Vol. 2 No. 3 (2024)

Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138
Print ISSN
3007-312X

A Survey on Latest Trends and Technologies of Computer Systems Network

Shehreyar Nawaz[1]
Department of Computer Science, Faculty of Computer Science & IT Superior University Lahore, 54000, Pakistan.
shehreyarnawaz786@gmail.com

Hamayun Khan[2]
Department of Computer Science, Faculty of Computer Science & IT Superior University Lahore, 54000, Pakistan
hamayun.khan@superior.edu.pk

Wajiha Salman[3]
Department of Computer Science, Faculty of Computer Science & IT Superior University Lahore, 54000, Pakistan

Umer Shahid[4]
Department of Computer Science, Faculty of Computer Science & IT Superior University Lahore, 54000, Pakistan
umershahid649@gmail.com

Momin Latif Khokhar[5]
Department of Computer Science, Faculty of Computer Science & IT Superior University Lahore, 54000, Pakistan
mominlatif2004@gmail.com

M Zaid Iqbal[6]
Department of Computer Science, Faculty of Computer Science & IT Superior University Lahore, 54000, Pakistan
mubaidiqbal36@gmail.com

Abdullah Hamid[7]
Department of Computer Science, Faculty of Computer Science & IT Superior University Lahore, 54000, Pakistan
abdullahchaudary10101@gmail.com

Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138
Print ISSN
3007-312X

Haroon Abdullah[8]

Department of Computer Science, Faculty of Computer Science & IT Superior University Lahore, 54000, Pakistan

ha0319999@gmail.com

Abstract

Zero trust (ZT) represents a set of evolving cybersecurity principles that shift defense strategies from fixed, network-centered perimeters to a focus on users, assets, and resources. A zero trust architecture (ZTA) applies these principles to design industrial and enterprise infrastructure and workflows. Zero trust operates on the idea that no implicit trust is granted to any asset or user account based solely on physical or network location (e.g., a local network versus the internet) or asset ownership (whether enterprise-owned or personal). Both authentication and authorization (of the user and device) are separate steps that must be completed before access to an enterprise resource is allowed. Zero trust is a response to modern network trends such as remote work, bring your own device (BYOD) practices, and the use of cloud-based resources outside an organization's direct network boundary. Rather than focusing on network segments, zero trust prioritizes securing resources—like assets, services, workflows, and user accounts—because network location alone is no longer considered a main factor in assessing the security posture of a resource. This document provides an outline of zero trust architecture (ZTA), along with general deployment models and use cases where zero trust can enhance an organization's overall IT security posture.

Keywords: Architecture; Cybersecurity; Enterprise; Network Security; Zero Trust.

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN 3007-3138
Print ISSN 3007-312X

Introduction

Modern enterprises face increasingly complex infrastructures, often including multiple internal networks, remote offices with local setups, mobile users, and cloud services. This complexity has surpassed the capabilities of traditional perimeter-based security, which proves inadequate when an attacker breaches the perimeter, allowing unrestricted lateral movement.[1, 4]

To address these limitations, the "zero trust" (ZT) model has emerged, focusing on safeguarding data and services, and extending to all enterprise assets—devices, applications, infrastructure, and users. In ZT models, "subjects" encompass users and non-human entities that request information. Zero trust assumes that attackers could be within the environment and treats enterprise and non-enterprise environments as equally untrusted. This approach requires continuous risk assessment and implementing protections tailored to the level of risk[5, 6].

Zero trust architecture (ZTA) is a cybersecurity framework that incorporates ZT principles to prevent breaches and restrict lateral movement. This document explores ZTA's components, deployment scenarios, and potential threats, along with a roadmap for organizations transitioning to a zero trust approach, including relevant federal policies that might affect its implementation.

ZT isn't a single structure but a set of guiding principles that improve security across different systems and sensitivity levels. Transitioning to ZTA is gradual and aligns with an organization's risk-based mission, often resulting in a hybrid ZT/perimeter-based model. Organizations should look to adopt ZT principles step-by-step by adapting processes and technologies to protect data and assets. Implementing zero trust effectively requires robust information security practices, identity and access management, and continuous monitoring. When combined with existing cybersecurity policies, these practices can enhance an organization's security posture through managed risk and resilience. [4, 7]

History of Zero Trust Efforts Related to Federal Agencies

The idea of zero trust in cybersecurity predates the term itself. Early foundations were laid by the Defense Information Systems Agency (DISA) and the Department of Defense, who introduced a "black core" strategy focused on securing individual transactions instead of relying on a perimeter-based model. Similarly, the Jericho Forum in 2004 highlighted the concept of de-perimeterization, questioning the reliance on static, location-based trust over large network areas. Over time, de-perimeterization principles evolved into the broader concept of zero trust, a term later coined by John Kindervag at Forrester. Zero trust now represents a range of cybersecurity solutions that assess trust per transaction rather than through assumed trust based on network location.

Both private sectors and academia have adopted this shift from perimeter-based to zero trust-based security. Federal agencies, too, have been encouraged to embrace zero trust principles over the last decade, supported by initiatives like the Federal Information Security Modernization Act (FISMA), the Risk Management Framework (RMF), Federal Identity, Credential, and Access Management (FICAM), Trusted Internet Connections (TIC), and Continuous Diagnostics and Mitigation (CDM) programs.

These frameworks are designed to control data and resource access for authorized individuals only. Initially limited by technology, these programs focused on enforcing security at major control points within a network. With technological advances, however, agencies can now dynamically assess access requests with a more granular "need to access" approach, reducing risks from compromised accounts, network monitoring threats, and other vulnerabilities. [9, 11]

Zero Trust Basics

Zero trust (ZT) is a cybersecurity framework based on the idea that no user or device should be trusted by default, regardless of their location within or outside the network. This approach emphasizes constant validation of access requests, ensuring that only authorized individuals or systems are granted the permissions they need to perform specific tasks. Unlike traditional security models, which assume trust once a user or device is inside the network, zero trust requires verification for every attempt to access resources.

Traditional security measures, such as firewalls and perimeter defenses, are designed to block external threats but are less effective at preventing breaches from internal or cloud-based sources. Zero trust addresses this challenge by applying the same level of scrutiny to all network interactions, whether they originate from within the organization or from remote users and devices.

At its core, zero trust aims to minimize risks by strictly controlling access based on identity and need. Every request for access is subject to verification, ensuring that only those with the proper credentials and authorization can interact with the network. This helps protect sensitive resources from unauthorized access, even in the event of a compromised account or system.

By shifting away from perimeter-based security and focusing on resource access, zero trust helps organizations ensure that security is maintained across all aspects of their infrastructure. It not only protects data but also secures devices, applications, and cloud environments, applying the principle of least privilege at every level of the enterprise[12, 15].

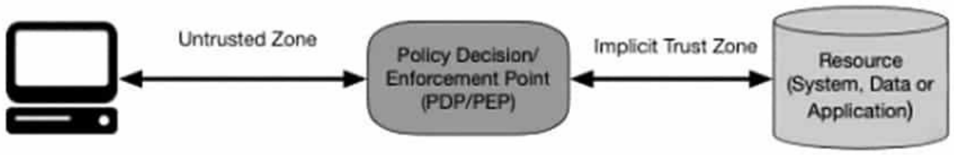
Untrusted Zone
Policy Decision/ Enforcement Point (PDP/PEP)
Implicit Trust Zone
Resource (System, Data or Application)

Figure 1: Zero Trust Access

Figure 1. Zero Trust Basics[15]

The framework should check the personality of the subject and approve the solicitation to decide whether admittance to the asset ought to be conceded. The Arrangement Choice Point (PDP) and Strategy Implementation Point (Enthusiasm) cooperate to evaluate what is happening and go with an educated choice in regards to get to. Zero trust standards basically center around two key regions: validation and approval. Key inquiries that should be considered include: How sure would we say we are in the character of the subject making the solicitation? Considering this certainty, ought to admittance to the asset be allowed? Is the gadget used to make the solicitation adequately secure? Should different variables, like the hour of solicitation, the subject's area, or the security stance of the subject, be considered to change the degree of certainty?

Ventures should create and keep up with adaptable, risk-based approaches that administer asset access and guarantee these strategies are authorized reliably for each entrance demand. This implies that an endeavor shouldn't work with the understanding that once a subject has been confirmed at a base level, all resulting demands for asset access are naturally substantial. All things considered, each solicitation ought to be assessed on its own benefits in light of the ongoing setting and security act.

An illustration of an "certain trust zone" can be drawn from air terminal security. When travelers go through a security designated spot (going about as the PDP/Enthusiasm), they are conceded admittance to specific regions, similar to the boarding entryways, and are verifiably trusted inside that space. In any case, this trust isn't programmed for all areas or circumstances, and proceeded with examination is applied to guarantee that all people are considered for access in light of their confirmed certifications, guaranteeing that no region or substance inside the framework is trusted naturally without legitimate approval. [16, 18]

A Zero Trust View of a Network

While carrying out Zero Trust Engineering (ZTA), a few critical presumptions about network should be thought of. These suppositions assist with molding the development of a ZTA, directing both endeavor possessed foundation and assets that work on outside, nonenterprise-claimed networks, (for example, public Wi-Fi or cloud administrations). The accompanying suppositions ought to be consolidated in network arranging and sending for ZTA:

1. The endeavor's confidential organization isn't consequently trusted. It is fundamental to accept that an aggressor

could be available inside the organization. Subsequently, all associations ought to be validated, and all correspondence ought to be scrambled to guarantee security, in accordance with the ZTA standards.

2. Gadgets interfacing with the organization may not be claimed or constrained by the endeavor.This incorporates situations where guests or project workers need admittance to play out their obligations. Bring-your-own-gadget (BYOD) strategies are a typical model, where venture clients access organization assets utilizing individual gadgets that may not be completely overseen by the endeavor.

3. No asset ought to be relied upon of course. Every resource should go through a security act assessment by means of a Strategy Requirement Point (Energy) before any solicitation to get to a venture asset is approved. This assessment ought to go on however long the meeting might last. For big business claimed gadgets, extra security relics can give a higher certainty level, yet subject qualifications alone are inadequate for gadget verification.

4. Endeavor assets may not necessarily live on big business claimed foundation. Assets could incorporate distant workers and cloud-based administrations. Indeed, even undertaking possessed gadgets might have to interface with nonenterprise networks for essential administrations like DNS goal or organization availability[19].

5. Distant endeavor clients and gadgets can't completely believe the neighborhood network they interface with. This incorporates networks beyond the undertaking, like those out in the open spots or outside specialist co-ops. All traffic ought to be thought to be helpless against observing or adjustment. Thusly,

remote access ought to constantly be confirmed and approved, with interchanges being gotten to safeguard secrecy, honesty, and source genuineness.

6. The security strategy and stance of resources ought to stay steady whether or not they are inside big business foundation or outer conditions. Gadgets and responsibilities ought to hold their security pose while progressing among big business and nonenterprise networks, guaranteeing constant insurance whether resources are on a neighborhood organization, far off gadgets, or cloud-based administrations.

These suspicions assist with guaranteeing a hearty security procedure is carried out while making arrangements for ZTA, upgrading the insurance of assets and guaranteeing consistence across various framework types. [20]

Logical Components of Zero Trust Architecture

There are numerous logical components that make up a ZTA deployment in an enterprise. These components may be operated as an on-premises service or through a cloud-based service. The conceptual framework model inshows the basic relationship between the components and their interactions. Note that this is an ideal model showing logical components and their interactions. From Figure 1, the policy decision point (PDP) is broken down into two logical components: the policy engine and policy administrator (defined below). The ZTA logical components use a separate control plane to communicate, while application data is communicated on a data plane.[21]

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

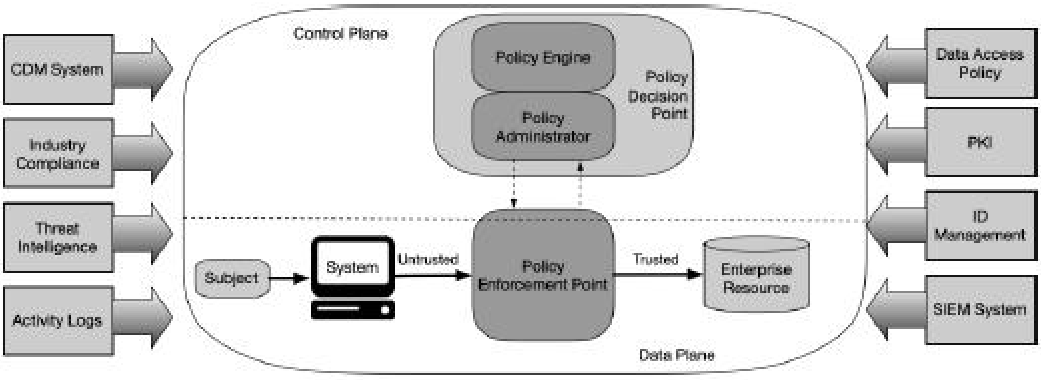

Figure 2. Components of Zero Trust Architecture[21]

Here is a reworded form of the part depictions to keep away from counterfeiting:

Strategy Motor (PE): The Approach Motor is liable for going with the last choice in regards to whether a subject ought to be conceded admittance to a particular asset. It assesses undertaking strategies and thinks about input from outside sources (like Persistent Diagnostics and Moderation (CDM) frameworks and danger insight administrations) as a feature of a trust assessment process. In light of this assessment, the PE decides if access ought to be conceded, denied, or disavowed. The choice is then logged. The PE works couple with the Approach Executive to carry out this choice.

Strategy Manager (PA): The Arrangement Executive deals with the foundation or end of correspondence ways among subjects and assets, interfacing with the pertinent Approach Requirement Focuses (PEPs) to do these assignments. It produces meeting explicit validation tokens or qualifications for the subject to get to big business assets. The Dad relies upon the PE's choice to either permit or deny a meeting. Assuming the meeting is approved and validated, the Dad designs the Enthusiasm to start the meeting. On the off chance that entrance is denied, or a formerly conceded meeting is renounced, the Dad flags the Enthusiasm to end the association. In certain frameworks, the PE and Dad might be treated as a bound together help, however here they are depicted independently. [21]

Policy Enforcement Point (PEP): This system is responsible for enabling, monitoring,and eventually terminating connections between a subject and an enterprise resource.The PEP communicates with the PA to forward requests and/or receive policy updates from the PA. This is a single logical component in ZTA but may be broken into two different components: the client(e.g., agent on a laptop) and resource side (e.g., gateway component in front of resource that controls access) or a single portal component that acts as a gatekeeper for communication paths. Beyond the PEP is the trust zone (see Section 2) hosting the enterprise resource.

In addition to the core components in an enterprise implementing a ZTA, several data sources provide input and policy rules used by the policy engine when making access decisions. Theseinclude local data sources as well as external (i.e., non enterprise-controlled or-created) data sources. These can include:

Continuous Diagnostics and Mitigation (CDM) System: This gathers information about the enterprise asset's current state and applies updates to configuration and software components. An enterprise CDM system provides the policy engine with the information about the asset making an access request, such as whether it is running the appropriate patched operating system (OS), the integrity of enterprise-approved software components or presence of non-approved components and whether the asset has any known vulnerabilities. CDM systems are also responsible for identifying and potentially enforcing a subset of polices on non enterprise devices active on enterprise infrastructure[22].

•**Industry Compliance System:** This ensures thatthe enterprise remains compliant withany regulatory regimethat it may fall under (e.g., FISMA, healthcare orfinancialindustryinformation security requirements). This includes all the policyrules that anenterprise develops to ensure compliance.

•**Threatintelligence Feed(s):**This provides information from internal or external sources that help the policy engine make access decisions. These could be multiple services that take data from internal and/or multiple external sources and provide information about newly discovered attacks or vulner abilities. This also includes newly discovered flaws in software, newly identified malware,and reported attacks to other assets that the policy engine will want to deny access to from enterprise assets.

•**Network and System Activity Logs:**This enterprise system aggregates asset logs, network traffic, resource access actions, and other events that provide real-time (or near-real-time) feedback on the security posture of enterprise information systems.

•**Data Accesspolicies:**These are the attributes, rules, and policies about access to enterprise resources. This set of rules could be encoded in (via management interface) ordynamically generated by the policy engine. These policies are the starting point forauthorizing access to a resource as they provide the basic access privileges for accounts and applications/services in the enterprise. These policies should be based on the defined mission roles and needs of the organization [23, 25].

ZTA using Network Infrastructure and Software Defined Parameters

Here's a rephrased version of the paragraph to avoid plagiarism:

The final method utilizes the network infrastructure to implement a Zero Trust Architecture (ZTA). This can be achieved through the use of an overlay network, which can operate at Layer 7, or even lower layers of the OSI model. Such strategies are often known as Software Defined Perimeter (SDP) solutions and may incorporate elements from Software Defined Networking (SDN) and intent-based networking (IBN). In this setup, the Policy Administrator (PA) functions as the network controller, dynamically adjusting the network configuration based on the decisions made by the Policy Engine (PE). Clients continue to initiate access requests through Policy Enforcement Points (PEPs), which are managed by the PA.

When implemented at the application network layer (Layer 7), the most typical deployment model involves an agent/gateway configuration .In this model, both the agent and the resource gateway, acting as a single PEP and configured by the PA, establish a secure communication channel between the client and the resource. Variations of this approach may also exist, such as those used in cloud virtual networks or non-IP networks[26].

Trust Algorithm Variation

Here's a rephrased version to eliminate plagiarism:

There are various approaches to implementing a Trust Algorithm (TA), and implementers may prioritize different factors based on their specific needs. Two key aspects differentiate these TAs: how the factors are evaluated and how requests are assessed in comparison to other requests made by the same subject, application/service, or device.

Criteria-based vs. Score-based: A criteria-based TA requires that a set of specific attributes be met before access to a resource or the execution of an action (e.g., read/write) is granted. These criteria are defined by the enterprise and must be individually configured for each resource. Access or actions are only allowed if all criteria are met. In contrast, a score-based TA calculates a confidence level based on values from multiple data sources and enterprise-defined weights. If the score surpasses a predefined threshold for the resource, access is granted or the action is performed; otherwise, the request is denied or privileges are limited (e.g., only read access granted, but not write access) [26, 28].

Singular vs. Contextual: A singular TA evaluates each request independently, without considering the subject's history. While this approach may enable quicker evaluations, it may miss detecting attacks that fall within the subject’s allowed role. On the other hand, a contextual TA factors in the recent history of the subject or network agent when assessing access requests. This approach requires the Policy Engine (PE) to maintain state information on all subjects and applications, increasing its chances of detecting anomalous behavior that could indicate an attack. A contextual TA may be more likely to identify an attacker using compromised credentials if the access patterns deviate from normal behavior. This method also requires the PE to be informed about user actions by the Policy Administrator (PA) and the Policy Enforcement Points (PEPs) involved in communications.

These factors can be independent. For instance, a TA can assign confidence levels to each subject or device but still evaluate every access request individually (i.e., singular). However, contextual, score-based TAs offer more dynamic and detailed access control, as the score reflects the current confidence level of the subject’s request and adapts to changing conditions faster than static, manually adjusted policies[28, 29].

Ideally, a ZTA would implement a contextual TA, although this may not always be feasible depending on the available infrastructure components. Contextual TAs can help detect attacks where the compromised subject account remains within a "normal" pattern of access requests, such as in cases of insider threats or subtle external intrusions. However, balancing security with user convenience and cost-efficiency is crucial. Requiring subjects to frequently reauthenticate based on their historical behavior could create usability challenges. For example, if an HR employee typically accesses 20–30 records daily, a contextual TA could flag as suspicious an attempt to access over 100 records in one day or any access after business hours, which may suggest data exfiltration by an attacker using a compromised HR account.

In another scenario, a financial system accessed by an accountant during normal hours might trigger a contextual TA if the system is accessed late at night from an unusual location. This could trigger an alert and require a higher confidence level for authentication, as specified in NIST Special Publication 800-63A.

Establishing the criteria or thresholds for each resource demands careful planning and testing. During the initial stages of ZTA implementation, administrators may encounter situations where legitimate access requests are incorrectly denied due to misconfiguration. This often leads to a "tuning" phase, where criteria or scoring weights are adjusted to ensure policies are enforced without disrupting business operations. The duration of this phase depends on the enterprise's tolerance for access denials or approvals during the tuning period and the metrics set for evaluating progress[29].

Network/Environment Components

Here is a reworded rendition of your text to eliminate literary theft:

In a Zero Trust (ZT) climate, it's essential to keep a distance — either consistent or perhaps physical — between the correspondence streams that are liable for controlling and designing the organization and the application/administration correspondence streams that handle the association's functional undertakings. This division is regularly ordered into a control plane for network the board and an information plane for application/administration correspondence streams.

The control plane is utilized by different foundation parts, whether venture possessed or from specialist co-ops, to oversee and design assets, approve or deny admittance to resources, and lay out correspondence ways between assets. The data plane, then again, is devoted to the real correspondence between programming parts. A correspondence way may not be laid out in the information plane until it has been set up through the control plane. For instance, the control plane could be utilized by the Strategy Head (Dad) and Strategy Requirement Focuses (PEPs) to make a protected correspondence way between the client and the venture asset, after which the information plane is utilized to do the responsibility[30].

Network Prerequisites for Supporting ZTA

Basic Organization Availability for Assets: Endeavor resources ought to have fundamental network, normally given by the neighborhood (LAN), which can be either venture controlled or not. This organization gives fundamental foundation administrations, like DNS, albeit far off resources may not depend on every one of the accessible administrations.

Distinguishing Venture Claimed Assets: The undertaking should have the capacity to separate between its own resources and others, in view of the security stance of the gadgets. This should be possible utilizing venture gave qualifications and approved data, as opposed to depending on information like spoofable organization Macintosh addresses.

Observation of Organization Traffic: The undertaking should have the option to screen network traffic on the information plane. Albeit full application layer review (OSI Layer 7) everything being equal, may not generally be imaginable, the venture should have the option to channel metadata (e.g., objective, time, gadget character) to refresh security approaches powerfully and illuminate the Strategy Motor (PE) for access independent direction.

Controlled Asset Access: Endeavor assets ought not be open straightforwardly from the web. Assets just acknowledge associations that have been pre-designed and verified through the Kick. These associations ought to be set up after appropriate validation, guaranteeing that assailants can't perform network sweeps or start DoS assaults. Some organization parts, like DNS servers, may have to stay open.

Separation of Information and Control Planes: The information plane and the control plane ought to remain sensibly isolated. The

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X
SES

correspondence between the PE, Dad, and PEPs occurs over the control plane, while the information plane is utilized solely for application or administration traffic. The PEPs should have the option to cooperate with the two planes.

Access to the PEP: Endeavor resources ought to have the option to arrive at the Kick to get sufficiently close to assets. This can be accomplished through an online interface, network gadget, or programming specialist introduced on the endeavor resource that works with the association.

PEP's Job in Business Flows: Just the Enthusiasm can collaborate with the Dad to lay out correspondence ways. All traffic related with business processes should go through at least one PEPs on the undertaking organization.

Remote Admittance to Resources: Distant endeavor resources ought to have the option to get to big business assets straightforwardly, without expecting to cross the venture's organization foundation. For example, far off clients ought to have the option to get to cloud-facilitated endeavor administrations, like email, without steering through a VPN.

Scalability for ZTA Components: The foundation that upholds the ZTA dynamic cycle ought to be adaptable to deal with shifting burdens. The PE, Dad, and Enthusiasm parts are pivotal for business tasks, and deferrals or disappointments in these parts can upset work processes. Undertakings should arrangement these parts to satisfy expected need or scale rapidly depending on the situation.

Policy-Based Restrictions: There might be arrangements keeping specific resources from getting to specific PEPs. For instance, cell phones situated external the undertaking's assigned nation may be confined from getting to explicit assets, in view of area, gadget type, or different standards[31, 33].

Deployment Scenarios/Use Cases

Any association can be organized utilizing Zero Trust standards. Many ventures currently consolidate specific parts of No Confidence in their foundation or are effectively making progress toward taking on data security and flexibility strategies alongside best practices. There are different sending situations and use situations where Zero Trust Engineering (ZTA) can be actually applied. ZTA, specifically, has been gotten from conditions with circulated associations or a labor force that is profoundly versatile. In any case, even associations without these attributes can get benefits from executing Zero Trust.

The utilization cases portrayed beneath don't unequivocally name their frameworks as ZTA, as the association is possible working with a blend of conventional border based security and Zero Trust parts. As noted before, it is normal for ventures to have both ZTA parts and customary edge based network foundation running in lined up during the change time frame[33, 34].

Undertaking with Satellite Areas

A typical situation includes an organization with a focal base camp and at least one far off workplaces or areas, which don't have a direct actual association with the organization's fundamental organization (see Figure 8). Representatives at these far off areas frequently miss the mark on full venture possessed neighborhood network yet expect admittance to basic endeavor assets. The organization could have a MPLS (Multiprotocol Mark Exchanging) interface associating the distant office to the HQ organization, however this association may not offer sufficient transmission capacity for all information traffic or probably won't be great for steering traffic to cloud-based administrations. Furthermore, representatives who are working from a distance or working from home might be utilizing individual or organization claimed gadgets. In such cases, the association might need to give admittance to specific assets (like email or representative schedules) while confining or restricting admittance to additional delicate frameworks (like the HR data set).

For this utilization case, the Approach Motor (PE) and Strategy Chairman (Dad) are regularly facilitated as cloud administrations, giving better accessibility and guaranteeing that telecommuters don't need to depend on the venture foundation to get to cloud-facilitated assets. Endpoints in this situation could utilize specialists (as portrayed in Segment) or access an asset entryway (as depicted in Area). Facilitating the PE/Dad parts on the undertaking neighborhood organization could be less proficient, as it would require distant workplaces and laborers to course their traffic through the base camp, particularly to get to cloud-facilitated applications and administrations[35].

This reworded adaptation keeps the first importance in one piece while guaranteeing uniqueness.

Spectrum of Engineering Sciences
Online ISSN
3007-3138
Print ISSN
3007-312X
SPECTRUM OF ENGINEERING SCIENCES

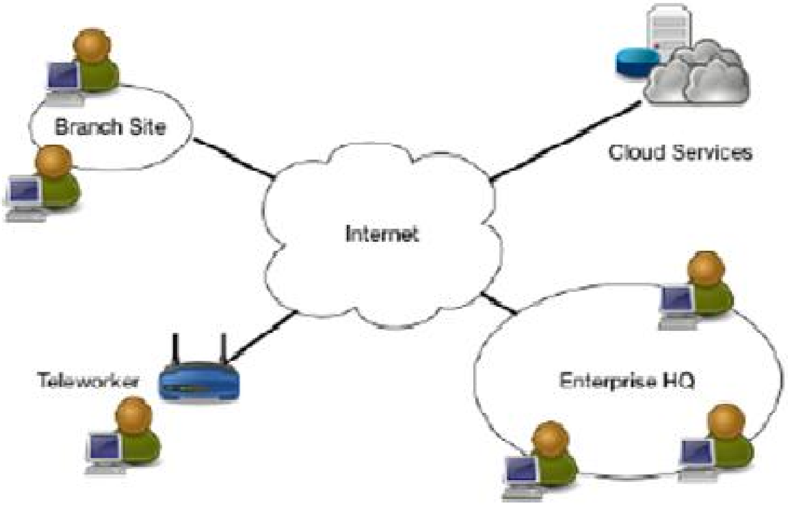

Figure 3. Undertaking with Satellite Areas[35]

Collaboration Across Enterprise Boundaries

A fourth use case is cross-enterprise collaboration. For example, there is a project involving employees from Enterprise A and Enterprise B (see Figure 11). The two enterprises may be separate federal agencies (G2G) or even a federal agency and a private enterprise (G2B). Enterprise A operates the database used for the project but must allow access to the data for certain members of Enterprise B. Enterprise A can set up specialized accounts for the employees of Enterprise B to access the required data and deny access to all other resources, but this can quickly become difficult to manage. Having both organizations enrolled in a federated ID management system would allow quicker establishment of these relationships provided that both organizations' PEPs can authenticate subjects in a federated ID community[36].

This scenario can be similar to Use Case 1 as employees of both enterprises may not located on their organizations' network infrastructures, and the resource they need to access may be within one enterprise environment or hosted in the cloud. This means

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN 3007-3138
Print ISSN 3007-312X

that there do not need to be complex firewall rules or enterprise-wide access control lists (ACLs) allowing certain IP addresses belonging to Enterprise B to access resources in Enterprise A based on Enterprise A's access policies. How this access is accomplished depends on the technology in use. Similar to Use Case 1, a PE and PA hosted as a cloud service may provide availability to all parties without having to establish a VPN or similar. The employees of Enterprise B may be asked to install a software agent on their asset or access the necessary data resources through a web gateway[37].

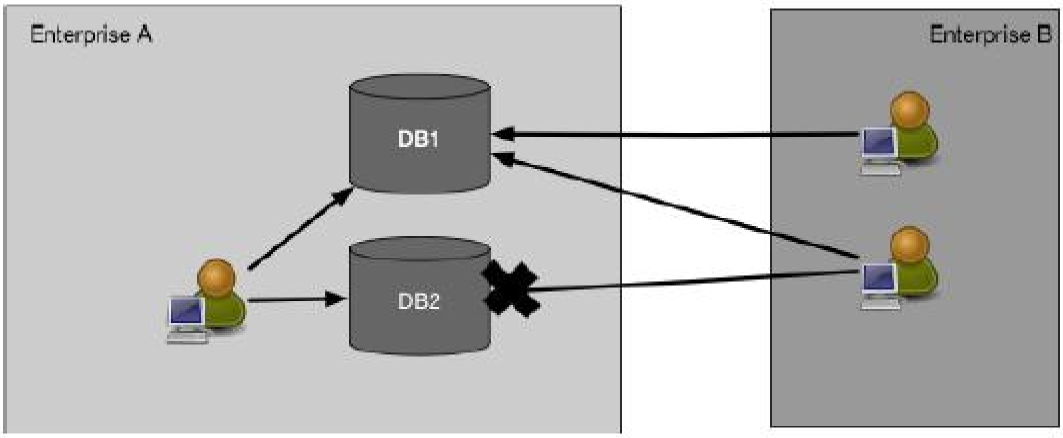

Figure 11: Cross-Enterprise Collaboration

Figure 4. Collaboration Across Enterprise Boundaries[36]

Visibility on the Network

As mentioned in Section 3.4.1, all traffic is inspected and logged on the network and analyzed to identify and react to potential attacks against the enterprise. However, as also mentioned, some (possibly the majority) of the traffic on the enterprise network may be opaque to layer 3 network analysis tools. This traffic may originate from nonenterprise-owned assets (e.g., contracted services that use the enterprise infrastructure to access the internet) or applications/services that are resistant to passive monitoring. The enterprise that cannot perform deep packet inspection or examine the encrypted traffic and must use other methods to assess a possible attacker on the network.

That does not mean that the enterprise is unable to analyze encrypted traffic that it sees on the network. The enterprise can collect metadata (e.g., source and destination addresses, etc.) about the encrypted traffic and use that to detect an active attacker or possible malware communicating on the network. Machine learning techniques [Anderson] can be used to analyze traffic that cannot be decrypted and examined. Employing this type of machine learning would allow the enterprise to categorize traffic as valid or possibly malicious and subject to remediation.

Storage of System and Network Information

A related threat to enterprise monitoring and analysis of network traffic is the analysis component itself. If monitor scans, network traffic, and metadata are being stored for building contextual policies, forensics, or later analysis, that data becomes a target for attackers. Just like network diagrams, configuration files, and other assorted network architecture documents, these resources should be protected. If an attacker can successfully gain access to this information, they may be able to gain insight into the enterprise architecture and identify assets for further reconnaissance and attack.

Another source of reconnaissance information for an attacker in a ZT enterprise is the management tool used to encode access policies. Like stored traffic, this component contains access policies to resources and can give an attacker information on which accounts are most valuable to compromise (e.g., the ones that have access to the desired data resources).

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN 3007-3138
Print ISSN 3007-312X

As for all valuable enterprise data, adequate protections should be in place to prevent unauthorized access and access attempts. As these resources are vital to security, they should have the most restrictive access policies and be accessible only from designated or dedicated administrator accounts[38,39].

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] Y. A. Khan, U. Khalil, H. Khan, A. Uddin, S. Ahmed, "Power flow control by unified power flow controller",sss Engineering, Technology & Applied Science Research., vol. 9, no. 2, pp. 3900-3904, Feb. 2019

[2] Aburomman, A. A., &Reaz, M. B. I. (2017). A survey of intrusion detection systems based on ensemble and hybrid classifiers.Computers & Security,65, 135-152.

[3] Chawla, N. V., & Zheng, A. X. (2021). Deepfakes: A security and privacy perspective. *IEEE Transactions on Neural Networks and Learning Systems*, 32(5), 1234–1247.

[4] Floridi, L. (2018). Artificial intelligence as a public policy issue. *Philosophy & Technology*, 31(4), 639–648.

[5] Kietzmann, J., McCarthy, I., & Silvestri, L. (2020). Deepfakes: Trick or treat? *Business Horizons*, 63(2), 135–146.

[6] Westerlund, M. (2019). The emergence of deepfake technology: A review. *Technology Innovation Management Review*, 9(11), 39–52.

[7] Agrawal, S., & Agrawal, J. (2015). Survey on anomaly detection using data mining techniques.Procedia Computer Science,60, 708-713.

[8] Ahmad, S., Lavin, A., Purdy, S., & Agha, Z. (2017). Unsupervised real-time anomaly detection for streaming data.Neurocomputing,262, 134-147.

[9] Akhi, A. B., Kanon, E. J., Kabir, A., &Banu, A. (2019).Network Intrusion Classification Employing Machine Learning: A Survey. (Doctoral dissertation)Department of Computer Science and Engineering, United International University, Bangladesh.

[10] Alizadeh, H., Khoshrou, A., &Zuquete, A. (2015). Traffic classification and verification using unsupervised learning of Gaussian Mixture Models. In2015 IEEE international workshop on measurements & networking (M&N). 1-6. IEEE. Khan, I. Uddin, A. Ali, M. Husain, "An Optimal DPM Based Energy-Aware Task Scheduling for Performance Enhancement in Embedded MPSoC", Computers, Materials & Continua., vol. 74, no. 1, pp. 2097-2113, Sep. 2023

[11] S. Khan, I. Ullah, H. Khan, F. U. Rahman, M. U. Rahman, M. A. Saleem, A. Ullah, "Green synthesis of AgNPs from leaves extract of Salvia Sclarea, their characterization, antibacterial activity, and catalytic reduction ability", Zeitschrift für Physikalische Chemie., vol. 238, no. 5, pp. 931-947, May. 2024

[12] H. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, "Offline Earliest Deadline first Scheduling based Technique for Optimization of Energy using STORM in Homogeneous Multi-core Systems", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 125-130, Dec. 2018

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X
SES

[13] Waleed, A. Ali, S. Tariq, G. Mustafa, H. Sarwar, S. Saif, I. Uddin, "An Efficient Artificial Intelligence (AI) and Internet of Things (IoT's) Based MEAN Stack Technology Applications", Bulletin of Business and Economics (BBE)., vol. 13, no. 2, pp. 200-206, July. 2024

[14] Noor, A. Ilyas, Z. Javaid, H. Khan, "Framing a Knowledge Domain Visualization on Green Human Resource Management: A Bibliometric Analysis from 2008-2022", Pakistan Journal of Humanities and Social Sciences., vol. 11, no. 4, pp. 4200-4212, Aug. 2023

[15] M. Gondal, Z. Hameed, M. U. Shah, H. Khan, "Cavitation phenomenon and its effects in Francis turbines and amassed adeptness of hydel power plant", In 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-9, Mar. 2019

[16] U. Hashmi, S. A. ZeeshanNajam, "Thermal-Aware Real-Time Task Schedulabilty test for Energy and Power System Optimization using Homogeneous Cache Hierarchy of Multi-core Systems", Journal of Mechanics of Continua and Mathematical Sciences., vol. 14, no. 4, pp. 442-452, Mar. 2023

[17] Y. A. Khan, F. Khan, H. Khan, S. Ahmed, M. Ahmad, "Design and Analysis of Maximum Power Point Tracking (MPPT) Controller for PV System", Journal of Mechanics of Continua and Mathematical Sciences., vol. 14, no. 1, pp. 276-288, May. 2019

[18] Khan, A. Yasmeen, S. Jan, U. Hashmi, "ENHANCED RESOURCE LEVELING INDYNAMIC POWER MANAGEMENT TECHNIQUEOF IMPROVEMENT IN PERFORMANCE FOR MULTI-CORE PROCESSORS" ,Journal of Mechanics of Continua and Mathematical Sciences., vol. 6, no. 14, pp 956-972, Sep. 2019

[19] Khan, Q. Bashir, M. U. Hashmi, "Scheduling based energy optimization technique in multiprocessor embedded systems", In 2018 International Conference on Engineering and Emerging Technologies (ICEET), IEEE., pp. 1-8, Sep. 2018

[20] Y. A. Khan, M. Ibrahim, M. Ali, H. Khan, E. Mustafa, "Cost Benefit Based Analytical Study of Automatic Meter Reading (AMR) and Blind Meter Reading (BMR) used by PESCO (WAPDA)", In 2020 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-7, Aug. 2020

[21] Naz, H. Khan, I. Ud Din, A. Ali, and M. Husain, "An Efficient Optimization System for Early Breast Cancer Diagnosis based on Internet of Medical Things and Deep Learning", Eng. Technol. Appl. Sci. Res., vol. 14, no. 4, pp. 15957–15962, Aug. 2024

[22] Khan, I. Ullah, M. U. Rahman, H. Khan, A. B. Shah, R. H. Althomali, M. M. Rahman, "Inorganic-polymer composite electrolytes: basics, fabrications, challenges and future perspectives", Reviews in Inorganic Chemistry., vol. 44, no. 3, pp. 1-2, Jan. 2024

[23] Khan, M. U. Hashmi, Z. Khan, R. Ahmad, "Offline Earliest Deadline first Scheduling based Technique for Optimization of Energy using STORM in Homogeneous Multi-core Systems", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 125-130, Oct. 2018

[24] M. S. Abdul Razak, S. P. A. Gothandapani, N. Kamal, and K. Chellappan, "Presenting the Secure Collapsible Makerspace with Biometric Authentication", Eng. Technol. Appl. Sci. Res., vol. 14, no. 1, pp. 12880–12886, Feb. 2024.

[25] H. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, A. Saleem, "Performance Evaluation for Secure DES-Algorithm Based

Authentication & Counter Measures for Internet Mobile Host Protocol", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 181-185, July. 2018

[26] Amangele, P., Reed, M. J., Al-Naday, M., Thomos, N., & Nowak, M. (2019). Hierarchical Machine Learning for IoT Anomaly Detection in SDN. In2019 International Conference on Information Technologies (InfoTech). 1-4. IEEE.

[27] Anderson, J. P. (1980). Computer security threat monitoring and surveillance.Technical Report, Fort Washington, PA, James P. Anderson Co.

[28] Aung, Y. Y., & Min, M. M (2018). An analysis of K-means algorithm based network intrusion detection system. Advances in Science, Technology and Engineering Systems Journal,3(1), 496-501. Bauer, F. C., Muir, D. R., &Indiveri, G (2019). Real-Time Ultra-Low Power ECG Anomaly Detection

[29] Bhati, B. S., Rai, C. S., Balamurugan, B., & Al-Turjman, F. (2020). An intrusion detection scheme based on the ensemble of discriminant classifiers.Computers & Electrical Engineering,86, 106742.

[30] Bhattacharyya, D. K., &Kalita, J. K. (2013).Network anomaly detection: A machine learning perspective. CRCPress.

[31] Khan, A. Ali, S. Alshmrany, "Energy-Efficient Scheduling Based on Task Migration Policy Using DPM for Homogeneous MPSoCs", Computers, Materials & Continua., vol. 74, no. 1, pp. 965-981, Apr. 2023

[32] Shah, S. Ahmed, K. Saeed, M. Junaid, H. Khan, "Penetration testing active reconnaissance phase–optimized port scanning with nmap tool", In 2019 2nd International Conference on Computing,

Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-6, Nov. 2019

[33] Y. A. Khan, "A GSM based Resource Allocation technique to control Autonomous Robotic Glove for Spinal Cord Implant paralysed Patients using Flex Sensors", Sukkur IBA Journal of Emerging Technologies., vol. 3, no. 2, pp. 13-23, Feb. 2020

[34] Y. A. Khan, "A high state of modular transistor on a 105 kW HVPS for X-rays tomography Applications", Sukkur IBA Journal of Emerging Technologies., vol. 2, no. 2, pp. 1-6, Jun. 2019

[35] Khan, S. Ahmad, N. Saleem, M. U. Hashmi, Q. Bashir, "Scheduling Based Dynamic Power Management Technique for offline Optimization of Energy in Multi Core Processors", Int. J. Sci. Eng. Res., vol. 9, no. 12, pp. 6-10, Dec. 2018

[36] Y. A. Khan, "Enhancing Energy Efficiency in Temperature Controlled Dynamic Scheduling Technique for Multi Processing System on Chip", Sukkur IBA Journal of Emerging Technologies., vol. 2, no. 2, pp. 46-53, Jan. 2019

[37] Khan, K. Janjua, A. Sikandar, M. W. Qazi, Z. Hameed, "An Efficient Scheduling based cloud computing technique using virtual Machine Resource Allocation for efficient resource utilization of Servers", In 2020 International Conference on Engineering and Emerging Technologies (ICEET), IEEE., pp. 1-7, Apr. 2020

[38] Hassan, H. Khan, I. Uddin, A. Sajid, "Optimal Emerging trends of Deep Learning Technique for Detection based on Convolutional Neural Network", Bulletin of Business and Economics (BBE)., vol. 12, no. 4, pp. 264-273, Nov. 2023

[39] Sarwar, H. Khan, I. Uddin, R. Waleed, S. Tariq, "An Efficient E-Commerce Web Platform Based on Deep Integration of MEAN

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

Stack Technologies", Bulletin of Business and Economics (BBE)., vol. 12, no. 4, pp. 447-453, Jun. 2023