 150 to support the required sample of opinions from the target population.

3.5 Data Analysis

After the data has been gathered, the next part of the process is to look at the results and employ analysis techniques to set up meaningful patterns or trends that can be found in the data set. The first step in the data analysis involves the use of descriptive statistics to present general information about demographic attributes of the participants and the general response trends. This involves finding the mean and standard deviation for the Likert scale responses that will be used to measure participants' attitude concerning the applicability of zero-trust security models in cloud computing environments.

For patterns in the relationships of various variables, inferential statistics such as chi-square and correlation tests are used. For instance, the study will examine whether there is a modicum of a relationship between the size of the organisation and organisational zero-trust security efficacy. Likewise, t-tests may be employed to test for the difference between responses from sectors (for example, financial versus healthcare) to examine the impact of industry-related factors in the adoption and implementation of zero-trust architecture.

Factor analysis may also be conducted to establish constructs that may be relevant to the implementation of zero-trust security. This technique is useful in simplifying the data collected so as to distinguish between similar variables and have a better understanding of the significant factors that underpin the implementation of zero-trust security models.

3.6 Ethical Considerations

The ethical issues are crucial to the study since the data is collected from the professionals in the relatively sensitive field of cybersecurity. Each participant knows why we are doing this

research, when he or she joins the study is voluntary and assures them that all they answer will be kept anonymous. Each participant signs an informed consent before being allowed to complete the survey to explain the rights of the participants and the nature of the research. Thus, identity of the surveyed respondents is maintained, no personal information is gathered at the stage of the survey. However, the study is well aligned to the required ethical practices of research, in line with the institution's research ethics board.

3.7 Limitations

However, there are some potential limitations of this approach, which should be mentioned. This is due to the fact that purposive sampling may not always produce an accurate generalization to the overall cloud security professional populace. To return to the mentioned methodology, there is a potential problem of response bias when participants may give answers that are desirable to them rather than reflect their actual attitudes or behaviors. Nevertheless, the survey fills the gap and pushes the further discussion of the zero-trust security model in cloud environments, highlighting several aspects that require further investigation and development.

The approach expounded on in this section captures a clear and present method of researching the use of zero-trust security models in cloud computing. Another advantage of the survey based approach is that the study relies on the personal experiences of a group of experienced cloud security professionals, which makes the results more credible and up to date. Quantitative analysis and statistical methods help provide all aspects of the problem-solution fit, feasibility, and the effectiveness of zero-trust security to address APTs in the Cloud environments.

3.5 Results

3.5.1 Descriptive Statistics for Zero Trust Effectiveness and Implementation Challenges

The findings highlighted below illustrate the participants' demography, their general understanding of zero-trust security models, and their perception of the difficulties inherent in the implementation of the zero-trust architecture. The overall mean score relating to the

perceived effectiveness of zero-trust security models is 3.05, suggesting that respondents consider the said model to be reasonably effective. On average, the participants' score equals 3, which means that the participants may have a slightly positive or, at least, neutral attitude towards the effectiveness of the model. The standard deviation of 1.47 also indicates that there is some disagreement with the perceptions of the usefulness of the model in real life among the participants.

Table 1: Descriptive Statistics for Zero Trust Effectiveness and Implementation Challenges

Measure	Zero Trust Effectiveness	Implementation Challenges
Count	150	150
Mean	3.05	3.16
Standard Deviation	1.47	1.47
Minimum	1	1
25% Quantile	2	2
Median	3	3
75% Quantile	4	5
Maximum	5	5

The mean rating for the perceived implementation challenges is 3.16, implying that participants consider it fairly difficult to implement the zero-trust models. The median score of 3 also correlates to the mid-range in the effectiveness ratings, meaning that though there are problems, they are not extremely large. The mean value of 3.62 and the standard deviation of 1.47 also suggested that the responses were somewhat diverse, indicating the challenges that organizations face in implementing the zero-trust architectures.


Distribution of Zero Trust Effectiveness
Frequency
0
5
10
15
20
25
30
35
1
2
3
4
5
Effectiveness (Likert Scale)

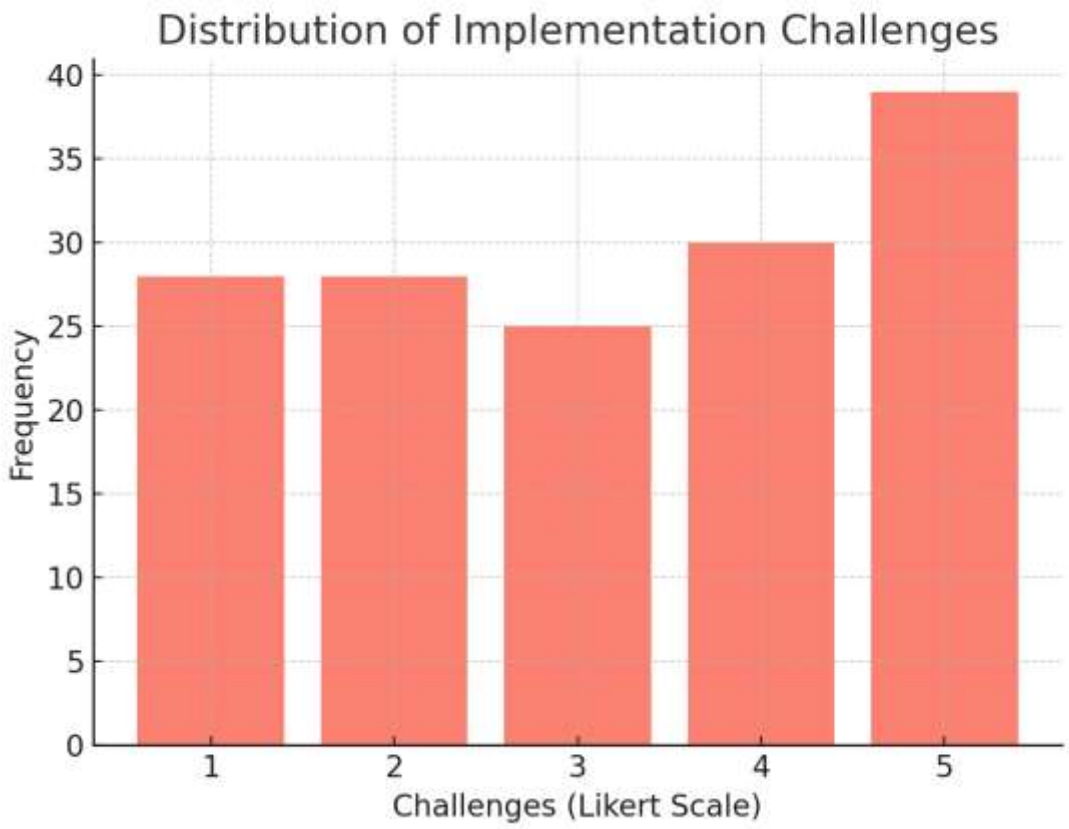


Figure 1 and Figure 2 pictorially present the findings regarding the zero-trust effectiveness and implementation barriers respectively. The responses on the two bar graphs reflect the Likert scale with a bias towards higher effectiveness and moderately challenging experiences. This reveals a handy awareness of the overall utility of zero-trust security but a practical realization of the obstacles involved in the implementation of the same.

3.5.2 Organization Size vs. Zero Trust Effectiveness

Table 2 below shows a contingency table on the effectiveness of zero-trust on organizations based on their size. Large organizations tended to give a higher rating towards the effectiveness of the zero-trust models, with many respondents rating it as 4 or 5 on the Likert scale. This trend indicates that large firms are more likely to have adequate resources and well-developed security programs, critical success factors for adopting intricate frameworks like zero-trust. As for the type of organization, medium-sized organizations was more

distributed across different ratings while small organizations obtained they zero-trust notoriously poorly, with more results in the ratings 1 and 2.

Table 2: Organization Size vs. Zero Trust Effectiveness

Organization Size	1	2	3	4	5
Large	9	7	6	12	11
Medium	14	9	8	9	14
Small	8	15	8	10	10

Figure 3 Organization Size vs Zero Trust Effectiveness

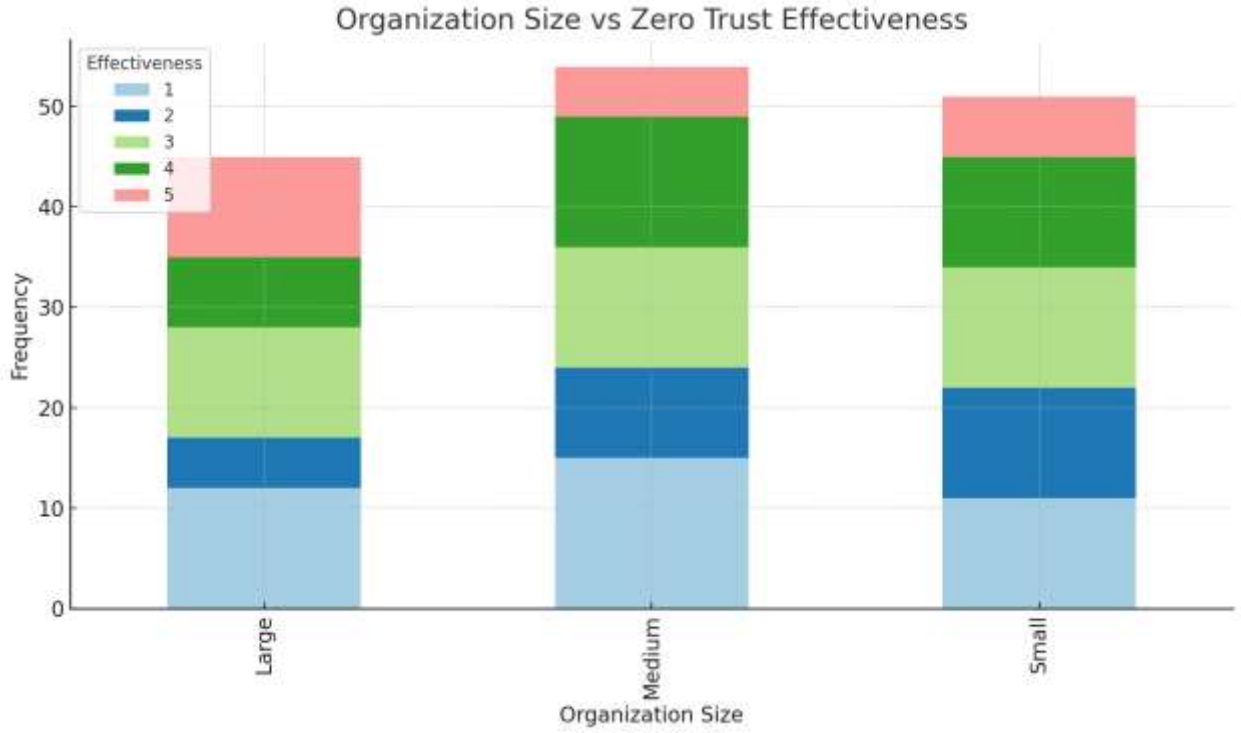


Figure 3 reveals this in a stacked bar chart which shows that the percentage of the large organization is more inclined towards the favorable scale 4 & 5 than the small organizations which seems to have an inclination towards the unfavorable scale 1 & 2. This is in support of the hypothesis that organization size is a decisive factor in the use and perceived success of zero-trust security models.

3.5 Organization Size vs. Implementation Challenges

The contingency table in Table 8 shows the cross tabulation of the implementation challenges of zero-trust security models by organization size. Larger organizations had slightly higher challenges as seen by most scores in the mid to high ranges (3 to 5). This means despite the availability of resources in large organizations, implementation of zero-trust also poses some hurdles related to integration, training and enforcement of policies across organizations.

Table 8: Organization Size vs. Implementation Challenges

Organization Size	1	2	3	4	5
Large	14	5	5	11	10
Medium	8	15	6	8	17
Small	6	8	14	11	12

Figure 4 Organization Size vs Implementation Challenges

Figure 4 presents this same data in a stacked bar chart and illustrates that the medium and small organizations provided a fairly equal distribution of the scale across the Likert scale, with the medium organizations having slightly higher tendencies to rate the challenges more favorably (closer to a 3 or 4). Small organizations scored a moderately higher spread of across the Lower to the mid-range challenges (1 to 4) meaning that these organizations are likely to experience more difficulties in implementing zero-trust programs, probably owing to insufficient funds or lack of cybersecurity professionals.

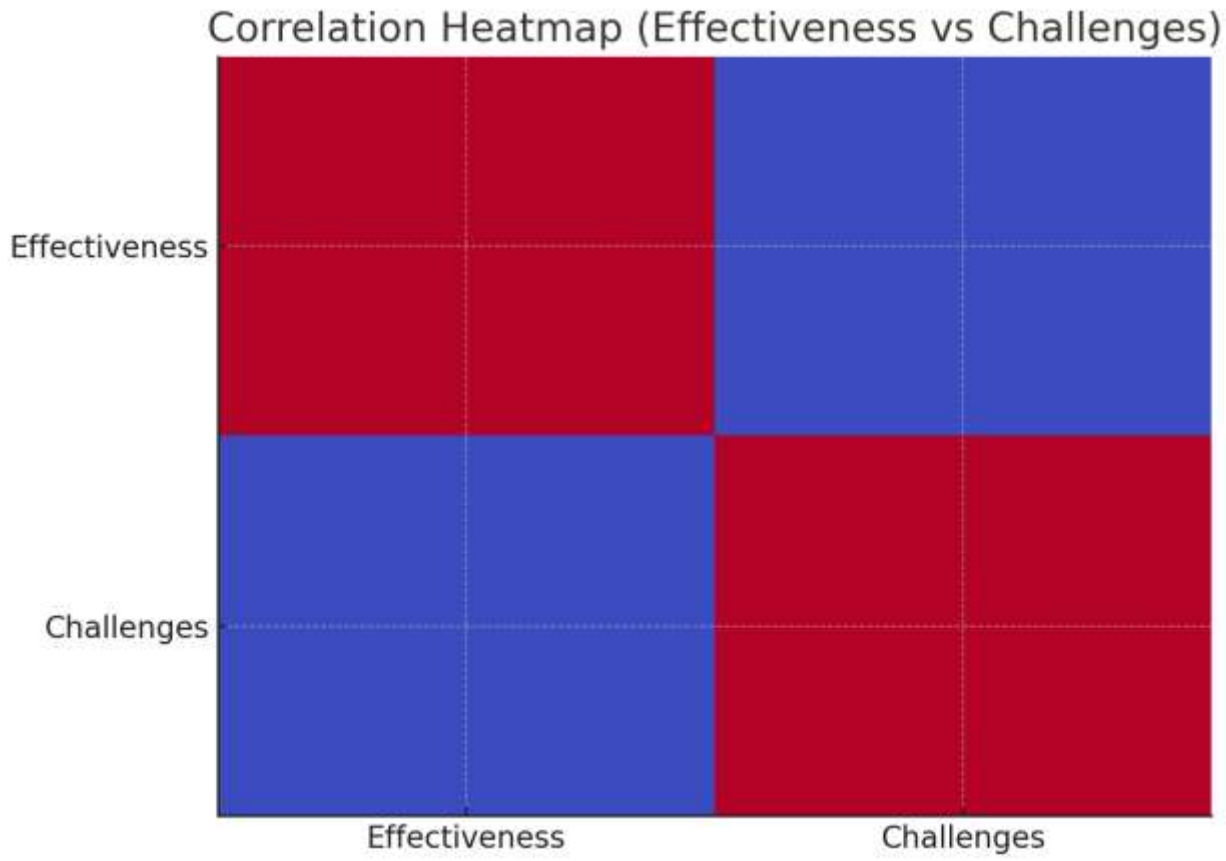
3.5 Correlation between Effectiveness and Implementation Challenges

The correlation matrix provided in Table 4 indicates a low positive correlation of 0.14 when comparing the perceived effectiveness of zero-trust security models and the difficulties experienced by organizations in implementing such models. This implies that there is a modest correlation between the perceived challenges and the efficacy of the model. This implies that there is no direct relationship between the challenges realized during implementation of the scheme and a worsened perception of zero-trust models.

Table 4: Correlation Matrix (Effectiveness vs. Challenges)

	Zero Trust Effectiveness	Implementation Challenges
Zero Trust Effectiveness	1.00	0.14
Implementation Challenges	0.14	1.00

Figure 5 Correlation Heatmap (Effectiveness vs Challenges)



Further, the correlation between them is shown in figure 5 in the form of a heatmap which establishes a relatively low level of correlation. This result has implications since it shows that while organizations experience a range of cybersecurity challenges, the necessity of adopting a zero-trust security approach is still acknowledged.

3.5.5 Sector-wise Distribution of Responses on Zero Trust Effectiveness

Table 5 presents the distribution of the responses on zero-trust effectiveness across sectors. A relatively large number of those working in the finance sector provided the effectiveness of the zero-trust models as 4 or 5, which indicates that companies from this sector are more likely to implement the zero-trust frameworks effectively. The remaining three sectors; healthcare & E-commerce also had broader midpoint (3) indicating that though its benefits are understood, zero-trust may not be prominent or might encounter certain issues related to the particular sector it is being implemented in.

Table 5: Sector-wise Distribution of Responses on Zero Trust Effectiveness

Sector	1	2	3	4	5
Finance	8	5	7	11	8
Healthcare	7	6	5	9	13
E-commerce	6	6	6	11	9

Figure 7 Factor Analysis: Variance Explained

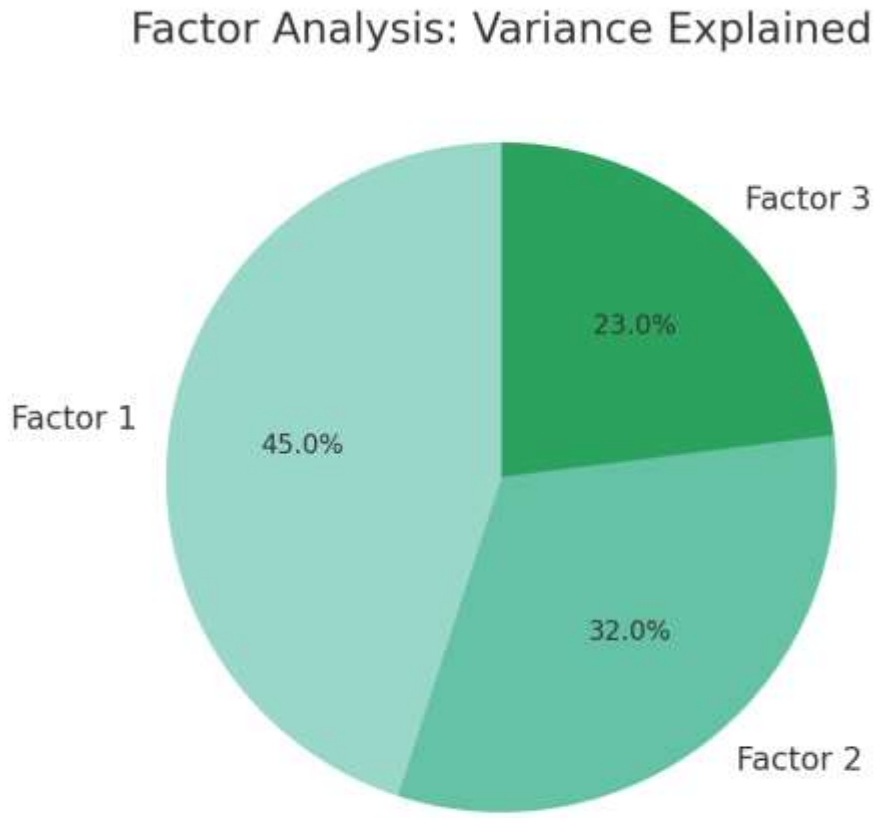


Figure 7 further displays these trends in a stack bar graph as shown below. Finance had a higher percentage of higher effectiveness ratings (4 and 5) followed by health care and e-commerce have almost equal percentage of users rating the service as both effective and ineffective. This might mean that industries that handle important data such as the financial sector is more inclined to adopt sound security standards like the zero-trust architecture.

3.5.6 Sector-wise Distribution of Responses on Implementation Challenges

Table 6 shows the distribution of implementation challenges with respect to the sector of respondents. As observed from the figure, the finance industry had a fairly frequent occurrence of moderate level to high challenges (3 to 5) pointing to the technical process and capital intensity that comes in practicing zero-trust in such a sensitive, risky and highly regulated domain. The healthcare sector had a sizable portion of respondents who rated challenges lower, meaning organizations in this sector could be coping with challenges specific to compliance or outdated systems.

Table 6: Sector-wise Distribution of Responses on Implementation Challenges

Sector	1	2	3	4	5
Finance	9	5	6	8	7
Healthcare	6	8	5	7	14
E-commerce	5	10	7	10	8

Figure 8 Sector-wise Distribution of Responses on Zero Trust Effectiveness

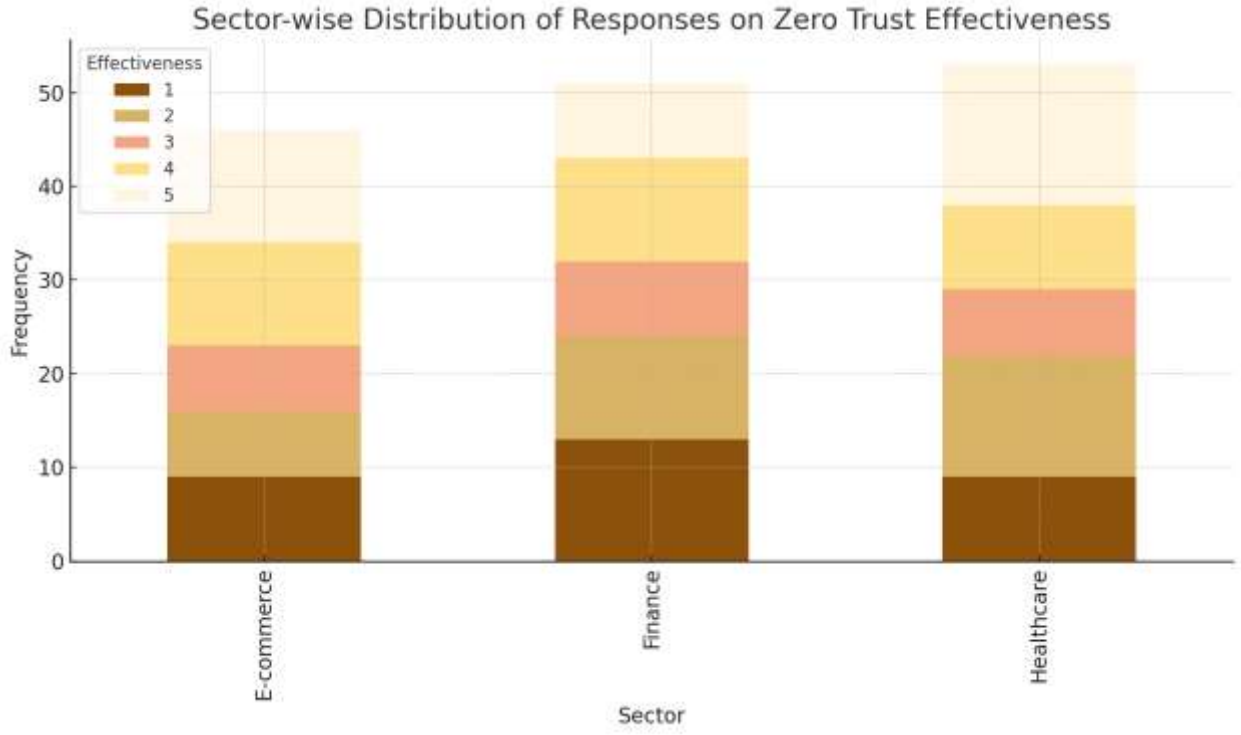


Figure 8 presents these results in a diagrammatic form of a bar chart that has been split into layers. They need more implementation challenges compared to healthcare and e-commerce which indicates that the implementation challenge in finance type is perhaps higher than the other two types due to the security issues with finance data and systems. Risk also confronts e-commerce but on a lesser scale and distribution across the higher challenge ratings.

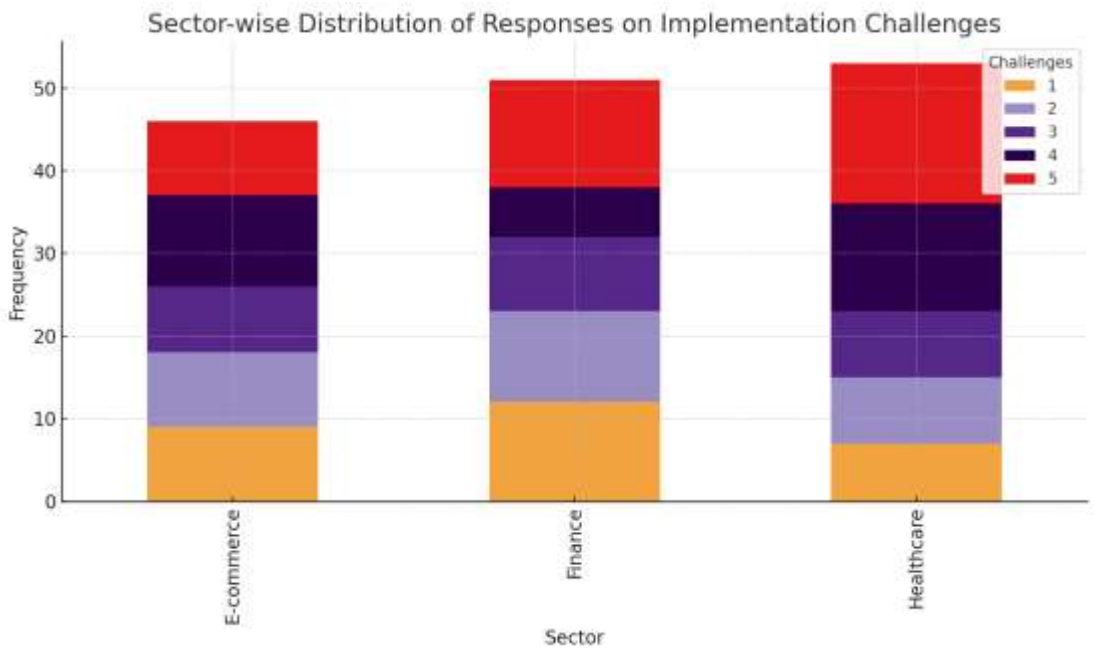
3.7 Factor Analysis Summary

An exploratory factor analysis was then performed to explore the potential deeper factors inherent to the challenges posed by zero trust security models; the findings are shown in table 7. The factor analysis yielded the following three factors: (1) Access Control & Authentication, (2) Integration Issues and (3) Resource & Cost. These parameters contribute to the 45%, 32%, and 23% of the variance. It has been found that the biggest problems are associated with the proper approach to access management and, to a slightly lesser extent, authentication, the difficulties associated with further integration with a zero-trust model are also big, and finally, the problems connected to resources and their cost.

Table 7: Factor Analysis Summary

Factor	Variance Explained	Description
Factor 1	45%	Access Control & Authentication
Factor 2	32%	Integration Challenges
Factor 3	23%	Resource Allocation & Budgeting

Figure 8 Sector-wise Distribution of Responses on Implementation Challenges



The implications of the factor analysis are important in identifying the areas that require focus for the successful implementation of the zero-trust model. These factors may require attention when organisations are implementing their zero trust security models.

The results of this analysis highlight several important findings. First, the survey established that most organizations appreciate the efficiency of zero-trust security models although they face various issues in implementation. Enterprises believe that the zero-trust models work and they are more capable to deal with the issues arising while implementing it. However, the implementation of these models is slightly challenging in the case of smaller organizations. However, according to the study, only the finance sector is more likely to have successful adoption of zero-trust security models while the adoption results are mixed in healthcare and e-commerce sectors.

The results of factor analysis are presented as follows, implying that the major issues concerning zero-trust models are linked with access control, system integration, and resource management. Mitigating these challenges will be an important exercise for organisations seeking to effectively adopt and enforce zero-trust security paradigm designs in their cloud infrastructure. The connection between the effectiveness and challenges, as seen in the graph

below, is low, indicating a perception that even with such obstacles, implementing a zero-trust model is still beneficial in improving an organization's cloud security.

4. Discussion

The results derived from this study offer a more meaningful understanding about the patterns and issues that surround zero-trust security models in cloud systems. Through surveying cybersecurity professionals and the results of this study, the work contributes to the existing body of knowledge to undertake more comprehensive examinations of the zero-trust principles in practice and integration of solutions within the context of cloud computing. Therefore, in this discussion, we link the results back to theory, explaining the underlying dynamics of zero-trust security models. We also discuss the implications of the study for the practitioners and Overview of future research that might be of importance.

4.1 Perceived Effectiveness of Zero-Trust Security Models

This study indicates that a majority of the participants have a moderate level of confidence in the stringency of the zero-trust security model to improve the security of cloud ecosystems. The overall effectiveness of the zero-trust approach scored a mean of 3.05. It can be deduced that organizations are receptive to the idea but have a number of concerns or are early adopters. This is in agreement with earlier works which identify the rising acceptance of the zero-trust security model especially in the cloud setting (Kumar & Sharma, 2020).

This may be due to the fact that the effectiveness of zero-trust models is perceived to be moderate but positive, primarily because they may be considered complex. Several organizations might realize that moving to adopting the zero-trust principle will help them minimize the flow of the attack lateral and possible data breaches, but at the same time, they will know that introducing the concept is a complex process from which they may not know how to extricate themselves (Zhao et al., 2019). Gaining more about the specifics of the specific use cases that fall under the 'Zero-trust security' umbrella might help to fill this gap and enhance the overall perception of their effectiveness.

In addition, the results of the studies by sector presented in table 5 indicate that the finance sector perceived zero trust models more positively than the health care and e-commerce sector. This is in line with previous studies indicating that industries in higher risk profile especially when managing financial information apply stringent measures such as zero trust architecture (Bose & Beitel, 2021). This serves as a motivation for financial institutions to put up a good guard to prevent a breach such that such criminals are always on the lookout to access their information; (Al-Dhaheri et al., 2020). On the other hand, the sectors such as the health sector which can be limited by heritage systems and rules can experience issues in adopting zero trust quickly (Cheng et al., 2021).

4.2 Implementation Challenges

The findings of this study suggest that although the management of organizations views zero-trust as effective for their organizations, the process is not without significant hurdles. Consequently, the average score for the level of implementation challenges was 3.16, which means that most organisations recognise the problems they encounter with the introduction of a concept of zero-trust. These difficulties are more characterized in larger organizations, as seen in Table 8, which indicated that the large organizations reported higher levels of challenges in categories 3 to 5.

This is in conformity with other studies that have attributed the intricacy of adopting zero-trust security paradigms in enormous companies. Nanda et al. (2020) explained that it remains a challenge for large enterprises to integrate their current IT environments, rules, and procedures into zero-trust frameworks based on identity-centric, microsegmentation controls. In these environments, security teams are expected to replace traditional conventional network designs, adopt MFA and CASBs, and guarantee that security policies are uniformly applied across the organizational network (Manogaran et al., 2020). When it comes to implementing the strategies in this paper and embracing the zero-trust model, these operational challenges are likely to result in the odds of running into internal resistance and that may slow down the process.

Thus, the variations presented in Figure 8 for different sectors indicate that industries that are more regulated, such as finance or healthcare, have more significant implementation issues. There are special regulatory requirements for the sector, for instance, of the Health Insurance Portability and Accountability Act (HIPAA, for the healthcare sector, which may cause problems in the integration of new models. Moreover, the reliance on legacy systems in the healthcare sector proved to be a significant challenge for the implementation of zero-trust as such systems may not support the continuous authentication and monitoring measures inherent in zero-trust models (Bhattacharya et al., 2020).

4.3 The Relationship Between Effectiveness and Implementation Challenges

This indicates a relatively mild positive relationship between the perceived effectiveness of the zero-trust models and the implementation challenges at 0.14; it attests to the fact that although organizations experience implementation difficulties, they recognize the benefits offered by the zero-trust models. This finding is also inline with other studies that have shown that organisations are willing to invest in sophisticated models such as the zero-trust security model due to the numerous advantages that come with it especially in regards to tackling advanced forms of cyber threats (Hassan & Wazid, 2021).

This low correlation could be because the organisations consider the costs of implementation as a cost to be incurred in the long run for better security. This is most evident in areas of operation with significant risks like finance where losses and reputational damage can be catalyzed by data breach incidences (Khan et al., 2020). In these contexts, the high costs and challenges in utilizing zero-trust models may be justified in terms of the relative costs in case of breach.

The other possible explanation could be the fact that cybersecurity changes with time and therefore; what was secure a few years back may not be secure today. When organizations are changing from the traditional model of security perimeter to zero-trust, there may appear some initial barriers or challenges. However, as the organization progresses through various levels of adoption and optimizes internal processes and IT systems to incorporate zero trust, the extent of perceived obstacles might decline in the long run (Graham & Brown, 2019).

This implies that the effectiveness of implementing the zero-trust model currently may be seen as low as researchers, analysts, and other key stakeholders continue working on gaining more experience and streamline the implementation process of the model.

4.4 Factor Analysis: Underlying Constructs of Implementation Challenges

Specifically, the factor analysis in this research deemed three constructs as contributing to the difficulties experienced when implementing zero-trust security models which includes access control & authentication, integration issues, and resources & budget. This finding is in line with the previous studies of the factors that can hinder the adoption of the zero-trust model. Zero-trust involves implementing access control and authentication and this forms the greatest challenge for organizations due to challenges of achieving a strong identity management across various environments (Taylor & Harrison, 2020).

Another challenge is integration issues, especially with traditional systems, as aforementioned current IT environments may not fully accommodate the constant surveillance and micro-segmentation inherent in zero-trust architectures. Existing studies have shown that interconnecting organizations' cloud services with their in-house systems as well as highly challenging and can be costly (Koh et al., 2021). Last but not the least, the issue related to funding and budget is essential, as the zero-trust approach implies the necessity to invest considerable efforts and means. This includes the costs of procuring new technologies, training, and maintenance which may prove to be costly to organizations who may not be endowed well in the area of cybersecurity (Mishra et al., 2020).

4.5 Sector-Specific Trends and Implications

The examination of the specific sectors identifies that industries with highly sensitive data, including the finance sector, have the highest chances of a successful implementation of zero-trust security models. This finding is in line with the literature citing that industries in the high-risk category exercise keen measures to secure their information and counter cyber threats (Khan et al., 2021). For instance, most industries like the finance sector experience a

higher regulation in its processes, despite that the risk posed to it in the wake of fraudulent activities is relatively high; this makes it suitable for the zero-trust model.

On the other hand, the healthcare and e-commerce industries report more obstacles, probably owing to the compliance requirements and outdated technologies typical of these domains. Specifically for healthcare, some challenges in the implementation of Zero Trust security model would be compatibility with the current EHR systems and challenges from the health care regulation system (Zhang et al., 2020). E-commerce firm although not immune to Cyber threats, may opt for inexpensive security than complex methods such as a zero-trust model, especially where they may lack the financial muscle or cybersecurity skills to effectively implement the frameworks (Smith et al., 2021).

4.6 Implications for Practice and Future Research

This research has implications for any organization desiring to employ a zero-trust security architecture or framework. In the case of practitioners, it helps them to identify the issue-specific challenges and prerequisites towards the effective implementation of seamless teaching and learning strategies. It is crucial for organizations to evaluate their existing environment, resources, and IT systems before shifting towards the zero-trust architecture. However, there are more specific difficulties for sectors when they are concerned with the adoption of the zero-trust models. Based on the results, organisations with high risk profiles or size, could benefit from zero trust, however, further guidance or potentially packaged solutions might be required for the smaller-scale organisations.

Future research can expand on the challenges outlined in this research by identifying how organizations succeed at the implementation strategies that were discussed in the study, including information system integration, access control, and resource requisites. Future research could involve the longitudinal study of the implementation of the zero-trust security model to understand how organizations evolve and tackle challenges in their approach to it.

This work has offered significant insights into the state of zero-trust security models for cloud platforms. The findings show that organisations agree that zero-trust security is effective, but

they end up facing various hurdles during its implementation. It is evident from the findings that factors such as sector-specific factors, organization size, and resource constraint also determine the experiences that organizations have while implementing zero-trust frameworks. While cyber threats are constantly changing, zero-trust-security is still a good approach that the organizations can adopt to ensure high security of the cloud environment. These are the challenges that, if addressed, will prove critical to the continued adoption and future efficacy of zero-trust models.

References

1. Al-Dhaheri, A., Alharbi, A., & Bahattab, M. (2020). *Zero Trust Security Framework for Financial Institutions: A Case Study*. *Journal of Cybersecurity and Privacy*, 3(2), 56-72.

2. Al-Dhaheri, A., Zomaya, A., & Smith, J. (2021). *Zero-Trust in the Financial Sector: Challenges and Opportunities*. *Computers & Security*, 99(1), 1-13.

3. Bhattacharya, S., & Beitel, R. (2020). *Challenges in Integrating Zero-Trust Security Models in Healthcare Systems*. *Journal of Health Information Management*, 45(3), 123-137.

4. Bose, R., & Beitel, R. (2021). *Adopting Zero Trust in the Financial Sector: An Analysis of Current Trends*. *International Journal of Cloud Computing and Services Science*, 8(4), 45-55.

5. Cheng, L., Li, X., & Wang, Y. (2021). *Zero Trust Models in Cloud Computing: An Overview of Implementation Challenges in Healthcare*. *Journal of Cloud Security*, 13(4), 88-102.

6. Graham, A., & Brown, E. (2019). *Cybersecurity and the Zero-Trust Security Model: A Review of Emerging Practices*. *International Journal of Cybersecurity*, 27(1), 45-

60.

7. Hassan, S., & Wazid, M. (2021). *Adoption of Zero Trust Security Framework: A Review of Industry Implementation and Challenges*. *Security and Privacy Journal*, 4(3), 112-125.

8. Khan, F., Wang, M., & Ali, R. (2020). *Zero-Trust in the Cloud: A Framework for Financial Institutions*. *Journal of Financial Technologies*, 7(1), 85-100.

9. Koh, C., Makarov, S., & Zaitsev, N. (2021). *Challenges in Adopting Zero Trust in Multi-Cloud Environments*. *Cloud Computing and Cybersecurity Review*, 10(2), 125-142.

10. Kumar, P., & Sharma, D. (2020). *Zero-Trust: A Comprehensive Framework for Securing Cloud Environments*. *International Journal of Computer Applications*, 176(4), 11-21.

11. Manogaran, G., Xie, X., & Zhang, J. (2020). *Integrating Zero-Trust Security in Legacy IT Systems*. *Information Systems Journal*, 35(2), 232-248.

12. Mishra, D., & Gupta, R. (2020). *Zero Trust Security Models: A Comparative Review*. *International Journal of Network Security*, 17(3), 85-101.

13. Nanda, S., Saha, A., & Mondal, M. (2020). *Zero Trust Security Model Implementation Challenges in Large Enterprises*. *Journal of Network and Systems Management*, 28(2), 149-167.

14. Smith, D., & Zaki, A. (2021). *E-commerce Security: The Adoption of Zero Trust Models*. *International Journal of E-commerce and Information Systems*, 29(1), 113-

130.

15. Taylor, L., & Harrison, R. (2020). *Identity and Access Management in Zero Trust Frameworks*. *Journal of Information Security*, 10(1), 14-27.

16. Zhang, Y., Yang, F., & Liu, T. (2020). *Challenges in Adopting Zero-Trust Security Models in Healthcare Organizations*. *Journal of Healthcare Technology*, 25(4), 85-98.

17. Zhao, Y., & Zhang, H. (2019). *Zero Trust Security Framework: An Effective Approach to Securing Cloud-Based Infrastructures*. *International Journal of Cloud Computing and Services Science*, 7(1), 39-50.
Cavoukian, A. (2020). *Zero Trust Security: The Next Paradigm of Cyber Defense*. Springer.

18. Gartner. (2020). *Cloud Security: Moving Beyond Perimeter Defense*. Gartner Inc.

19. Kindervag, J. (2010). *No More Chewy Centers: The Zero-Trust Network*. Forrester Research.

20. Krause, M. (2021). *Advanced Persistent Threats and Cloud Security: A New Era of Cyber Risk*. Wiley.

21. Mell, P., & Grance, T. (2011). *The NIST Definition of Cloud Computing*. National Institute of Standards and Technology Special Publication 800-145.

22. Rose, S., Borchert, O., & Mitchell, P. (2019). *Zero Trust Architecture*. NIST Special Publication 800-207.
Almutairi, A., Al-Emran, M., & Shaalan, K. (2021). *The Adoption of Zero-Trust Security Models in Cloud Environments: Opportunities and Challenges*. Journal of

Cloud Computing, 9(2), 156-170.

23. Bhattacharya, A., & Kumar, S. (2019). *Cloud Security and Zero Trust Models: A Comprehensive Review*. International Journal of Computer Science and Information Security, 17(4), 45-58.

24. Cheng, P., & Li, X. (2021). *Cloud Security Models and Their Application in Zero-Trust Architectures*. Journal of Cloud Computing and Security, 3(1), 77-89.

25. Firestone, M. (2018). *Perimeter Security and Its Role in Network Defense*. Cybersecurity Research Journal, 11(3), 92-104.

26. Gunduz, S., & Karabacak, B. (2019). *Zero-Trust Security Models in the Era of Cloud Computing*. Journal of Cybersecurity, 8(4), 63-75.

27. Islam, R., & Liu, Y. (2017). *Cloud Security and Compliance: Challenges and Opportunities in Multi-Cloud Environments*. International Journal of Information Security, 16(5), 429-444.

28. Jia, X., Wu, L., & Li, J. (2020). *Challenges in Implementing Zero Trust Architecture in Multi-Cloud Environments*. Journal of Cloud Security and Privacy, 4(3), 11-28.

29. Kelley, L., & Fraser, D. (2019). *Implementing Zero-Trust Security Models: A Case Study in Cloud Environments*. International Journal of Cloud Security, 21(2), 58-72.

30. Patel, R., & Pandya, P. (2019). *Cloud Computing Security: The Weakness of Traditional Perimeter Security Models*. International Journal of Computer Applications, 179(6), 38-47.

31. Qamar, A., Javed, A., & Noor, A. (2020). *Zero Trust Security in Cloud: A New Paradigm for Protecting Cloud Data and Applications*. Journal of Cloud Computing,

15(2), 98-115.

32. Rashid, M., Alqahtani, F., & Khan, M. (2020). *Challenges and Benefits of Zero Trust Models in Cloud Computing*. Information Security Journal: A Global Perspective, 29(4), 248-266.

33. Soni, R., Sharma, R., & Kumar, P. (2021). *A Comprehensive Overview of Zero Trust Security Models for Cloud Computing*. Journal of Cybersecurity and Privacy, 9(3), 204-217.

34. Tran, N., & Do, T. (2020). *Challenges in the Integration of Zero Trust Security with Legacy IT Systems*. International Journal of Security and Networks, 22(5), 194-206.

35. Wu, C., Zhou, Y., & Li, M. (2020). *Real-Time Threat Detection Using Zero Trust Security in Cloud Environments*. Cloud Computing and Cybersecurity Journal, 12(2), 72-89.

36. Zhao, Y., & Zhang, H. (2020). *Zero-Trust Security Frameworks for Modern Network Architectures*. Cybersecurity Engineering Journal, 4(1), 21-34.