Security of Zero Trust Networks in Cloud Computing: A Comparative Review

Sarkar, Sirshak ; Choudhary, Gaurav; Shandilya, Shishir Kumar ; Hussain, Azath ; Kim, Hwankuk

Published in:
Sustainability

Link to article, DOI:
10.3390/su141811213

Publication date:
2022

Document Version
Publisher's PDF, also known as Version of record

sustainability

MDPI

Review

Security of Zero Trust Networks in Cloud Computing: A Comparative Review

Sirshak Sarkar [1], Gaurav Choudhary [2], Shishir Kumar Shandilya [1], Azath Hussain [1] and Hwankuk Kim [3,*]

[1] School of Computing Science and Engineering, VIT Bhopal University, Bhopal 466114, Madhya Pradesh, India
[2] DTU Compute, Department of Applied Mathematics and Computer Science, Technical University of Denmark, 2800 Kongens Lyngby, Denmark
[3] Department of Information Security Engineering, Sangmyung University, Cheonan 31066, Korea
* Correspondence: rinyfeel@smu.ac.kr

Abstract: Recently, networks have shifted from traditional in-house servers to third-party-managed cloud platforms due to its cost-effectiveness and increased accessibility toward its management. However, the network remains reactive, with less accountability and oversight of its overall security. Several emerging technologies have restructured our approach to the security of cloud networks; one such approach is the zero-trust network architecture (ZTNA), where no entity is implicitly trusted in the network, regardless of its origin or scope of access. The network rewards trusted behaviour and proactively predicts threats based on its users' behaviour. The zero-trust network architecture is still at a nascent stage, and there are many frameworks and models to follow. The primary focus of this survey is to compare the novel requirement-specific features used by state-of-the-art research models for zero-trust cloud networks. In this manner, the features are categorized across nine parameters into three main types: zero-trust-based cloud network models, frameworks and proofs-of-concept. ZTNA, when wholly realized, enables network administrators to tackle critical issues such as how to inhibit internal and external cyber threats, enhance the visibility of the network, automate the calculation of trust for network entities and orchestrate security for users. The paper further focuses on domain-specific issues plaguing modern cloud computing networks, which leverage choosing and implementing features necessary for future networks and incorporate intelligent security orchestration, automation and response. The paper also discusses challenges associated with cloud platforms and requirements for migrating to zero-trust architecture. Finally, possible future research directions are discussed, wherein new technologies can be incorporated into the ZTA to build robust trust-based enterprise networks deployed in the cloud.

Keywords: zero trust; cloud security; zero-trust cloud networks; cloud computing; zero-trust models

Citation: Sarkar, S.; Choudhary, G.; Shandilya, S.K.; Hussain, A.; Kim, H. Security of Zero Trust Networks in Cloud Computing: A Comparative Review. *Sustainability* **2022**, *14*, 11213. https://doi.org/10.3390/su141811213

Academic Editor: Tin-Chih Toly Chen

Received: 8 August 2022
Accepted: 30 August 2022
Published: 7 September 2022

1. Introduction

In the modern era of distributed computing, there have been many advances in the adoption and implementation of networked security systems for cloud servers. Since 2010, the global cloud services industry has had a year-on-year increase which sums up-to a USD 370 billion valuation in 2020, posting a 380 percent growth in a decade. As a consequence of such breakneck adoption in 2022, over 60 percent of all corporate data is stored in the cloud. This increased by almost 30 percent in 2015 and has seen continual growth as firms rapidly migrate their resources and business applications into cloud environments with the hope of improving security, reliability and ease of business [1,2].

This dramatic expansion has caused issues with corporate and government networks hosted on cloud platforms, each deployed with a highly proprietary set of security mechanisms such as service-level agreements (SLA), identity management and access controls, intrusion detection systems (IDS) and application service management. It is quite evident that cloud service customers (CSC) deploy these services on their networks with their own

specifications, based on their past operational experiences and convenience. Some of the leading cloud network environments are Amazon Web Services, Microsoft Azure, IBM Cloud, VMware and Google Cloud [3,4].

However, these complex security systems have not stopped cloud platforms and networks from being exploited by ransomware groups, botnets and advanced persistent threats (APT), the main culprit being poor security practices and configuration and internal vulnerabilities [5,6]. Cloud networks can also be exploited by third-party applications which introduce unforeseen bugs and even zero-day vulnerabilities, giving attackers access to sensitive customer data. Additionally, unless organisations verify sources, third-party applications can come from anyone inside the network, including an APT. According to a study conducted by Palo Alto Network's Unit 42, approximately 96% of application containers in cloud infrastructure have known exploits and vulnerabilities [7,8].

The current threat landscape naturally leads us to believe that a trust-based authorisation mechanism is needed in a cloud network environment which monitors and assists different nodes of that network [9,10]. This network authority must also have the privilege of authorising users' access to services and distributing responsibilities based on the authenticity of their identity. The technology we have just described is called a zero-trust network model. The zero-trust network model is such that no entity inside such a network is explicitly trusted. For each individual action by that entity where it must make use of some mission critical data or service, the network management authority must first give clearance to that action. This can be set up with existing technologies such as IDS, real-time resource management, segmentation of resources and behaviour tracking, which provides visibility, granular control and access of endpoint devices to network security teams [11–13].

Unfortunately, there are many issues which organisations must handle before an environment is fully functional, such as issues with legacy hardware, lack of applications to manage endpoint devices and training employees to use complex virtualization software, etc. Moreover, the widespread use of cloud computing platforms has caused the boundaries of the network to collapse. When an institution deploys a hybrid cloud platform and stores business-critical data on-site and on the platform, it increases their threat surface area [14,15]. Thankfully, there are continual efforts by many government institutions and private companies, including cloud service providers (CSP), to streamline varying rules and guidelines into adaptable frameworks and models.

For example, The National Institute of Standards and Technology (NIST) released a special publication on Zero-Trust Architecture in 2020 [16]. On 26 January 2022, The Office of Management and Budget (OMB) released a federal strategy to move the U.S. Government toward a "zero trust" approach to cybersecurity; this was in line with Executive Order (EO) 14028, "Improving the Nation's Cybersecurity", which pushes U.S. agencies to adopt zero-trust cybersecurity principles and adjust their network architectures accordingly [17]. The memorandum by the OMB requires agencies to achieve specific zero-trust security goals by the end of Fiscal Year (FY) 2024. Many private firms have also developed and offer state-of-the-art zero-trust network security solutions such as VMware's NSX Advanced Threat Detection and Carbon Black Cloud, Google's BeyondCorp, Palo Alto Networks' Next Generation Firewall, Citrix's Workspace, Microsoft's Azure and 365 Security.

However, the adoption of such frameworks and technologies have been overlooked by smaller and medium-sized firms and institutions who do not have sufficient resources, time or the inclination to implement such a framework to their cloud ecosystem. It is thus important to engage in a survey of the current implementations of zero-trust-based cloud network models. The survey will compare the different methods and approaches to validate identity and authorise the use of critical services in trust-based cloud networks. Thus, the objective of our paper is to help firms, institutions and governments achieve Zero-Trust Maturity for their cloud networks.

1.1. Contributions of This Paper

1. This paper discusses the current trends in the adoption of cloud infrastructure to host networks, how cost-effectiveness has prompted organisations to switch to cloud infrastructure and the issues faced when using such services;
2. The paper introduces the origin of trust evaluation as a precursor of zero trust. It links the natural progression of different projects and precursor technologies for distributed networks into the zero-trust architecture model. It also lists the core motivations behind the model, why it was needed and details of the workings of mature state-of-the-art research categorically;
3. The paper discusses the many challenges to the security of cloud networks, such as the interoperability of different cloud architectures, flaws in perimeter-based network design, vulnerabilities in virtualisation and poor practices prevalent in the cloud industry regarding the access to and oversight of data;
4. The paper explains the concept of zero-trust architecture, enumerates the properties a network must have to be based on ZTA and compares it with traditional network security architecture, as well as the required attributes of the algorithm for calculating trust.
5. The paper also maps out the specific changes that a pre-existing cloud network can undertake to migrate to ZTA and briefly talks about some problems that might arise operating this complex network architecture;
6. The paper then provides a type-focused comparison of the related state-of-the-art-works, emphasising their features and categories such as ZTA-based network models, frameworks and proof-of-concept technologies;
7. Conclusively, the paper outlines ongoing research and future directions for including emerging as well as proven technologies to enhance the ZTA as a whole with some use cases

1.2. Outline of the Survey

The paper is structured as follows: Section 1 introduces the current scenario of cloud platform adoption and issues that cloud service providers face in relation to the challenges of traditional networks and states the recent advancements undertaken by academia and industry to remediate them. Section 2 elucidates the development of the ZTA, followed by a detailed discussion of related works on ZTA models, frameworks, surveys and road maps according to their types. Section 3 includes the taxonomy of challenges faced by cloud networks. Section 4 highlights how the migration of traditional networks can be executed to mitigate detrimental effects and the long-term consequences of migrating to a ZTA. Section 5 compares related works based on various features, and Section 6 concludes the paper. Section 7 consists of recommendations and future directions.

2. Comparison with Existing Survey Articles

There are many studies which survey the architectural and technical features of ZTA. Table 1 includes a summary of existing surveys about Zero Trust. Buck et al. [18] provided a survey which analysed papers written on ZTA using a search model which distinguished academic literature from grey literature, the latter being from non-academic, commercial or private sources. Alevizos et al. [19] covered the fusion of blockchain's immutability to use intrusion prevention and detection at network endpoints. He et al. [20] provide a study on the advantages and disadvantages of access control models and authentication protocols and compare popular evaluation methods for trust. This work about access control methods and authenticating protocols in a network is also the focus of Syed et al. [21]. They discuss the challenges to such an architecture and expand its scope towards software-defined perimeters and micro-segmentation. Pittman et al. [22] survey a novel idea, applying zero-trust tenets and principles to data objects instead of pathways that allow users to access data. They conclusively state that the calculation of trust in a dynamic system such as a network is both a classification problem and a regression problem.

Most surveys primarily focused on the development of the architecture and management of ZTA or specific derived topics such as micro-segmentation, software-defined perimeter and intrusion prevention systems. This paper provides a comparison of the properties of the network or distinct features which are commonly used. As zero-trust architecture is not a monolithic one: it employs many proven and emerging technologies; comparing these is essential to sorting out the best-fit features. Of the papers surveyed, many authors also state that ZTNs have not been able to replace existing approaches to network security.

Table 1. A comparison of existing surveys and reviews (discussed: ✓; never mentioned: x; partially mentioned: -). P1: Categorisation of types of works surveyed, P2: Comparison of Models based on novel features, P3: Comparison of works based on independent parameters, P4: Details about challenges to cloud networks, P5: Discussion on Zero-Trust Lifecycle (maturity model), P6: Specifies possible domains of future research.

Author(s)	Primary Contributions	P1	P2	P3	P4	P5	P6
Buck et al. [18]	Consolidation of works based on Zero Trust, analysis of knowledge gaps in industry and academia	✓	x	x	-	x	✓
Alevizos et al. [19]	Analysis of ZTA-based models, blockchain-based intrusion detection and prevention to augment end-point security	x	✓	x	-	x	✓
He et al. [20]	Analysis of core technologies mainly relied on in Zero Trust and comparison of pros and cons	✓	✓	✓	x	x	-
Syed et al. [21]	Discussion about access control and authentication in different scenarios and impact of ZT implementation	✓	-	✓	-	x	✓
Pittman et al. [22]	Application of Zero Trust tenets and principles to data objects instead of data access pathways	✓	x	x	-	x	x
This Paper	Categorization and comparison of novel features used in Zero Trust Models for Cloud Networks	✓	✓	✓	✓	✓	✓

3. Related Work

The idea of a continuous 'trust evaluation'-based computer network has been around for a long time, having been proposed and even designed by the U.S. Department of Defence (DoD) in association with the Defence Information Systems Agency (DISA). It was named Black Core. Black Core was a communication network architecture in which user data traversing a global IP (Internet Protocol) network was encrypted end-to-end at the IP layer [23]. It was an experiment to re-focus network security across distributed servers from the model of perimeter security to request-based security.

But the very first instance of the term 'Zero Trust' being used was in 2010 by John Kindervag, from Forrester Research. It described the objective of the zero-trust model as 'to look at everything from a data-centric perspective, we can design networks from the inside out and make them more efficient, more elegant, simpler, and more cost-effective' [24]. Shortly after, further papers were published describing proposed methods of continuous interactions between users and the network authorisation mechanism [25].

The cloud industry and academia have started to formally develop many zero-trust cloud network models [16,18,26]. It must be understood that the Zero-Trust Model is a collection of different technologies and methods implemented in a system, by which the trust of an entity is determined. Thus, there are three main types of implementations, which we shall consolidate and compare according to their type. They are, namely, frameworks

for the trust model, which can be used to develop and design use cases, practical zero-trust models and theoretical proof-of-concepts, which showcase individual cases of specific technologies that fall under the umbrella term of Zero Trust [27,28].

3.1. Models

Casimer et al. produced a model which used tokens included inside the first TCP (Transmission Control Protocol) packet to verify and validate user identity during packet authentication. This was used to show that their network model could prevent DDoS attacks, spoofing of identity and fingerprinting of the network by adversaries in different environments such as enterprise-class servers, cloud computing data centres and a campus-based network connecting different physical locations [23,29]. This approach of first packet authentication using tokens was further developed for geographically distributed higher education cloud networks [30].

Dayna et al. published a proposed zero-trust cloud data centre network. Their model used identity management along with automated threat response and packet-based authentication for establishing trust. The model then dynamically managed eight distinct network trust levels it had generated [31]. An incredibly unique approach to a lateral problem in the domain of privacy for location-based service users was put forward by Anwar et al. Location information such as history and overall regional proximity to certain 'business-specific' areas can give third-party information processors a huge insight. Their model distributes user location data into different servers according to a partitioning model based on multi-level policy. Third-party applications are granted access only to designated servers where the privacy of the user profile is also ensured, as these applications are not trustable. Zero-Trust identity management is used in a cloud environment to manage the access to systems containing sensitive data, using different trust levels [32].

Further use of Zero Trust can be seen in different domains. One such domain was a distributed volunteer cloud network, which, in practice, might be comparable to a blockchain volunteer network where nodes are awarded with higher trust. Abdullah et al. [33] proposed a client-server model to verify the trust of nodes participating as volunteer nodes in a zero-trust cloud network. The nodes are initially not trusted by the system. They proposed an adaptive behaviour-based system which assigns tasks to the most trusted nodes and manages their lifecycle. Nodes with low trust scores are added to a blocklist and given less essential or no tasks at all. This trust score is generated by their analysis of the entire lifecycle of the node, which includes its behaviour, efficiency and availability, among other factors [33].

3.2. Frameworks

Frameworks are also essential to building zero-trust networks in the cloud. They help cloud architects and network administrators design, setup and manage essential procedures for trust-based identity management. Many times, such frameworks outline stringent policy-based enforcement, such as in paper by Romans et al., where a policy enforcement framework called FURZE (Fuzzy Risk Framework for Zero Trust Networks) was created to address challenges in Zero-Trust Networks. The researchers outline specific language choices for the design of a risk-based access control framework, created using fuzzy logic and with an emphasis on continuity updates to the system. They also put forth some generic firewall policy language and rules which may help in creating specific firewall rules [34].

Other authors have leaned towards creating typologies and philosophies such as by Mehraj et al. The authors compiled a list of typologies and strategies related to zero-trust networks. One such strategy is the complete automation of trust calculation using a 'Trust Engine', which is an integrated system which controls the data, users and applications. The proposed system would then dynamically calculate the consolidated trust of a user, device or application by applying a trust score in a particular segment of the network.

The trust engine would work on a Zero-Trust triangle, much like the CIA Triad, the trio being application, user and device [35].

An enterprise-oriented Software-Defined Perimeter (SDP) Framework was proposed by Abdallah Moubayed et al., which adopted a zero-trust architecture by authenticating and verifying a host for every session using a client-gateway architecture. It could address lateral threats and internal pivoting attacks often found in such environments. Their performance analysis showed the potential as an alternative to VPNs for internal enterprise networks [36]. Ahmed and Petrova proposed a federated IAM framework using zero trust as a basis to stop CSP's from accessing virtual assets of their customers [37]. For zero-trust deployments in multi-cloud environments, a performance analysis was performed by Simone et al., which pointed to no negative effects [27].

3.3. Proof-of-Concepts

The much talked about eZTrust by Zirak Zaheer et al. provides a network-independent perimeter solution for micro-services. It focuses on contextual and granular control of workload identities by tracing them using the Berkeley Packet Filter. It also enables data centres to create and enforce access control policies based on the previously mentioned workload identity. The system can verify and trace authentic workload identities and tags to packets received [27]. A research project by Weever and Andreou highlighted the importance of securing data in-transit from one containerized application to another. It is during the transit that attacks can occur and data can be stolen. By securing the data, the authors were able to regulate the flow of traffic and find out the attack's origin [38].

4. Security Challenges to Cloud Computing Networks

This section discusses the internal security challenges that networks hosted on cloud platforms face. One such example is the inherent flaw of the model of the implicit trust of entities inside the network. Although this is not an exhaustive list of issues, the primary focus of this section is to highlight the core design flaws of modern cloud networks with traditional network security controls. Cyber threats such as malware, ransomware, data breaches and phishing attacks are influenced by external factors that have leeway to affect systems due to vulnerabilities arising from the issues discussed below. For example, vulnerabilities in virtualization constitute a significant aspect of the spread of ransomware from a host OS to its hypervisor and eventually to other host operating systems. Poor security controls and lack of oversight are pivotal problems that allow attackers to cause damage to the IT systems of CSCs and CSPs.

4.1. Architecture Interoperability Issues

There is no one type of conformal cloud computing architecture. Several different cloud computing models, types and services have emerged to serve evolving requirements of organisations and institutions. Currently, there are three types of cloud computing infrastructure:

(a) **Public Cloud Infrastructure** Cloud services where the hosting infrastructure and computing capabilities are available publicly. The CSP develops, operates and manages the service which is made available for public use, either free-of-cost or for a nominal fee. Google Cloud offers its services for free to Google users, such as Drive for hosting data, Classroom for educational management, Meet for video–audio calls, Gmail for email services and YouTube as a separate video platform ecosystem which is hosted on Google Cloud, etc. These types of cloud platforms are for general purpose use, with little or no option for customisable/modular features.

(b) **Private Cloud Infrastructure** Cloud services where the hosting infrastructure and computing capabilities are available to a limited user base. In this architecture, the resources are used by one firm or organisation. The servers which host the platform are physically located at an on-site data centre or they are hosted by a third-party CSP. The infrastructure is dedicated solely to one firm or a group of firms, and as

such, the services and applications hosted on the cloud platform are not available to entities outside the organisation. Microsoft's Azure has many such services which are available to customer organisations on a subscription basis. These services are also highly customised and modular in accordance to the customer's request. Leading examples are Microsoft Azure, Oracle Cloud and VMware.

(c) **Hybrid Cloud Infrastructure** Cloud services are hosted both on-site at the customer location and on a private or public cloud platform. This approach is way more scalable and modular; however, it is not more secure. The hybrid cloud environment usually includes a plethora of application suites and network software with micro-segmentation, where networks are segmented according to user groups, departments or physical locations such as offices or outlets. Hybrid Cloud deployments are scalable as resources, and parts of the network can be opened for routine use in a phased manner. Innovative technologies can also be integrated much faster than private-only cloud networks as they can be deployed on a certain segment of the network for testing and evaluation.

According to a survey conducted in 2019, of 786 cloud professionals at large and small enterprises across a multitude of industries, such as software, financial services, telecommunications, education, government and healthcare, 22% of CSC's were utilizing public-only cloud services, 3% were using private and 68% were using hybrid models of cloud infrastructure. This is clearly an issue since each firm has a specific standard operating procedure when a network anomaly is detected. Cloud professionals and network specialists must be trained each time a new component is brought online or joins the firm, increasing costs and time consumed due to training.

4.2. Network Design

The fundamental model of cloud security still makes use of a reactive model, that of perimeter security where the connections and flow of data originating internally are trusted more than that originating externally, and mission-critical components of the network are cordoned off using firewalls. This model often includes a DMZ or demilitarized zone where untrusted requests for services present inside the 'protected' are accepted or denied as per the security policy. However, some non-essential network components, such as an email server or a publicly available FTP server, as commonly found in academic institutions, are exposed for convenience. This introduces insecurity into the network. This is most often how network penetration occurs, by gaining entry into a non-privileged part of the network and pivoting towards administrated areas. The Perimeter Based Security Model of Cloud Network is shown in Figure 1.

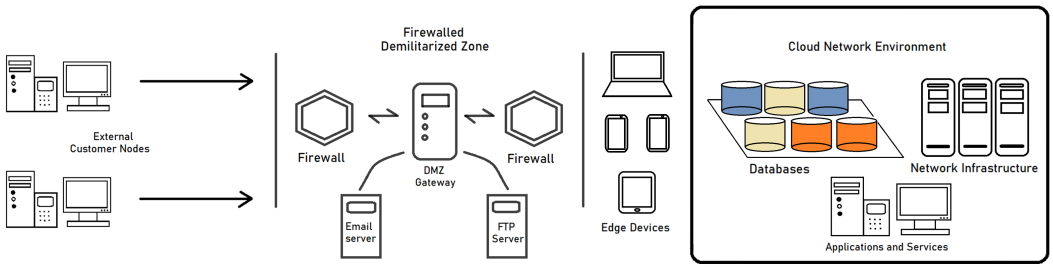

Figure 1. Perimeter Based Security Model of Cloud Network.

This is a reactive and static approach to networks where both physical and virtual services of the network are either secured or left insecure based on business requirements; however, this breaks down in modern cloud computing and ad-hoc endpoint device environments, where dynamic changes to the composition of the network and available resources make the DMZ irrelevant. Conventional networks verify the identity of users and the applications they use based on unique parameters such as MAC addresses, IP addresses, group policy and access privileges. However, these unique parameters can be

spoofed and changed at will by attackers with moderate network knowledge, as noted by an NIST report in 2013.

4.3. Vulnerabilities in Virtualisation

The use of virtualisation software to emulate the hardware stack has allowed CSPs to create and offer complex cloud platforms, complete with operating systems, applications and code running natively inside virtual machines. This use of multiple operating systems and applications with the same type or types of hardware that CSPs use has enabled feature creep and thus introduced vulnerabilities associated with such software and hardware.

Virtual machines (VM) use a software system called a hypervisor. which is often called the Virtual Machine Monitor (VMM). The sole purpose of the VMM is to manage and assign resources such as virtualised OSs (Operating Systems) to users. The hypervisor is responsible for creating, stopping, and modifying the VMs. It is evident that such a software system which is responsible for the management of many VMs, will most definitely have vulnerabilities. According to Guodong Zhu et al., there are three main types of virtualisation errors which give rise to vulnerabilities, hardware logic errors, device state management errors and resource availability errors. The most common being the first hardware logic errors [39]. The authors state that the implementation of VMs works differently than their physical counterparts. Such slight erroneous differences cause technical issues which are worked around for operational continuity. It is at this time that the vulnerabilities are introduced due to oversights in the logic. Moreover, the hypervisor may have distinct levels of control for a server farm. Cloud customer often use a variety of services, such as the cloud infrastructure (IaaS), cloud developer platform (PaaS) or just the application software hosted by the CSP (SaaS).

A second issue being during migration or backup of VMs, device state errors can occur. Every time a VM is started, it does so by remembering its previous backup state in a specific configuration. This is essential for repeated use of the same VM by different users, who have different tasks. Bad handling of the VM either by CSCs or the hypervisor can lead to corruption of guest the OS (Operating System) and possibly the entire VM stack. Such errors can be minute and trivial to the guest OS during operation; however, on boot-up, a few corrupted CPU register values or logical errors of the OS kernel can cause catastrophic damage to the VM hardware stack, which further corrupts other guest operating systems.

The final issue being resource availability errors, it becomes relevant as the scale and complexity of the cloud providers available VM resource pool increases. Errors may be introduced into the VMM implementation when managing a large data centre with multiple types of hardware stacks, this combined with ad-hoc use of resources by VMs, and their guest OS can lead to lack of available resources.

As stated by Guodong Zhu et al., a virtualised OS cannot differentiate between virtual and physical hardware. The authors also state that physical isolation of such VMMs is essential to alleviate this issue. Other essential work has also been performed by Gábor Pék et al. where the different hardware virtualisation vulnerabilities are classified according to their source, attack strategies and adversary models, as well as structure of attack vectors [40].

4.4. Poor Security Practices and Insider Threats

There exists a huge gap in the quality and quantity of a cloud security workforce, especially that of Security Operation Centers (SOC) in-charge of cloud networks. The overall challenges that SOCs are struggling with are real-time visibility of the infrastructure they protect, compliance by CSCs and design of security policies that remain enforceable across architectures, on-site and off-site [41]. Another alarming trend for cloud networks is insider threats, an insider threat is a possible threat to the network by an individual with heightened privileges and access. Most often insider threats are accidental and not purposely done. This issue arises due to lack of transparency by CSPs. To a potential customer firm, the pipeline of procedures that a CSP employee can use to access and exploit

customer data is not visible. CSPs do not give adequate information to their users, about the scope and scale of information available to its own employees. This is security through obscurity, which is flawed. An insider or a CSP employee can focus on a specific part of the cloud platform and may have any reasons to exploit the system ranging personal financial incentive to sociopathic behaviour. There are also no concrete methods to precisely predict such an attack, the attacker can plan in advance and even make use of the cloud platform to schedule the exploitation [42]. The main reason cloud networks attract such attention from adversaries internal and external is due to the varied nature of the data stored in these systems. A meagre 16 percent of firms using cloud platform to host their business networks say that current security tools and technologies are sufficient [41]. It is thus imperative that further research be conducted based on a human-centric approach, to effectively combat insider threats and poor security practices in cloud networks.

5. Concepts of Zero-Trust Architecture

The traditional security model is the perimeter (boundary) security model with the concept "Trust but verify". This concept has been operated that trusts internal users who have passed the security functions in the system or network but is wary of external attacks. However, the Zero-Trust model does not have a 'trust zone' and is based on verifying without trust even if it is an internal user. While the perimeter security model focuses on blocking, the zero-trust model focuses on thorough and continuous verification rather than blocking. The comparison between traditional security model and zero-trust model is presented in Table 2.

Table 2. The comparison between traditional security model and zero-trust model.

Features	Traditional Security Model	Zero-Trust Model
Approach	Trust but verify	Trust nothing and verify everything
Trust Boundary	External (Non-trust), Internal (Trust)	Micro Segmentation
Access Control	IP (Port, Protocol) based access control	Data-centric access control
Communication Encryption	External (Encryption)/Internal (No Encryption)	Full traffic encryption
Authentication	Once verification at initial access	Before access and continuous verification
Security Policy	Pre-defined rules and common policies	Fine-grained rules and adaptive policies (Needs Security Assessment)
Security Managements	Individual Monitoring and visibility	Visibility, automation orchestration of behaviour, devices, services and security

The Zero-Trust Architecture (ZTA) can quite simply be described as a set of coordinated system design principles based on the core concept that threats to a computer network or integrated networks can originate both internally and externally. This proposed network system design concept requires near-continuous verification and analysis of network nodes, services, applications and groups of users. This is simply because the network does not implicitly trust any entity. Only after the process of verification and subject to a decreasing time interval can elements of the network be entrusted to access, utilize and even modify network resources such as databases, other network nodes, servers present on the network and network policies. Once the pre-established time interval expires, the node must go through the verification process again.

It is important to note that even authorised nodes are given least-privilege access, which means access to only necessary components, 'no more no less' than what is required. To employ such a system, the network must have the following properties:

- Automation of system security;
- Dynamic access control policies based on risk management;
- Internal and external network traffic monitoring;
- Behaviour analysis for network nodes;
- Complete infrastructure visibility;
- Focus on protection of mission critical assets ensuring business continuity.

5.1. Leverage Zero-Trust Design Concepts

Each following subsection of this section is supposed to represent the stages in achieving Zero-Trust Maturity. The following points are meant to represent the stages of Zero-Trust Maturity:

1. **Define Architecture Priorities**—Derive your priorities from organization-specific mission requirements. The design team must identify the critical assets, services and data (ASD).
2. **Design the network architecture from the inside out**—Primarily, the focus should be on protecting the ASD; after this has been achieved, list and harden methods of accessing ASD.
3. **Devise access control policies**—Creation of a consistent security policy and standard operating procedures (SOPs) must be performed across all environments: endpoint, internal, edge and perimeter.
4. **Establishing visibility and Automation**—This is the last stage of maturity. Every activity/event occurring across all environments must be collected and analyzed by an automated threat detection system. Archiving major threats and events of interest should be conducted. Leveraging data analytics for detecting rogue users should be the outcome of this stage.

5.2. Transitioning to ZTA

When the process of transition begins, many challenges will arise. The first hurdle can be a lack of support from department administrators, executive members of management, normal employees and sometimes even top-level leadership. The second challenge may come in the implementation phase, oversights in access controls and proper configuration of security responses may allow some parts of the network to be left accessible by non-essential entities. So, it is essential that network engineers and company security teams are motivated to follow-up on these issues and plug in the gaps. Meanwhile, the management must also have the will to support the initiative financially and operationally.

Finally, the most prominent issue would come after the system is operational, work fatigue may set in and as time progresses the security posture can degrade due to overwork and the embodying the mindset of constant network compromise [43].

5.3. Achieving Zero-Trust Maturity

Before we begin to modify our network, we must adopt the mindset crucial to effectively make use of the security controls. It is essential to define expected outcomes when the system is fully operational. The organisation must identify its mission critical assets deployed in the network, cloud and on-site. The designers should have complete visibility over the components which would be added to the final network, this would enable them to assess and create an overall strategy for the protection of the entire system right from the design phase.

There must also be security measures which align themselves with the normal functioning of the network, they should not be more intrusive than they need to be, so it is essential to define the acceptable boundaries of surveillance.The National Security Agency

(NSA) provides four main principles for adopting the Zero-Trust mindset [43]. They are as follows:

(a) Coordinated management and monitoring of the system as well as its defensive capabilities;
(b) Assume all requests for critical resources and network traffic to be malicious;
(c) Assume that the network infrastructure and devices are already compromised;
(d) Assume all approvals for critical resources as risky and be prepared to perform damage control and recovery operations.

Implementing the above for, say, an enterprise-grade network cannot be done quickly, and transitioning everything and everyone all at once can cause faults to be introduced. So, we must have a maturity model, where the network is modified in a transitional manner, phase by phase. Most firms have existing infrastructure which requires the acquisition of additional software and hardware for this transition. The Figure 2 provides a visual discernment of what we have discussed so far.

Second, the Cybersecurity and Infrastructure Security Agency (CISA) in the U.S. released a zero-trust maturity model (ZTMM). The ZTMM model was classified into five pillars: identity, device, network/environment, application/workload and data from an asset perspective to be protected. Each pillar includes common elements regarding visibility and analysis, automation and orchestration, and governance. When the organization applied the zero-trust model, zero-trust maturity was divided into traditional, advanced and optimal levels. The traditional stage means a level without zero trust implementation. The traditional stage means a level without the implementation of a Zero-Trust model. The advanced stage means some implementation of a Zero-Trust model and the optimal stage means the fully automated implementation.

Third, Microsoft published a maturity model to implement the zero-trust model. MS's maturity model is similar to CISA's model, divided into six security elements: ID, device, application, infrastructure, network and data. In addition, the level of maturity was divided into traditional, advanced and optimal stages. The comparisons of ZTMM models (NIST, CISA, Microsoft) is shown in Table 3.

Table 3. The comparisons of ZTMM models (NIST, CISA, Microsoft).

Category		**NSA Model**	**CISA Model**	**MS Model**
Maturity Levels		**5 Stages**	**3 Stages**	**3 Stages**
Security Elements	Identities	✓	✓	✓
	Device	✓	✓	✓
	Network	✓	✓	✓
	Application		✓	✓
	Workload		✓	✓
	Data		✓	✓
	Infrastructure (VM, Cloud etc.)	✓		✓
	Visibility and Analytics	✓	✓	
	Automation/Orchestration	✓	✓	
	Governance (Polices)	✓	✓	

We need to understand that as the Zero-Trust Model is brought online, issues will most certainly occur, but coordination of the network improves over time as it is used. The enhanced infrastructure visibility and automation of security controls will give network administrators the ability to better thwart threats and mitigate risks before major damage can occur, much more than a traditional perimeter security system.

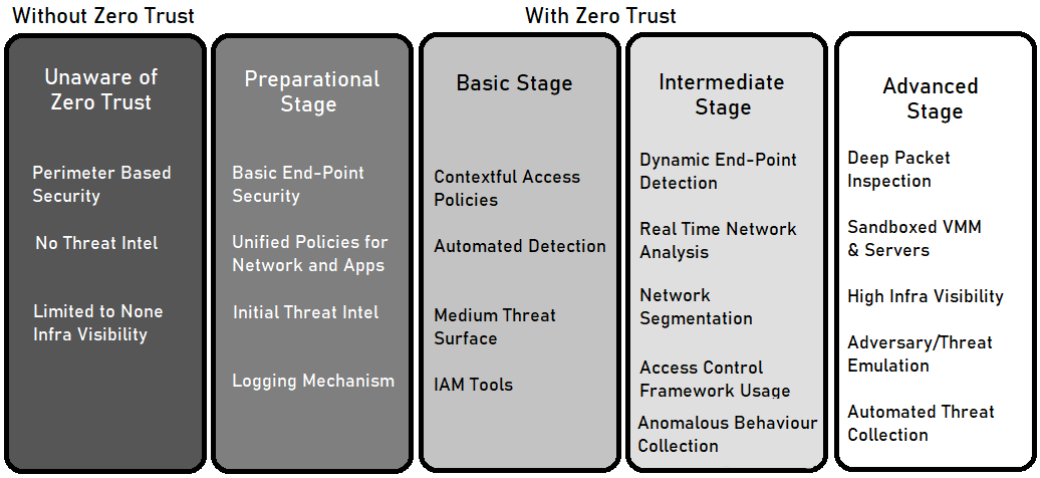

Figure 2. Stages of Zero-Trust Maturity.

5.4. Implementing the ZTA

A thorough implementation of a Zero-Trust Network must make use of several network sensors to achieve elevated levels of awareness inside and on the perimeter of the network. This system should not negatively impact performance; security is there only to prevent unauthorised events. Additional measures may have to be taken when implementing the model for a network, for example, east–west security controls (segmentation of network), grouping of users and nodes based on access policies, end-point detection response (EDR) and sandboxing of certain network components such as the VMM.

The ZTA is incomplete without an algorithm which calculates trust. As seen in Section 2, there are many variations in the method of calculating trust. However, it is the algorithm which will decide whether to deny or allow each individual request for access and use of network resources. Such an algorithm can be thought of as a function with inputs being relevant attributes such as access request type, previous behaviour of the requesting entity, resource usage history, previous history of penalties, current IAM policies, trust of the group to which the entity belongs to and current threat scenario, etc. Some of these are described in further detail below:

(a) **Current Threat Scenario**: This may include the type, severity and time intervals of recently detected attacks or network anomalies. This is a collection of threat intelligence to create a threat matrix for the network. The trust algorithm can use certain attributes selectively from the pool of threat attributes as needed.

(b) **Resource Usage Behaviour**: Previous usage of resources such as databases requests and network protocols used to access administrated areas, files and directories accessed on web servers and applications generally used by the user can be used as attributes for trust calculation. This would provide a histological aspect to the trust calculated: how a specific network resource was used and how it related to the work assigned to that entity.

(c) **Access Request**: The current request by the entity for entry to a protected component must have some additional metadata, such as time of request, number of previous requests made for the same component, level of authority required for access, current details of service or application being used to make the request (software version, OS version) and logical network identifiers such as MAC addresses and IP address.

(d) **Resource Status and Requirements**: In a dynamic network, the individual security of certain resources can be elevated or decreased as needed. The network may increase scrutiny of requests being made for access to that particular resource. So, in a case where the network might have recently had unauthorised access or anomalous behaviour, the ZTA authority may require the entity requesting access to meet certain

security standards such as updated software version, updated firmware version, use of only secure protocols and accepting responsibility for their actions when given access.

The algorithm may assign more attributes specific to the current network condition and give different weights to each attribute. This would allow granular, on-the-fly changes to the network security policy by security administrators as needed, as proposed by NIST.

5.5. Expanding the ZTA

Once a flow of actions has been integrated into the network response mechanism, a pre-set response policy can help automate responses to suspicious behaviour in the network. Now would be the time to establish a database of past recorded anomalies, which the network authority can use to further calculate trust values for requests and flow of data. If this is not possible, network responders should try to use operational experience to modify access policies as needed. However, automation would be more suitable for this task since the key concept is alleviating human errors and lapses in oversight.

It is now that the ZTA would be operational and extremely mission-critical networks can be further integrated into the established network, creating a distributed zero-trust network. It must be noted that with a major overhaul of the network such as the introduction of completely new virtualisation hardware and software, critical web server migration, shifting endpoint network terminals to a different OS, software updates to network component firmware, etc., there must be a re-evaluation of the ZTA and how the flow of response occurs. It is not necessary to change the ZTNA but rather re-evaluate as needed. Needless overhauls can also introduce security flaws. Another area of focus might be in Internet-of-Things (IoT) networks where Zero Trust can be used to validate transactions and nodes can have varying levels of trust, as discussed by Samaniego and Deters in [44]. Zero Trust can also be combined and used in conjunction with other novel technologies such as blockchain and the IoT, as proposed by Dhar and Bose [45].

6. Comparative Analysis of Zero-Trust Cloud Network Technologies

As zero trust is not a monolithic architecture, it employs many proven and emerging technologies. Comparing these is essential to sorting out the best- or worst-fit features. As adversaries change, regressive designs can be retired from the domain in favour of ones which work. The operational necessity is given precedence over the economic efficiency of this model. Furthermore, the various authors provide crucial insight into how most papers have contributed mainly to the architectural design and approach of ZTNs. These parameters were used for comparisons, reflecting the common key necessities found across many different implementations of cloud networks. The basis for using these parameters is discussed below, with references to works supporting their requirement. Although this is not an exhaustive list of parameters, the above set can be considered a higher priority based on the pre-established challenges.

1 **Variable Trust Levels**—In an unreliable environment such as a computer network, cooperation of beneficiary nodes as a distinct group has been shown to be a key component of the network's safety [46]. Since the security of resources is of paramount importance for the proper operation of cloud networks, determining the trustworthiness of a request must be based on available historical information. Judging every request with an unchanging standard causes gaps to arise in the authentication. Thus, the separation of trustworthiness of nodes according to different levels is optimal. A sound analogy can be drawn from a study on trust management in ad-hoc wireless networks, where rogue nodes' selfish behaviour regularly disrupts network operations, causing drops in throughput [47].

2 **Access Control Policies**—Implementing access controls for users in a fragmented network with different policies and standard procedures is not a new design choice [48]. A homogeneous policy globally across many data centres for a company can be catastrophic. User access controls in industrial control systems in standard practice, especially those connected to cloud-dependent hardware [49].

3 **Includes DMZ**—Creating a buffer zone with limited visibility for networks (DMZ) is the surface area of the main network. Unauthorized users may be able to exploit vulnerabilities in this zone, but access to the main network protected by a hard firewall would be difficult and detectable. Defense-in-depth, although a traditional aspect of network security, can be the front-line rather than the only counter available to a network [50].

4 **Logging Mechanism**—Maintaining network logs can be performed relatively quickly, but efficiency is the key in the cloud. Storing logs in a standard format which can be parsed by automated software such as intrusion detection and prevention can maximize the potential of preemptively safeguarding the network from attacks [51].

5 **Supports Segmented Networks**—Cloud networks are often deployed block by block, with services becoming operational in a transitory phase. This is practical as demand fuels the growth of a company's capabilities, and cloud platforms amply provide flexibility in the form of subscription plans for additional storage or computational needs. Segmenting sections is essential to keeping the confidentiality and integrity of data used by each cloud service or department in a company. Network devices need to segregate and direct traffic based on the affiliation of the service in the overall organizational structure, as demonstrated by [52]. Segmentation of the network also has some security benefits, as discussed by Du et al. [53], and improves the automation of the network's defenses against the enumeration of its resources [54,55].

6 **Supports Multi-Cloud Environment**—The cloud industry's gravitation towards offering support for many different cloud platforms can be attributed to its many advantages. There may be unique features and offerings by disparate CSPs that, when coupled, enhance the business capabilities of CSC, such as maintenance of information, preservation of data confidentiality, management of delicate infrastructure and improvements in performance [56–60].

7 **Supports Geographical Distribution of System**—Due to natural disasters, businesses can be severely affected if their offerings can no longer be available. Thus, cloud networks require reliability and fall-back options. CSCs are also unevenly distributed across the globe, and parallel servers must be provided to reduce issues such as latency, traffic load balancing, non-repudiation of data, and primarily balancing the allocation of resources offered to users [61,62].

8 **Supports Open-Source Tools**—Open-Source has long been a cornerstone of public engagement in software development. The use of open-source tools and software which are free and publicly available gives government institutions and corporations the ability to modify the software as per their need and quickly deploy it for use. Open-Source software is generally more secure and has had many improvements, which comes with the pooling of human resources and skillsets common in Open-Source communities. A case study by Rodriguez-Martinez et al. [63] on the use of Open-Source software for weather systems hosted on the cloud showed that the cost of ownership was relatively low, the reliability of the system high and the huge potential of scalability for their system. The only downsides were the learning curve was challenging at first and the lack of specific management tools such as a Graphical User Interface (GUI)-based system for operating their cloud stack. A similar study by Huang et al. [64] on open-source cloud computing solutions for geo-sciences showed that the performance of such systems was better in most and comparative in others to commercially available counterparts. Finally, other potential benefits were described by I. Voras et al. [65].

9 **Support for Containers and Micro-services**—The final parameter support for micro-services and containerized applications results from consumer demand. The use of containers provides higher levels of scalability, reliability, and isolation of sensitive resources. Packaging entire programs or software suites is efficient and streamlines maintenance. This is potentially valuable for governance-related scenarios such as healthcare or use in Internet of Things (IoT)-enabled networks for vehicles [66–69].

These parameters were used after a study of the aforementioned papers, and they reflect the key common necessities found across many different implementations of cloud networks. Although this is not an exhaustive list of parameters, the above set can be considered higher priority based on the pre-established challenges.Variable levels of trust for different areas of the network in a cloud environment is a key necessity. Separation of bias during analysis of malicious events in one domain of the network would provide a reasonably specific picture of the daily events occurring in a certain part of the network and eliminate false-positives. It would also enable administrators to assess users not just individually but as a whole group and adopt specific countermeasures. This is where Access Control Policies come into use, although not essential, having a configurable default policy setting globally across many data-centers for a company can be considered essential. Logging mechanisms are important as they provide transparency providing detailed reasoning behind the calculation of trust for a particular entity, based on known events. The comparison of existing research models based on parameters associated with Zero-Trust Cloud Networks is shown in Table 4.

Table 4. A detailed comparison of existing research models based on parameters associated with Zero-Trust Cloud Networks. {P1: Variable Trust Levels, P2: Access Control Policies, P3: Includes DMZ, P4: Logging Mechanism, P5: Supports Segmented Networks, P6: Supports Multi-Cloud Environment, P7: Supports Geographical Distribution of System, P8: Supports Open-Source Tools, P9: Support for Containers and Micro-services}.

Authors	Novel Features	P1	P2	P3	P4	P5	P6	P7	P8	P9
Casimer et al. [23]	Transport Access Control and First Packet Authentication		✓		✓	✓		✓	✓	
Dayna et al. [31]	Autonomic control plane threat response using Boyd's OODA framework	✓	✓		✓	✓			✓	
Casimer et al. [30]	Transport Access Control and First Packet Authentication with geolocation attributes		✓		✓	✓		✓	✓	✓
Anwar et al. [32]	User data privacy protection for location-based services using data partitioning		✓		✓	✓				
Abdullah et al. [33]	Identity verification using client-server model and adaptive behaviour evaluation model of trusted nodes	✓	✓	✓	✓	✓				

As part of a maturity cycle, having a pre-established DMZ can be useful. It would filter out many commonly used attack patterns originating externally and it would carry no additional commitment of resources. In 2020, almost 93% of all organisations using the cloud were adopting a multi-cloud strategy [70]; this is why multi-cloud support is a future-proof solution for networked security systems, especially ZTA-based solutions which make use of a wide scope of emerging and proven technologies. Considering that the big three cloud services are based across different geographies and have large distances and are under many differing jurisdictions, it would be pertinent to have some semblance of support for distributed cloud networks. Taking into account latency in situations where multiple cases of repudiation show up or unwanted feedback loops are formed in cloud environments communicating across great physical distances, it would be wise to have a well-tested remediation system in place for any ZTCN. The comparison of existing research frameworks based on parameters associated with Zero-Trust Cloud Networks is shown in Table 5.

Table 5. A comparison of existing research frameworks based on parameters associated with Zero-Trust Cloud Networks. {P1: Inclusion of Variable Trust Levels, P2: Develops Access Control Policy Language, P3: Includes DMZ, P4: Includes Logging Mechanisms, P5: Includes Segmentation of Networks, P6: Includes Multi-Cloud Strategy, P7: Accounts for Geographical Distribution of System, P8: Includes Performance Analysis, P9: Includes Containers and Micro-services}.

Authors	Novel Feature	P1	P2	P3	P4	P5	P6	P7	P8	P9
Romans et al. [34]	Fuzzy Risk evaluation-based access control enforcement framework		✓	✓		✓				
Abdallah et al. [36]	SDP-based framework using a client-gateway architecture			✓	✓	✓			✓	
Mehraj et al. [35]	Typologies of Trust in Zero-Trust context. Use of Zero-Trust Triangle for calculation of trust for an entity		✓	✓	✓	✓				
Ahmed et al. [37]	Zero-trust framework for federated Identity Access Management in Cloud Computing using decentralised audit logs		✓		✓	✓	✓			
Simone et al. [27]	Performance Analysis of the cloud data plane under load and impact on the control plane			✓		✓	✓		✓	✓

Segmentation of a network is the only parameter other than variable level of trust which is common across all solutions compared in this paper, except Zirak Zaheer's perimeter security solution. This clearly shows that segmenting areas is highly beneficial to the security posture of any system in the long run. The comparison of existing proof-of-concept technologies associated with Zero-Trust Cloud Networks based on the various parameters is shown in Table 6.

Table 6. A comparison of existing proof-of-concept technologies associated with Zero-Trust Cloud Networks based on the following parameters. {P1: Variable Trust Levels, P2: Access Control Policies, P3: Supports DMZ, P4: Logging Mechanism, P5: Supports Segmented Networks, P6: Supports Multi-Cloud, P7: Supports Geographically Distributed Cloud System, P8: Supports FOSS, P9: Supports Containers and Micro-services}.

Authors	Novel Feature	P1	P2	P3	P4	P5	P6	P7	P8	P9
Zirak et al. [27]	Network-independent perimeter solution which traces authentic identities using per-packet tagging and verification.		✓	✓	✓			✓	✓	✓
Weever et al. [38]	Operational controls which mitigate data leaks during service-to-service transit of data in public cloud.					✓	✓	✓	✓	✓

In the many implementations of Zero-Trust Cloud Networks we encountered, almost all models included support for segmentation of the cloud network. This indicates an increase in complexity of the systems being hosted on cloud networks, leading to the need for segmentation. Again, almost all implementations included a logging mechanism. Even if not visible to the administrators, the logging mechanism stores necessary proof for future trust calculations and enforcement of access control policies.

Open-source tool integration is also on the rise as administrators need tools which give them fine-grained control of the cloud network. Another interesting observation was that of geographical distribution of the systems or support for networks hosted across a huge physical distance. This may indicate a wider use of network resources across different regions. The addition of micro-segmentation and Zero Trust does not have an enormous impact on performance of the network as stated by Muji M. et al. [71].

There currently exist proof-of-concepts for key components of a fully independent zero-trust network, purpose-built for cloud micro-services. eZTrust is the most mature in a practical and deployment use-case. An operational control and monitoring tool for in transit data by Weever and Andreou adds to potential features for future ZTCNs [36].

In the future, more support is required for applications hosted as micro-services and containers on the cloud, as well as multi-cloud environments, where hardware and software from different vendors are in use.

7. Potential Future Work

Zero Trust as the basis for cloud networks should be used to re-prioritize existing technologies available to the end-user and design a streamlined system to minimize authentication delays while ensuring business continuity. ZTA currently uses security information and event management (SIEM), data analytics, trust calculation using event logging, modification of file system permissions using active directory and multi-factor authentication (MFA). These are individual technologies used in conjunction. There remains a vast scope of improvement and addition to the compendium of ZTCN technologies; some of the areas of particular focus are listed below:

- **Internet-of-Things and Blockchains**: Zero-Trust can be used to validate transactions, and nodes can have varying levels of Trust. As proposed by Dhar and Bose, Zero Trust can also be combined and used with other novel technologies such as blockchain and the IoT.
- **5G/6G Networks**: Given the advances in data transfer rates, traditional security controls will become overwhelmed by the sheer quantity and variety of data they have to process and verify. This calls for revolutionary changes in the design of network protocols and how the routing of data works in 5G-enabled networks [72]. Artificial Intelligence algorithms can deter malicious requests and thwart network performance degradation in real-time or almost real-time [73]. This would be essential in mission-critical sectors such as healthcare, air defense and autonomous vehicle networks [74].
- **Military Networks**: The need for Zero Trust arose from concerns about the reliability of military communication networks spanning many different operational environments. It has now come full circle and matured into a technology used to keep adversaries out of military networks, many of which use cloud services ranging from non-essential to highly critical. In conventional armed forces, offensive and defensive cyber capabilities are often developed in isolation in different branches and agencies, called 'silos', and there is no real-time sharing of capabilities. This enables adversarial nation-states and APTs to exploit this gap in the command structure and breach government data servers [75]. Thus, with this philosophy, the United States Army is migrating to a Zero-Trust architecture as mandated by EO 14028. The zero trust road-map developed by the U.S government involves the NSA, DoD, CISA, NIST and OMB all pooling their resources to convert the entire government ecosystem into a ZT-based one. A simultaneous transformation effort by the various agencies will result in a system with a common operational picture devised by the DoD's Zero Trust Reference Architecture and meet the national security objective.
- **Containerized software and micro-services**: Using micro-services as a basis for comparison shows it requires further research and improvements. Micro-services are essentially programs running in an austere environment; the problems associated with scheduling and managing processes generated by such micro-services can metastasize into more significant problems [69]. More performance improvements are necessary to analyze the micro-services' impact on cloud networks thoroughly.
- **Sustainable Cloud Systems**: Any IT system's security relies on its availability just as much as its confidentiality and integrity. Thus, future cloud networks must not only balance security and reliability, but effective use of electricity and overall sustainability

of their network design must also be a focus. Sustainable cloud networks would have a higher tolerance for unwarranted disruptions [76].

8. Conclusions

This paper presented a comprehensive discussion of current zero-trust cloud network technology implementations along with their strengths and limitations. Zero Trust provides a highly granular and case-specific solution to network security issues in the cloud. It is a highly agile approach; however, further research and commercial use are required to present comprehensive conclusions about its effectiveness in real-world deployments. The scope of our paper is limited to publicly available research projects. This paper compares security-based features of recently published zero-trust-based cloud network models, frameworks and proofs-of-concept employed for network security. Comparing these models and frameworks used in zero-trust networks will enable future researchers to focus on security issues and oversights plaguing modern cloud computing networks. It allows them to create robust zero-trust cloud networks and implement intelligent Security Orchestration, Automation and Response. Commercial software products based on Zero-Trust Architecture for the cloud exist and require further extrapolation of their effectiveness. VMware's Carbon Black is a great example, which provides east–west security using multi-hop network traffic analysis.

The scope of this paper is such that future researchers would be able to follow the general timeline and milestones in developing the Zero-Trust Architecture their cloud platform needs. This would be beneficial to map the actual capabilities and operational needs of their network. It would inhibit feature creep in their design while allowing their network to become more agile, automated and transparent in its decision making. Currently, many network test-beds and proofs-of-concept are available for specific purposes; unfortunately, none provide a comprehensive platform or a 'one-size-fits-all' type of system. To alleviate this, a cloud network architecture which uses a modular, add-drop style of trust-based technologies can be developed in the future. This can provide the right balance of business flexibility and adaptive security.

Author Contributions: Conceptualization, S.S., G.C., S.K.S., A.H. and H.K.; methodology, S.S., G.C. and A.H.; validation, G.C., S.K.S., A.H. and H.K.; investigation, G.C. and H.K.; resources, G.C., S.K.S., A.H. and H.K.; data curation, S.S., G.C., S.K.S., A.H. and H.K.; writing—original draft preparation, S.S., G.C. and H.K.; writing—review and editing, G.C. and H.K.; visualization, G.C., S.K.S., A.H. and H.K.; supervision, G.C., S.K.S., A.H. and H.K.; project administration, G.C. and H.K.; funding acquisition, H.K. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by Institute of Information and communications Technology Planning and Evaluation (IITP) grant funded by the Korea Government (MSIT) (No. 2021- 0-00358, AI Big data based Cyber Security Orchestration and Automated Response Technology Development).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Share of Corporate Data Stored in the Cloud in Organizations Worldwide from 2015 to 2022. Available online: https://www.statista.com/statistics/1062879/worldwide-cloud-storage-of-corporate-data/ (accessed on 30 July 2022).
2. El-Shrkawey, M.; Alalfi, M.; Al-Mahdi, H. An Enhanced Intrusion Detection System Based on Multi-Layer Feature Reduction for Probe and DoS Attacks. *J. Internet Serv. Inf. Secur.* **2021**, *11*, 61–78.
3. Rahmadika, S.; Firdaus, M.; Lee, Y.H.; Rhee, K.H. An Investigation of Pseudonymization Techniques in Decentralized Transactions. *J. Internet Serv. Inf. Secur.* **2021**, *11*, 1–18.
4. Pagano, F.; Verderame, L.; Merlo, A. Understanding Fuchsia Security. *J. Wirel. Mob. Netw. Ubiquitous Comput. Dependable Appl.* **2021**, *12*, 47–64.

5. Gupta, T.; Choudhary, G.; Sharma, V. A survey on the security of pervasive online social networks (POSNs). *arXiv* **2018**, arXiv:1806.07526.
6. Velumani, R.; Sudalaimuthu, H.; Choudhary, G.; Bama, S.; Jose, M.V.; Dragoni, N. Secured Secret Sharing of QR Codes Based on Nonnegative Matrix Factorization and Regularized Super Resolution Convolutional Neural Network. *Sensors* **2022**, *22*, 2959. [CrossRef] [PubMed]
7. Unit 42 Cloud Threat Report 2H 2021. Available online: https://www.paloaltonetworks.com/prisma/unit42-cloud-threat-research-2h21 (accessed on 30 July 2022).
8. Teerakanok, S.; Uehara, T.; Inomata, A. Migrating to zero trust architecture: Reviews and challenges. *Secur. Commun. Netw.* **2021**, *2021*, 9947347. [CrossRef]
9. Greitzer, F.L.; Purl, J.; Sticha, P.J.; Yu, M.C.; Lee, J. Use of Expert Judgments to Inform Bayesian Models of Insider Threat Risk. *J. Wirel. Mob. Netw. Ubiquitous Comput. Dependable Appl.* **2021**, *12*, 3–47.
10. Rahmadika, S.; Astillo, P.V.; Choudhary, G.; Duguma, D.G.; Sharma, V.; You, I. Blockchain-based Privacy Preservation Scheme for Misbehavior Detection in Lightweight IoMT Devices. *IEEE J. Biomed. Health Inform.* **2022**.[CrossRef]
11. Alagappan, A.; Venkatachary, S.K.; Andrews, L.J.B. Augmenting Zero Trust Network Architecture to enhance security in virtual power plants. *Energy Rep.* **2022**, *8*, 1309–1320. [CrossRef]
12. Tyler, D.; Viana, T. Trust No One? A Framework for Assisting Healthcare Organisations in Transitioning to a Zero-Trust Network Architecture. *Appl. Sci.* **2021**, *11*, 7499. [CrossRef]
13. Astillo, P.V.; Choudhary, G.; Duguma, D.G.; Kim, J.; You, I. TrMAps: Trust management in specification-based misbehavior detection system for IMD-enabled artificial pancreas system. *IEEE J. Biomed. Health Inform.* **2021**, *25*, 3763–3775. [CrossRef] [PubMed]
14. RightScale 2019 State of the Cloud Report, (March 2022). Available online: https://www.flexera.com/about-us/press-center/rightscale-2019-state-of-the-cloud-report-from-flexera-identifies-cloud-adoption-trends#:~:text=In (accessed on 30 July 2022).
15. Garbis, J.; Chapman, J.W. *Zero Trust Security: An Enterprise Guide*; Springer: Berlin/Heidelberg, Germany, 2021.
16. Stafford, V. Zero trust architecture. *NIST Spec. Publ.* **2020**, *800*, 207.
17. Moving the U.S. Government Toward Zero Trust Cybersecurity Principles. Available online: https://www.whitehouse.gov/omb/briefing-room/2022/01/26/office-of-management-and-budget-releases-federal-strategy-to-move-the-u-s-government-towards-a-zero-trust-architecture (accessed on 30 July 2022).
18. Buck, C.; Olenberger, C.; Schweizer, A.; Völter, F.; Eymann, T. Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust. *Comput. Secur.* **2021**, *110*, 102436. [CrossRef]
19. Alevizos, L.; Ta, V.T.; Hashem Eiza, M. Augmenting zero trust architecture to endpoints using blockchain: A state-of-the-art review. *Secur. Priv.* **2022**, *5*, e191. [CrossRef]
20. He, Y.; Huang, D.; Chen, L.; Ni, Y.; Ma, X. A Survey on Zero Trust Architecture: Challenges and Future Trends. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 6476274. [CrossRef]
21. Syed, N.F.; Shah, S.W.; Shaghaghi, A.; Anwar, A.; Baig, Z.; Doss, R. Zero Trust Architecture (ZTA): A Comprehensive Survey. *IEEE Access* **2022**, 10, 57143–57179. [CrossRef]
22. Pittman, J.M.; Alaee, S.; Crosby, C.; Honey, T.; Schaefer, G.M. Towards a Model for Zero Trust Data. *AJSE* **2022**, *3*, 18–24.
23. DeCusatis, C.; Liengtiraphan, P.; Sager, A.; Pinelli, M. Implementing zero trust cloud networks with transport access control and first packet authentication. In Proceedings of the 2016 IEEE International Conference on Smart Cloud (SmartCloud), New York, NY, USA, 18–20 November 2016; pp. 5–10.
24. Kindervag, J. *No More Chewy Centers: The Zero Trust Model of Information Security*; Forrester Research Inc.: Cambridge, MA, USA, 2016.
25. Kindervag, J. *Build Security into Your Network's Dna: The Zero Trust Network Architecture*; Forrester Research Inc.: Cambridge, MA, USA, 2010.
26. Zhang, P.; Tian, C.; Shang, T.; Liu, L.; Li, L.; Wang, W.; Zhao, Y. Dynamic access control technology based on zero-trust light verification network model. In Proceedings of the 2021 International Conference on Communications, Information System and Computer Engineering (CISCE), Beijing, China, 14–16 May 2021; pp. 712–715.
27. Rodigari, S.; O'Shea, D.; McCarthy, P.; McCarry, M.; McSweeney, S. Performance Analysis of Zero-Trust multi-cloud. In Proceedings of the 2021 IEEE 14th International Conference on Cloud Computing (CLOUD), Chicago, IL, USA, 5–10 September 2021; pp. 730–732.
28. Shore, M.; Zeadally, S.; Keshariya, A. Zero Trust: The What, How, Why, and When. *Computer* **2021**, *54*, 26–35. [CrossRef]
29. D'Silva, D.; Ambawade, D.D. Building a zero trust architecture using Kubernetes. In Proceedings of the 2021 6th international conference for convergence in technology (i2ct), Maharashtra, India, 2–4 April 2021; pp. 1–8.
30. DeCusatis, C.; Liengtiraphan, P.; Sager, A. Advanced intrusion prevention for geographically dispersed higher education cloud networks. In *Online Engineering & Internet of Things*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 132–143.
31. Eidle, D.; Ni, S.Y.; DeCusatis, C.; Sager, A. Autonomic security for zero trust networks. In Proceedings of the 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), New York, NY, USA, 19–21 October 2017; pp. 288–293.

32. Jasim, A.C.; Hassoon, I.A.; Tapus, N. Cloud: Privacy For Locations Based-services' through Access Control with dynamic multi-level policy. In Proceedings of the 2019 6th International Conference on Control, Decision and Information Technologies (CoDIT), Paris, France, 23–26 April 2019; pp. 1911–1916.
33. Albuali, A.; Mengistu, T.; Che, D. ZTIMM: A zero-trust-based identity management model for volunteer cloud computing. In Proceedings of the International Conference on Cloud Computing, Honolulu, HI, USA, 18–20 September 2020; Springer: Cham, Switzerland, 2020; pp. 287–294.
34. Vanickis, R.; Jacob, P.; Dehghanzadeh, S.; Lee, B. Access control policy enforcement for zero-trust-networking. In Proceedings of the 2018 29th Irish Signals and Systems Conference (ISSC), Belfast, UK, 21–22 June 2018; pp. 1–6.
35. Mehraj, S.; Banday, M.T. Establishing a zero trust strategy in cloud computing environment. In Proceedings of the 2020 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 22–24 January 2020; pp. 1–6.
36. Moubayed, A.; Refaey, A.; Shami, A. Software-defined perimeter (sdp): State of the art secure solution for modern networks. *IEEE Netw.* **2019**, *33*, 226–233. [CrossRef]
37. Ahmed, M.; Petrova, K. A Zero-Trust Federated Identity and Access Management Framework for Cloud and Cloud-based Computing Environments. Available online: https://aisel.aisnet.org/wisp2020/4/ (accessed on 30 July 2022).
38. de Weever, C.; Andreou, M. *Zero Trust Network Security Model in Containerized Environments*; University of Amsterdam: Amsterdam, The Netherlands, 2020.
39. Zhu, G.; Yin, Y.; Cai, R.; Li, K. Detecting virtualization specific vulnerabilities in cloud computing environment. In Proceedings of the 2017 IEEE 10th International Conference on Cloud Computing (CLOUD), Honolulu, HI, USA, 25–30 June 2017; pp. 743–748.
40. Pék, G.; Buttyán, L.; Bencsáth, B. A survey of security issues in hardware virtualization. *ACM Comput. Surv.* **2013**, *45*, 1–34. [CrossRef]
41. Crowd Research Partners, Cloud Security Report 2018. Available online: https://crowdresearchpartners.com/portfolio/cloud-security-report/ (accessed on 30 June 2022).
42. Kandias, M.; Virvilis, N.; Gritzalis, D. The insider threat in cloud computing. In Proceedings of the International Workshop on Critical Information Infrastructures Security, Lucerne, Switzerland, 8–9 September 2011; Springer: Berlin/Heidelberg, Germany, 2011; pp. 93–103.
43. Info Sheet: Embracing a Zero Trust Security Model (February 2021). Available online: https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF (accessed on 30 June 2022).
44. Samaniego, M.; Deters, R. Zero-trust hierarchical management in IoT. In Proceedings of the 2018 IEEE international congress on Internet of Things (ICIOT), San Francisco, CA, USA, 2–7 July 2018; pp. 88–95.
45. Dhar, S.; Bose, I. Securing IoT devices using zero trust and blockchain. *J. Organ. Comput. Electron. Commer.* **2021**, *31*, 18–34. [CrossRef]
46. Zhang, B.; Huang, Z.; Xiang, Y. A novel multiple-level trust management framework for wireless sensor networks. *Comput. Netw.* **2014**, *72*, 45–61. [CrossRef]
47. Luo, J.; Liu, X.; Fan, M. A trust model based on fuzzy recommendation for mobile ad-hoc networks. *Comput. Netw.* **2009**, *53*, 2396–2407. [CrossRef]
48. Singh, S.; Choudhary, G.; Shandilya, S.K.; Sihag, V.; Choudhary, A. Counterfeited Product Identification in a Supply Chain using Blockchain Technology. *Res. Briefs Inf. Commun. Technol. Evol.* **2021**, *7*, 3.
49. Lopez, J.; Rubio, J.E. Access control for cyber-physical systems interconnected to the cloud. *Comput. Netw.* **2018**, *134*, 46–54. [CrossRef]
50. Dadheech, K.; Choudhary, A.; Bhatia, G. De-militarized zone: A next level to network security. In Proceedings of the 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT), Coimbatore, India, 20–21 April 2018; pp. 595–600.
51. Tovarnák, D.; Vaekova, A.; Novák, S.; Pitner, T. Structured and interoperable logging for the cloud computing Era: The pitfalls and benefits. In Proceedings of the 2013 IEEE/ACM 6th International Conference on Utility and Cloud Computing, Dresden, Germany, 9–12 December 2013; pp. 91–98.
52. Jeuk, S.; Salgueiro, G.; Baker, F.; Zhou, S. Network segmentation in the cloud a novel architecture based on UCC and IID. In Proceedings of the 2015 IEEE 4th International Conference on Cloud Networking (CloudNet), Niagara Falls, ON, Canada, 5–7 October 2015; pp. 58–63.
53. Du, R.; Zhao, C.; Li, S.; Li, J. A strategy of network coding against wiretapping attack based on network segmentation. In Proceedings of the Second International Conference on Communications, Signal Processing, and Systems, Tianjin, China, 1–2 September 2013; Springer: Cham, Switzerland, 2014; pp. 1137–1144.
54. Wagner, N.; Şahin, C.Ş.; Winterrose, M.; Riordan, J.; Pena, J.; Hanson, D.; Streilein, W.W. Towards automated cyber decision support: A case study on network segmentation for security. In Proceedings of the 2016 IEEE Symposium Series on Computational Intelligence (SSCI), Athens, Greece, 6–9 December 2016; pp. 1–10.
55. Wagner, N.; Şahin, C.Ş.; Pena, J.; Riordan, J.; Neumayer, S. Capturing the security effects of network segmentation via a continuous-time markov chain model. In Proceedings of the 50th Annual Simulation Symposium, Virginia Beach, VA, USA, 23–26 April 2017; pp. 1–12.
56. Raj, J.S. Efficient information maintenance using computational intelligence in the multi-cloud architecture. *J. Soft Comput. Paradig.* **2019**, *1*, 113–124. [CrossRef]

57. Sulochana, M.; Dubey, O. Preserving data confidentiality using multi-cloud architecture. *Procedia Comput. Sci.* **2015**, *50*, 357–362. [CrossRef]
58. Kovács, J.; Kacsuk, P. Occopus: A multi-cloud orchestrator to deploy and manage complex scientific infrastructures. *J. Grid Comput.* **2018**, *16*, 19–37. [CrossRef]
59. Gundu, S.R.; Panem, C.A.; Thimmapuram, A. Hybrid IT and Multi Cloud an Emerging Trend and Improved Performance in Cloud Computing. *SN Comput. Sci.* **2020**, *1*, 256. [CrossRef]
60. Alshammari, M.M.; Alwan, A.A.; Nordin, A.; Al-Shaikhli, I.F. Disaster recovery in single-cloud and multi-cloud environments: Issues and challenges. In Proceedings of the 2017 4th IEEE International Conference on Engineering Technologies and Applied Sciences (ICETAS), Salmabad, Bahrain, 29 November–1 December 2017; pp. 1–7.
61. Endo, P.T.; de Almeida Palhares, A.V.; Pereira, N.N.; Goncalves, G.E.; Sadok, D.; Kelner, J.; Melander, B.; Mangs, J.E. Resource allocation for distributed cloud: Concepts and research challenges. *IEEE Netw.* **2011**, *25*, 42–46. [CrossRef]
62. Hogade, N.; Pasricha, S.; Siegel, H.J. Energy and network aware workload management for geographically distributed data centers. *IEEE Trans. Sustain. Comput.* **2021**, *7*, 400–413. [CrossRef]
63. Rodriguez-Martinez, M.; Seguel, J.; Greer, M. Open source cloud computing tools: A case study with a weather application. In Proceedings of the 2010 IEEE 3rd International Conference on Cloud Computing, Miami, FL, USA, 5–10 July 2010; pp. 443–449.
64. Huang, Q.; Yang, C.; Liu, K.; Xia, J.; Xu, C.; Li, J.; Gui, Z.; Sun, M.; Li, Z. Evaluating open-source cloud computing solutions for geosciences. *Comput. Geosci.* **2013**, *59*, 41–52. [CrossRef]
65. Voras, I.; Mihaljević, B.; Orlić, M.; Pletikosa, M.; Žagar, M.; Pavić, T.; Zimmer, K.; Čavrak, I.; Paunović, V.; Bosnić, I.; et al. Evaluating open-source cloud computing solutions. In Proceedings of the 34th International Convention MIPRO, Opatija, Croatia, 23–27 May 2011; pp. 209–214.
66. Esposito, C.; Castiglione, A.; Tudorica, C.A.; Pop, F. Security and privacy for cloud-based data management in the health network service chain: A microservice approach. *IEEE Commun. Mag.* **2017**, *55*, 102–108. [CrossRef]
67. Lakhan, A.; Memon, M.S.; Elhoseny, M.; Mohammed, M.A.; Qabulio, M.; Abdel-Basset, M. Cost-efficient mobility offloading and task scheduling for microservices IoVT applications in container-based fog cloud network. *Clust. Comput.* **2022**, *25*, 2061–2083. [CrossRef]
68. Amaral, M.; Polo, J.; Carrera, D.; Mohomed, I.; Unuvar, M.; Steinder, M. Performance evaluation of microservices architectures using containers. In Proceedings of the 2015 IEEE 14th International Symposium on Network Computing and Applications, Cambridge, MA, USA, 28–30 September 201; pp. 27–34.
69. Kyryk, M.; Pleskanka, N.; Pleskanka, M.; Kyryk, V. Infrastructure as Code and Microservices for Intent-Based Cloud Networking. In *Future Intent-Based Networking*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 51–68.
70. State of the Cloud Report, (March 2022). Available online: https://info.flexera.com/CM-REPORT-State-of-the-Cloud (accessed on 30 June 2022).
71. Mujib, M.; Sari, R.F. Performance evaluation of data center network with network micro-segmentation. In Proceedings of the 2020 12th International Conference on Information Technology and Electrical Engineering (ICITEE), Yogyakarta, Indonesia, 6–8 October 2020; pp. 27–32.
72. Dzogovic, B.; Santos, B.; Hassan, I.; Feng, B.; Jacot, N.; Van Do, T. Zero-Trust Cybersecurity Approach for Dynamic 5G Network Slicing with Network Service Mesh and Segment-Routing over IPv6. In Proceedings of the 2022 International Conference on Development and Application Systems (DAS), Suceava, Romania, 26–28 May 2022; pp. 105–114.
73. Ramezanpour, K.; Jagannath, J. Intelligent Zero Trust Architecture for 5G/6G Networks: Principles, Challenges, and the Role of Machine Learning in the context of O-RAN. *arXiv* **2021**, arXiv:2105.
74. Bello, Y.; Hussein, A.R.; Ulema, M.; Koilpillai, J. On Sustained Zero Trust Conceptualization Security for Mobile Core Networks in 5G and Beyond. *IEEE Trans. Netw. Serv. Manag.* **2022**, *19*, 1876–1889. [CrossRef]
75. Stewart, A. Three Emerging Innovative Technologies Required for Cyber Operations to Execute Commander's Intent at Machine Speed. *Mil. Cyber Aff.* **2020**, *4*, 3. [CrossRef]
76. Chen, T.; Marques, A.G.; Giannakis, G.B. DGLB: Distributed stochastic geographical load balancing over cloud networks. *IEEE Trans. Parallel Distrib. Syst.* **2016**, *28*, 1866–1880. [CrossRef]