Zero Trust Architecture and Identity Threat Detection for Securing Cloud, IoT, and Hybrid Enterprise Systems

(Author Details)
Santosh Kumar Jadala
Cyber Security & Business Analysis Specialist
Independent Researcher

Abstract

Modern enterprise security has become more complex as organizations increasingly depend on cloud platforms, Internet of Things devices, hybrid networks, remote users, application programming interfaces, and third-party digital services. These developments have made traditional perimeter-based security less effective, since users, devices, applications, and workloads now operate across distributed environments that cannot be protected by a fixed network boundary alone. Zero Trust Architecture provides a more suitable security approach by removing implicit trust and requiring every access request to be continuously verified based on identity, device status, access context, and risk level. Within this model, identity threat detection plays a central role because many cyberattacks now exploit valid credentials, excessive privileges, compromised accounts, insider access, and abnormal user behavior. By combining identity governance, risk-based authentication, least privilege access, anomaly detection, and continuous monitoring, organizations can improve their ability to detect unauthorized access, reduce lateral movement, and respond more effectively to emerging threats. This article examines the relationship between Zero Trust Architecture and identity threat detection in cloud, IoT, and hybrid enterprise systems. It also develops a conceptual framework for integrating Zero Trust principles with identity-centered security controls to strengthen enterprise cyber resilience.

Keywords: Zero Trust Architecture; Identity Threat Detection; Cloud Security; IoT Security; Hybrid Enterprise Systems; Access Control; Risk-Based Authentication; Cybersecurity; Continuous Monitoring; Identity Governance

DOI: 10.21590/ijhit.06.04.15

1. Introduction

Cybersecurity has moved far beyond the traditional idea of protecting a fixed network boundary. For many years, enterprise security was built around a perimeter-based model in which systems inside the organizational network were treated as relatively trusted, while external access was treated as risky. That model worked better when employees, applications, data, and devices were mainly located within controlled corporate environments. Today, that assumption is increasingly

difficult to defend. Organizations now depend on cloud platforms, Internet of Things (IoT) devices, remote work arrangements, mobile endpoints, third-party services, application programming interfaces, and hybrid infrastructure. As a result, users and workloads regularly operate outside conventional enterprise boundaries, and sensitive resources may be accessed from many locations, devices, and network paths.

This shift has made identity and context central to modern cybersecurity. Instead of relying mainly on whether a user or system is inside the network, security decisions now need to consider who is requesting access, what device is being used, what resource is being accessed, whether the behavior is normal, and whether the request matches organizational policy. In distributed environments, a user with valid credentials can become more dangerous than an unknown external actor, especially when those credentials are stolen, abused, or linked to excessive privileges. This is why modern cybersecurity increasingly treats identity as a critical control point rather than a simple login mechanism.

Zero Trust Architecture has emerged as a major response to this change. It is commonly associated with the principle of "never trust, always verify," which means that no user, device, application, workload, or network segment should be trusted automatically, even when it operates within the enterprise environment (Buck et al., 2021; Wylde, 2021). Zero Trust does not assume that internal access is safe. Instead, it requires continuous verification and policy-based decision-making before access is granted and while access is being maintained. This approach is especially important in cloud, IoT, and hybrid systems, where the network perimeter is difficult to define and where attackers may use legitimate credentials to move across systems.

The strength of Zero Trust lies in its use of layered and adaptive security controls. These include continuous identity verification, least privilege access, microsegmentation, device posture assessment, policy enforcement, and ongoing monitoring. Together, these controls reduce the risk of unauthorized access and limit the ability of attackers to move laterally after gaining access to one part of an enterprise system (Syed et al., 2022; Dhiman et al., 2024). In this sense, Zero Trust is not simply a technical product or a single security tool. It is a security architecture that changes how organizations think about trust, access, identity, and risk.

Identity threat detection is a key part of this model. Many modern cyberattacks exploit identity weaknesses rather than only technical vulnerabilities. Attackers may use stolen passwords, compromised accounts, weak authentication, excessive privileges, insider access, or poorly monitored service accounts to bypass traditional defenses. Once inside, they may appear to be legitimate users, making detection more difficult. Studies on insider threats and identity-related risks show that suspicious access patterns, abnormal behavior, and privilege misuse can provide important signals for detecting potential compromise (Gheyas & Abdallah, 2016; Dasu et al., 2023). Therefore, Zero Trust becomes more effective when it is combined with identity threat

detection methods such as risk-based authentication, anomaly detection, access monitoring, and behavioral analytics.

The aim of this article is to examine how Zero Trust Architecture and identity threat detection can be integrated to secure cloud, IoT, and hybrid enterprise systems. The article argues that effective enterprise security now depends on the ability to verify identities continuously, assess access risk in context, enforce least privilege, monitor behavior, and respond to suspicious activity across distributed environments. By connecting Zero Trust principles with identity-centered threat detection, organizations can develop a stronger and more practical approach to cyber resilience.

1.1 Problem Statement

The growing adoption of cloud computing, Internet of Things systems, remote work technologies, and hybrid enterprise networks has changed the structure of organizational cybersecurity. Many enterprise systems no longer operate within a clearly defined network boundary. Employees connect from different locations, applications run across public and private clouds, IoT devices communicate continuously with enterprise platforms, and third-party services often require access to internal resources. As a result, traditional perimeter-based security models have become less reliable because they were built around the assumption that systems inside the network could be trusted more than those outside it. In modern enterprise environments, this assumption creates serious security weaknesses.

Zero Trust Architecture has emerged as a response to this problem. Its central idea is that no user, device, application, workload, or network connection should be trusted automatically. Instead, every access request must be verified based on identity, device status, access context, risk level, and policy requirements. Existing studies show that Zero Trust can strengthen enterprise cybersecurity by reducing implicit trust, enforcing least privilege access, supporting continuous verification, and limiting lateral movement within networks (Buck et al., 2021; Syed et al., 2022). However, although many organizations recognize the importance of Zero Trust, actual implementation remains difficult. Zero Trust is not a single tool that can simply be installed. It requires changes in identity management, access control, network segmentation, monitoring, governance, and organizational security maturity (Phiayura & Teerakanok, 2023; Yeoh et al., 2023).

One of the most difficult areas is identity-centered security. In cloud, IoT, and hybrid enterprise systems, identity is no longer limited to human users. It now includes administrators, contractors, service accounts, APIs, workloads, connected devices, and machine identities. Each of these identities can become a target for attackers if it is poorly managed or overprivileged. Weak authentication, excessive permissions, poor account monitoring, fragmented identity systems, and limited visibility into user behavior can allow attackers to gain access using valid

credentials. Once access is obtained, the attacker may appear legitimate, making detection more difficult. This is why identity threat detection has become a critical part of modern cybersecurity.

Despite this need, many organizations still treat identity governance and threat detection as separate functions. Identity and access management systems may handle authentication and authorization, while security information and event management tools may collect logs and detect suspicious activities. However, when these systems are not properly integrated, security teams may struggle to connect access decisions with behavioral risk indicators. This creates gaps in detecting credential misuse, privilege escalation, insider activity, unauthorized access, and abnormal user behavior. Dasu et al. (2023) emphasized the importance of risk-based authentication in defending against identity threats, while Gheyas and Abdallah (2016) showed that insider threat detection requires careful analysis of behavior, access patterns, and security events.

Cloud and IoT environments make this problem more complex. Cloud systems are often affected by insecure configurations, account hijacking, data leakage, weak access controls, and shared infrastructure risks (Hashizume et al., 2013; Tabrizchi & Kuchaki Rafsanjani, 2020). IoT systems also introduce risks because many devices have limited processing power, weak authentication mechanisms, long lifecycles, and poor patching support (Roman et al., 2013; Sicari et al., 2015). In hybrid enterprise systems, these risks become even more difficult to manage because security controls must work across on-premises infrastructure, cloud services, remote endpoints, IoT devices, and third-party platforms.

The central problem addressed in this article is that many organizations adopt Zero Trust principles at a general level but lack a clear and integrated framework for applying Zero Trust and identity threat detection together across cloud, IoT, and hybrid enterprise systems. Existing research has examined Zero Trust Architecture, access control, cloud security, IoT security, anomaly detection, and insider threat detection as important areas of cybersecurity. However, there remains a need for a structured framework that brings these areas together and explains how identity verification, access control, risk-based authentication, anomaly detection, SIEM monitoring, and continuous policy enforcement can operate as a unified security approach. Without this integration, Zero Trust implementation may remain incomplete, and organizations may continue to face identity-based attacks, privilege misuse, visibility gaps, and inconsistent access enforcement across distributed enterprise environments.

1.2 Research Aim

The aim of this article is to examine how Zero Trust Architecture and identity threat detection can be integrated to secure cloud, IoT, and hybrid enterprise systems. The article focuses on how identity-centered controls, continuous verification, least privilege access, risk-based

authentication, anomaly detection, and security monitoring can work together to reduce unauthorized access, detect suspicious behavior, and improve enterprise cyber resilience.

1.3 Research Objectives

The objectives of this article are as follows:

- To examine the limitations of traditional perimeter-based security in modern enterprise systems.
  This objective focuses on why older security models are no longer sufficient for organizations that rely on cloud platforms, IoT devices, remote access, APIs, and hybrid infrastructure. It considers how distributed systems have weakened the idea of a fixed security boundary and why modern organizations require more adaptive security models.
- To analyze the principles, implementation requirements, and maturity factors of Zero Trust Architecture.
  This objective examines the main principles of Zero Trust, including continuous verification, least privilege access, microsegmentation, device posture assessment, identity-based access control, and policy-based enforcement. It also considers the practical and organizational factors that influence Zero Trust adoption, including cost, governance, security culture, technical readiness, and maturity assessment (Adahman et al., 2022; Yeoh et al., 2023).
- To evaluate the role of identity threat detection in detecting credential misuse, privilege escalation, insider activity, and unauthorized access.
  This objective focuses on identity as a major security concern in modern enterprise systems. It examines how risk-based authentication, behavioral analytics, anomaly detection, SIEM monitoring, and insider threat detection can help organizations identify suspicious identity activity before it leads to wider compromise (Bhatt et al., 2014; Ahmed et al., 2016; Dasu et al., 2023).
- To examine the security challenges affecting cloud, IoT, and hybrid enterprise environments.
  This objective investigates the specific security risks associated with cloud platforms, IoT devices, and hybrid enterprise systems. It considers issues such as cloud misconfiguration, insecure APIs, weak IoT authentication, poor device visibility, fragmented policies, and the difficulty of maintaining consistent security controls across distributed environments (Hashizume et al., 2013; Sicari et al., 2015; Tabrizchi & Kuchaki Rafsanjani, 2020).
- To propose a conceptual framework that integrates Zero Trust Architecture with identity threat detection.
  This objective presents the main contribution of the article. The proposed framework will connect identity verification, access control, risk evaluation, anomaly detection, SIEM

monitoring, continuous policy enforcement, and governance into a single conceptual model for securing cloud, IoT, and hybrid enterprise systems.

3.4 Research Questions

This article is guided by the following research questions:

- How does Zero Trust Architecture improve security in cloud, IoT, and hybrid enterprise systems?
- What role does identity threat detection play in strengthening Zero Trust implementation?
- What identity-based threats are most relevant to modern enterprise systems?
- How can organizations integrate continuous verification, least privilege access, anomaly detection, and policy enforcement into a unified security framework?

2. Background and Literature Review

2.1 Evolution from Perimeter-Based Security to Zero Trust

Traditional cybersecurity models were largely designed around the protection of a defined network perimeter. Under this model, firewalls, intrusion prevention systems, virtual private networks, and internal network controls were used to separate trusted internal users from untrusted external actors. The weakness of this approach is that it depends heavily on the assumption that users and systems inside the network are safer than those outside it. In modern enterprise environments, this assumption is no longer reliable. Cloud adoption, mobile computing, remote work, IoT connectivity, and third-party integration have created systems that are widely distributed and constantly changing.

Zero Trust developed as a response to this breakdown of the traditional perimeter. Rather than granting trust based on network location, Zero Trust requires continuous validation of access requests. Every request is treated as potentially risky until it is verified through identity, device, context, policy, and behavior-based controls (Buck et al., 2021; Syed et al., 2022). This does not mean that every user is treated as malicious. Rather, it means that access is no longer granted simply because a user or device appears to be inside the organization's network.

The literature also makes clear that Zero Trust is not a single product that an organization can purchase and deploy instantly. It is a strategic architecture that requires changes in identity management, access control, policy enforcement, device posture assessment, network segmentation, monitoring, and governance (Phiayura & Teerakanok, 2023; Yeoh et al., 2023). This distinction is important because many organizations misunderstand Zero Trust as a technology upgrade rather than a broader security transformation. A mature Zero Trust approach requires organizations to understand their assets, classify users and devices, define access policies, monitor activity continuously, and improve controls over time.

2.2 Core Principles of Zero Trust Architecture

The core idea of Zero Trust is that trust should never be implicit. Access should be verified explicitly and repeatedly based on the sensitivity of the resource, the identity of the requester, the condition of the device, the access context, and the level of risk involved. Syed et al. (2022) describe Zero Trust Architecture as a security approach that reduces dependence on perimeter-based trust and focuses instead on continuous verification and controlled access. Similarly, Dhiman et al. (2024) emphasize that Zero Trust models rely on adaptive security decisions, network control, and ongoing monitoring to protect modern systems.

Several principles define Zero Trust Architecture. The first is explicit verification. Users, devices, applications, and workloads must be authenticated and authorized before access is granted. The second is least privilege access, which means that users and systems should receive only the minimum access needed to perform a legitimate task. The third is continuous monitoring, which ensures that access is not treated as permanently safe after login. The fourth is microsegmentation, which limits movement across systems by dividing networks and workloads into smaller controlled zones. The fifth is policy-based access control, which ensures that access decisions are guided by organizational rules, identity attributes, device status, and risk signals.

Zero Trust implementation also requires organizational maturity. It is not enough to introduce multi-factor authentication or restrict access to some systems. Organizations must also address governance, cost, security culture, implementation readiness, and long-term management. Adahman et al. (2022) note that cost-effectiveness and organizational security planning are important considerations when evaluating Zero Trust adoption. Yeoh et al. (2023) also highlight the importance of critical success factors and maturity assessment, showing that successful Zero Trust implementation depends on leadership, planning, technical capability, and continuous improvement. Therefore, Zero Trust should be treated as a staged security journey rather than a one-time deployment.

2.3 Identity as the New Security Perimeter

Identity has become one of the most important control points in modern cybersecurity. In the past, enterprise access was often associated with employees working from managed devices inside a corporate network. In cloud, IoT, and hybrid environments, access is much broader. It may involve remote workers, administrators, contractors, third-party partners, service accounts, APIs, machine identities, IoT devices, and cloud workloads. Each of these identities can become a pathway for unauthorized access if it is not properly managed.

Identity management provides the foundation for determining who or what is requesting access and whether that request should be allowed. Bertino and Takahashi (2010) explain that identity management involves the technologies and processes used to manage digital identities across systems. In a Zero Trust environment, this function becomes even more important because

access decisions depend heavily on reliable identity verification, authentication, authorization, and accountability.

Access control models also provide important foundations for Zero Trust. Role-based access control assigns permissions based on organizational roles, making it useful for managing access in structured enterprise settings (Sandhu et al., 1996). Attribute-based access control provides a more flexible approach by considering user attributes, resource attributes, environmental conditions, and access context (Jin et al., 2012). Both models remain relevant to Zero Trust because they support more disciplined and policy-driven access decisions. However, Zero Trust extends these ideas by requiring continuous evaluation rather than one-time authorization.

In modern enterprise systems, identity must also include non-human actors. APIs, IoT devices, service accounts, containers, and workloads often communicate with one another automatically. If these identities are overprivileged, poorly monitored, or weakly authenticated, they may create serious security gaps. This makes identity governance essential not only for human users but also for machines, devices, and automated services.

2.4 Identity Threat Detection and Risk-Based Authentication

Identity threat detection focuses on identifying suspicious, unauthorized, or risky identity-related activity. This includes unusual login behavior, impossible travel, credential misuse, privilege escalation, abnormal session activity, suspicious account creation, unauthorized access attempts, and unexpected use of administrative privileges. These activities are important because many attacks do not begin with obvious malware or direct system exploitation. Instead, attackers may first obtain valid credentials and then use them to access systems in ways that appear legitimate.

Risk-based authentication strengthens identity security by evaluating the risk level of an access attempt before deciding how to respond. For example, a login from a familiar device and location may be treated differently from a login from an unusual country, unknown device, or abnormal time of day. Dasu et al. (2023) show that risk-based authentication can help defend against identity threats by using contextual signals to improve access decisions. In a Zero Trust model, this is especially useful because access is not based only on a password or a single authentication event. It is based on the risk surrounding the request.

Identity threat detection is also closely connected to insider threat detection and anomaly detection. Insider threats may involve employees, contractors, administrators, or compromised legitimate users. Such threats are difficult to detect because the activity often appears to come from authorized accounts. Salem et al. (2008) emphasize that insider attacks require careful monitoring of user behavior and access activity. Gheyas and Abdallah (2016) also show that insider threat detection benefits from predictive and behavioral approaches, especially when organizations need to identify suspicious activity before major damage occurs.

Anomaly detection supports this process by identifying behavior that differs from normal patterns. Ahmed et al. (2016) explain that anomaly detection techniques are widely used to identify unusual activity in network and system environments. When applied to identity activity, anomaly detection can help identify suspicious login patterns, abnormal resource access, unexpected privilege use, and unusual data movement. However, it must be carefully managed because false positives can create alert fatigue and reduce the effectiveness of security teams.

2.5 Zero Trust in Cloud, IoT, and Hybrid Enterprise Systems

Zero Trust applies differently across cloud, IoT, and hybrid enterprise systems, but the central principle remains the same: access should be verified, limited, monitored, and adjusted based on risk. In cloud environments, organizations face risks such as misconfiguration, insecure APIs, shared infrastructure concerns, account hijacking, weak access management, and data leakage. Hashizume et al. (2013) identify several cloud security issues related to confidentiality, integrity, availability, and access control. Fernandes et al. (2014) also show that cloud environments introduce security challenges that require strong governance and technical controls. Tabrizchi and Kuchaki Rafsanjani (2020) further emphasize that cloud security threats require solutions involving identity management, encryption, secure configuration, and continuous monitoring.

In IoT environments, the challenge is different but equally serious. IoT systems often include large numbers of connected devices, many of which have limited processing power, weak authentication, poor patching support, insecure communication channels, or long operational lifecycles. Roman et al. (2013) explain that distributed IoT environments create major privacy and security challenges because devices are often deployed across open and uncontrolled settings. Sicari et al. (2015) also highlight the importance of security, privacy, and trust in IoT systems, while Mosenia and Jha (2016) show that IoT security must address device-level vulnerabilities, communication risks, and system-wide exposure. Machine learning and deep learning methods have also been studied for IoT security, especially for detecting attacks and abnormal device behavior (Al-Garadi et al., 2020).

Hybrid enterprise systems combine the complexity of both cloud and on-premises environments. They may include private data centers, public cloud services, SaaS applications, IoT endpoints, remote users, mobile devices, and third-party access. This makes consistent policy enforcement difficult. It also creates gaps in visibility, identity federation, monitoring, and incident response. Stergiou et al. (2018) show that secure integration of IoT and cloud computing requires careful attention to security, privacy, and communication controls. Tabrizchi and Kuchaki Rafsanjani (2020) also emphasize that cloud-based systems require coordinated protection across technical and organizational layers.

Zero Trust is particularly relevant to cloud, IoT, and hybrid enterprise systems. It provides a way to manage security across environments that cannot be protected by a single perimeter. By

combining identity verification, least privilege access, device posture checks, segmentation, risk-based authentication, and continuous monitoring, organizations can reduce their exposure to unauthorized access and improve their ability to detect suspicious activity. In this context, identity threat detection is not a separate security function. It is a necessary part of making Zero Trust work in real enterprise environments.

3. Methodology

3.1 Research Design

This article adopts a conceptual review methodology. A conceptual review is appropriate because the article does not aim to collect primary data from organizations, users, or technical experiments. Instead, it aims to examine existing research and develop a structured understanding of how Zero Trust Architecture and identity threat detection can be combined to secure cloud, IoT, and hybrid enterprise systems.

The conceptual review approach is useful for this type of study because Zero Trust implementation involves several connected areas of cybersecurity. These include identity and access management, cloud security, IoT security, insider threat detection, anomaly detection, SIEM monitoring, access control, and security governance. A single empirical method may not fully capture the relationship between these areas. Therefore, reviewing and synthesizing existing literature allows the article to build a broader framework that connects technical controls with organizational security requirements.

The study draws on peer-reviewed journal articles, conference papers, cybersecurity surveys, and foundational access control literature. Key Zero Trust studies are used to explain the concept, principles, adoption challenges, and maturity requirements of Zero Trust Architecture (Buck et al., 2021; Syed et al., 2022; Phiayura & Teerakanok, 2023; Yeoh et al., 2023). Studies on role-based access control, attribute-based access control, and identity management are used to support the discussion of identity-centered security (Sandhu et al., 1996; Bertino & Takahashi, 2010; Jin et al., 2012). Cloud and IoT security studies are also included because the article focuses specifically on distributed enterprise environments where traditional perimeter models are less effective (Hashizume et al., 2013; Sicari et al., 2015; Tabrizchi & Kuchaki Rafsanjani, 2020).

This design allows the article to move beyond a general discussion of Zero Trust and instead develop a practical conceptual structure. The framework proposed in the article is not presented as a tested technical product. Rather, it is developed as a research-based model that can guide future empirical studies, enterprise security planning, and cybersecurity implementation strategies.

3.2 Literature Selection Criteria

The literature used in this article was selected based on relevance to Zero Trust Architecture, identity threat detection, cloud security, IoT security, hybrid enterprise systems, access control, anomaly detection, and security monitoring. The selection focused mainly on peer-reviewed journal articles and reputable conference papers because the article is intended for academic and professional use. Foundational studies were also included where necessary because some cybersecurity concepts, such as role-based access control and attribute-based access control, were established before the recent rise of Zero Trust but remain important to its implementation.

The first group of literature includes studies on Zero Trust Architecture. These sources were selected because they explain the development of Zero Trust, its principles, migration requirements, maturity models, and implementation challenges. Buck et al. (2021) provided a broad review of Zero Trust knowledge and research gaps, while Syed et al. (2022) offered a comprehensive survey of Zero Trust Architecture. Phiayura and Teerakanok (2023) were also relevant because their work focused on migration toward Zero Trust, which is important for organizations moving away from perimeter-based security. Yeoh et al. (2023) were included because they examined critical success factors and maturity assessment, which are important for understanding why Zero Trust adoption can succeed or fail.

The second group of literature focuses on identity and access control. These sources were selected because identity is central to the proposed framework. Sandhu et al. (1996) were included because role-based access control remains a key foundation for assigning permissions based on organizational roles. Jin et al. (2012) were included because attribute-based access control supports more flexible and contextual access decisions. Bertino and Takahashi (2010) were also included because identity management provides the broader conceptual background for managing users, credentials, access rights, and identity-related technologies.

The third group of literature addresses identity threat detection, insider threats, anomaly detection, and monitoring. These sources were selected because identity-centered security is not limited to authentication. Organizations must also detect abnormal behavior after access has been granted. Salem et al. (2008) and Gheyas and Abdallah (2016) support the discussion of insider threat detection, while Ahmed et al. (2016) and Buczak and Guven (2015) support the discussion of anomaly detection and machine learning methods for cybersecurity. Bhatt et al. (2014) were included because SIEM systems play an operational role in collecting and correlating security events across enterprise systems.

The fourth group of literature focuses on cloud, IoT, fog, and hybrid security challenges. These sources were selected because the article applies Zero Trust and identity threat detection to distributed enterprise environments. Hashizume et al. (2013), Subashini and Kavitha (2011), Fernandes et al. (2014), and Tabrizchi and Kuchaki Rafsanjani (2020) support the discussion of

cloud security risks. Roman et al. (2013), Sicari et al. (2015), Raza et al. (2013), Mosenia and Jha (2016), and Al-Garadi et al. (2020) support the discussion of IoT security challenges and intrusion detection. Stergiou et al. (2018) and Atlam et al. (2018) support the discussion of secure integration between IoT, cloud, fog, and edge systems.

The inclusion criteria for the literature were as follows:

- The source must be directly related to Zero Trust Architecture, identity management, access control, cloud security, IoT security, anomaly detection, insider threat detection, or intrusion detection.
- The source must be peer-reviewed or published through a reputable academic or professional outlet.
- The source must contribute to the conceptual development of the article's framework.
- Foundational works were included when they were necessary for explaining core concepts such as access control, identity management, cloud security, and IoT security.
- Recent Zero Trust studies were prioritized where available, especially those published before June 2024, in line with the reference date requirement.

Sources that were not clearly related to cybersecurity, Zero Trust, identity security, cloud security, IoT security, or enterprise threat detection were not treated as central sources for the article. This is important because the article is likely to be reviewed for both accuracy and relevance.

3.3 Analytical Approach

The article uses thematic synthesis as its analytical approach. Thematic synthesis is suitable because the selected literature covers different but connected areas of cybersecurity. Instead of treating each source separately, the analysis groups the literature into major themes that help explain how Zero Trust Architecture and identity threat detection can be integrated into one enterprise security framework.

The first theme is Zero Trust principles. This theme examines the core ideas behind Zero Trust, including continuous verification, least privilege access, reduced implicit trust, microsegmentation, and policy-based enforcement. The analysis under this theme draws mainly on Zero Trust studies that explain the architecture, implementation models, and maturity requirements of Zero Trust (Buck et al., 2021; Syed et al., 2022; Phiayura & Teerakanok, 2023; Yeoh et al., 2023).

The second theme is identity and access management. This theme focuses on the role of identity in modern enterprise security. It examines how users, devices, workloads, administrators, service accounts, and APIs should be authenticated, authorized, and continuously assessed. The analysis

also considers the relevance of role-based and attribute-based access control in supporting Zero Trust access decisions (Sandhu et al., 1996; Bertino & Takahashi, 2010; Jin et al., 2012).

The third theme is **identity threat detection**. This theme examines how organizations can detect suspicious activity involving valid or compromised identities. It includes risk-based authentication, anomaly detection, insider threat detection, SIEM monitoring, behavioral analytics, and intrusion detection. This theme is central to the article because Zero Trust does not end after login. Even after access is granted, identity activity must be monitored for signs of misuse, privilege abuse, or abnormal behavior (Salem et al., 2008; Bhatt et al., 2014; Ahmed et al., 2016; Dasu et al., 2023).

The fourth theme is **cloud and IoT security challenges**. This theme examines the specific risks found in cloud platforms, IoT systems, fog computing, edge environments, and hybrid enterprise networks. Cloud systems often involve risks such as misconfiguration, insecure APIs, account hijacking, and data leakage. IoT systems introduce additional problems such as weak authentication, resource limitations, insecure firmware, and poor lifecycle management. These risks show why identity-based and continuously monitored security models are necessary (Hashizume et al., 2013; Sicari et al., 2015; Stergiou et al., 2018; Tabrizchi & Kuchaki Rafsanjani, 2020).

The fifth theme is **integrated enterprise security governance**. This theme examines how organizations can bring together Zero Trust principles, identity governance, threat detection, monitoring, and policy enforcement. It considers the practical need for security maturity assessment, implementation planning, continuous improvement, and alignment between technical controls and organizational policies. This theme supports the development of the article's proposed conceptual framework (Adahman et al., 2022; Phiayura & Teerakanok, 2023; Yeoh et al., 2023).

Through this thematic approach, the article identifies the major connections between Zero Trust Architecture and identity threat detection. The analysis shows that Zero Trust provides the security philosophy and architectural direction, while identity threat detection provides the monitoring and response capability needed to identify suspicious behavior after access is requested or granted. Together, these elements form the basis for a unified framework that can support stronger protection across cloud, IoT, and hybrid enterprise environments.

4. Zero Trust Architecture for Modern Enterprise Systems

4.1 Identity Verification and Access Control

Identity verification is the foundation of Zero Trust Architecture because every access request begins with one basic question: who or what is trying to gain access? In traditional network

security, trust was often attached to location. A user or device inside the corporate network was treated as safer than one outside it. That assumption is no longer reliable in modern enterprise environments. Cloud platforms, remote work, mobile devices, IoT systems, application programming interfaces, and hybrid infrastructures have made enterprise access more distributed and more difficult to control. In this context, Zero Trust requires organizations to verify the identity of every user, administrator, device, application, API, and workload before granting access.

Identity verification in a Zero Trust environment is not limited to username and password authentication. It involves a broader process of confirming whether the requesting entity is legitimate, whether it has the right to access a particular resource, and whether the access request matches the expected context. This means that a user may be authenticated successfully but still denied access if the request appears risky, unusual, or inconsistent with policy. For example, an employee attempting to access a sensitive cloud database from an unfamiliar device or unusual location may be required to complete additional verification before access is granted. This reflects the Zero Trust principle that access should be continuously evaluated rather than permanently assumed.

Access control models provide the theoretical base for this process. Role-based access control assigns permissions based on a user's organizational role, making it useful for defining structured responsibilities within an enterprise (Sandhu et al., 1996). For example, a finance officer may be granted access to financial reporting systems but denied access to engineering repositories. However, role-based access control may not always be flexible enough for modern enterprise environments where access decisions depend on several changing factors. Attribute-based access control extends this logic by allowing access decisions to be based on user attributes, resource attributes, environmental conditions, and contextual information (Jin et al., 2012). This is especially important in Zero Trust systems because access decisions may depend on the user's identity, device posture, location, time of access, sensitivity of the requested resource, and current risk level.

Identity management systems also play a central role in Zero Trust implementation. They help organizations manage digital identities, authentication processes, authorization rules, account lifecycles, and access privileges across multiple platforms. Bertino and Takahashi (2010) emphasized that identity management involves not only identifying users but also managing credentials, roles, privileges, and trust relationships across distributed systems. This is highly relevant to cloud, IoT, and hybrid enterprise environments, where identities may include employees, contractors, administrators, service accounts, APIs, virtual machines, containers, and connected devices.

In modern enterprise security, identity must therefore be treated as a control point rather than a simple login requirement. A strong Zero Trust system should verify human and non-human

identities, enforce appropriate access rules, review privileges regularly, and revoke unnecessary permissions. Without strong identity verification and access control, Zero Trust becomes difficult to implement because attackers can exploit weak credentials, excessive privileges, and poorly managed accounts to move across systems. For this reason, identity verification is not just one part of Zero Trust Architecture. It is the starting point for every access decision.

4.2 Least Privilege and Policy-Based Access

Least privilege is one of the most important principles of Zero Trust Architecture. It means that users, devices, applications, and workloads should only receive the minimum level of access required to perform an authorized task. This approach reduces the damage that can occur if an account, endpoint, or application is compromised. Instead of allowing broad access across an enterprise network, Zero Trust limits access to specific systems, resources, and actions based on need, role, context, and risk.

In many organizations, excessive privilege remains a major security weakness. Employees may retain access to systems they no longer use. Administrators may hold broad permissions that are not regularly reviewed. Service accounts may be granted long-term access without proper monitoring. Cloud workloads may be configured with permissions that exceed their operational requirements. These weaknesses create opportunities for attackers. Once an attacker compromises a privileged account, they may be able to access sensitive data, disable security controls, create new accounts, or move laterally across the enterprise environment.

Zero Trust reduces this risk by enforcing policy-based access. Under this model, access is not granted simply because a user has logged in or because a device is connected to the network. Instead, access is granted based on defined policies that consider identity, role, device condition, resource sensitivity, location, behavior, and risk level. Syed et al. (2022) described Zero Trust Architecture as a model that removes implicit trust and requires continuous evaluation of access requests across enterprise systems. This means that access is not a one-time decision. It is a controlled process that can be adjusted as conditions change.

Least privilege is also closely linked to the prevention of lateral movement. Lateral movement occurs when an attacker uses one compromised account or device to move across other systems. In a flat network or poorly controlled environment, one compromise can expose many resources. In a Zero Trust environment, however, least privilege limits what a compromised account can access. Even if an attacker gains valid credentials, their movement is restricted by access policies, segmentation, authentication requirements, and monitoring controls.

Policy-based access also improves accountability. When access policies are clearly defined, organizations can track who accessed what, when access occurred, and whether the access

matched approved rules. This makes it easier to detect suspicious behavior, investigate incidents, and enforce compliance. Yeoh et al. (2023) noted that successful Zero Trust implementation depends not only on technical controls but also on maturity, governance, and organizational readiness. This means that least privilege must be supported by regular access reviews, privilege audits, policy updates, and clear responsibility for identity governance.

For cloud, IoT, and hybrid enterprise systems, least privilege is especially important. Cloud platforms often involve multiple users, administrators, applications, and automated workloads. IoT environments may contain many devices with limited security controls. Hybrid systems combine internal infrastructure with external services and remote access points. In each of these settings, broad or poorly managed access can create serious exposure. A Zero Trust approach limits this exposure by ensuring that every entity receives only the access it needs and nothing more.

5.3 Device Posture and Endpoint Trust

Zero Trust Architecture does not automatically trust devices. A device may belong to the organization, but that does not mean it is secure at all times. It may be outdated, infected, misconfigured, unmanaged, or connected through an unsafe network. In modern enterprise systems, users may connect from laptops, smartphones, tablets, personal devices, virtual machines, cloud workloads, and IoT endpoints. Because of this, device posture has become an important part of access control.

Device posture refers to the security condition of a device at the time it requests access. This may include whether the device is patched, whether antivirus or endpoint protection is active, whether encryption is enabled, whether the device is managed by the organization, and whether it has signs of compromise. A device with poor security posture should not receive the same level of access as a healthy, managed, and compliant device. This is consistent with the Zero Trust idea that access decisions should be based on current evidence rather than fixed assumptions.

In hybrid enterprise environments, device trust becomes more complicated. A user may access business systems from a company laptop at the office, a personal laptop at home, a mobile phone while traveling, or a virtual desktop connected to a cloud environment. Each access request presents a different level of risk. Phiayura and Teerakanok (2023) emphasized that migration to Zero Trust requires organizations to consider architecture, identity, devices, networks, applications, and policies as connected parts of a security strategy. Device posture is therefore not a separate concern. It must be integrated with identity verification, access control, monitoring, and policy enforcement.

Device posture is also important for IoT systems. Many IoT devices have limited processing power, weak authentication mechanisms, poor patching support, and long operational lifecycles. Some devices may be difficult to update or monitor, especially in industrial or large-scale

enterprise environments. If such devices are trusted automatically, they can become entry points for attackers. Dhiman et al. (2024) noted that Zero Trust network models are designed to reduce implicit trust and strengthen control over users, devices, and network interactions. This is particularly relevant to IoT because connected devices often expand the attack surface of an organization.

Endpoint trust must therefore be treated as dynamic. A device that was secure yesterday may not be secure today. A laptop may become compromised after connecting to an unsafe network. A mobile device may lose compliance after missing security updates. An IoT sensor may begin behaving abnormally after being tampered with. Zero Trust addresses these possibilities by continuously checking device posture and linking device status to access decisions.

A mature Zero Trust system should be able to deny access, restrict access, or require additional verification when a device does not meet security requirements. For example, an unmanaged device may be allowed to access low-risk resources but blocked from accessing sensitive systems. A device missing critical updates may be redirected for remediation before access is granted. A device showing suspicious behavior may trigger alerts or session termination. This approach strengthens enterprise security because trust is not given permanently. It is earned through continuous verification.

4.4 Microsegmentation and Lateral Movement Control

Microsegmentation is a key Zero Trust control because it limits how far an attacker can move after gaining access to one part of a system. In traditional enterprise networks, once a user or device gained internal access, it often had broad visibility across multiple systems. This created serious risk because a single compromised account or endpoint could allow attackers to move from one system to another. Zero Trust challenges this model by dividing enterprise environments into smaller, controlled segments and enforcing access rules between them.

The purpose of microsegmentation is not only to separate networks but also to control communication between users, devices, applications, workloads, and data resources. Each segment can have its own access policies, authentication requirements, and monitoring rules. For example, a cloud application may be allowed to communicate with a specific database but blocked from accessing unrelated systems. An IoT device may be permitted to send data to a monitoring platform but denied access to administrative systems. A remote user may be allowed to access a business application but not the underlying infrastructure.

This approach is especially important because many modern attacks depend on lateral movement. After gaining access through phishing, credential theft, malware, or a vulnerable device, attackers often search for additional systems, escalate privileges, and move toward sensitive data. Microsegmentation makes this process more difficult by reducing unnecessary

pathways across the enterprise environment. Even if one account or device is compromised, the attacker's access remains limited.

Syed et al. (2022) identified segmentation and strict access control as important components of Zero Trust Architecture. These controls help organizations move away from flat networks and toward more controlled security zones. Zanasi et al. (2024) also highlighted the relevance of flexible Zero Trust Architecture for industrial IoT infrastructures, where connected devices, operational systems, and networked assets must be protected against unauthorized access and lateral movement. In industrial settings, the consequences of lateral movement can be especially serious because attackers may target production systems, sensors, controllers, or critical operational processes.

Microsegmentation is also valuable in cloud environments. Cloud workloads often communicate with other services, storage systems, APIs, and databases. If these connections are not controlled, a compromised workload may expose other parts of the cloud environment. Microsegmentation allows organizations to define which workloads can communicate, under what conditions, and for what purpose. This supports least privilege not only for users but also for applications and workloads.

In hybrid enterprise systems, microsegmentation provides a way to control movement across on-premises infrastructure, cloud platforms, remote endpoints, and IoT systems. Without segmentation, hybrid environments can become difficult to monitor and defend. With segmentation, organizations can create smaller security boundaries that are easier to manage. However, microsegmentation must be planned carefully. Poorly designed segmentation may disrupt business operations, create policy conflicts, or increase administrative complexity. For this reason, organizations should begin by identifying critical assets, mapping communication flows, classifying sensitive systems, and applying access policies gradually.

Microsegmentation supports the broader Zero Trust goal of reducing implicit trust. Instead of assuming that everything inside a network should communicate freely, it requires every connection to be justified, controlled, and monitored. This makes enterprise systems more resilient because attackers face barriers at each stage of movement.

4.5 Continuous Monitoring and Security Analytics

Continuous monitoring is essential to Zero Trust Architecture because risk is not static. A user may be legitimate at login but later behave suspiciously. A device may pass a posture check at the beginning of a session but become compromised later. A cloud workload may operate normally for weeks and then begin making unusual requests. Because of these possibilities, Zero Trust requires ongoing visibility into users, devices, applications, workloads, and network activity.

Traditional security models often focused heavily on initial authentication. Once access was granted, users and devices were allowed to continue operating with limited re-evaluation. Zero Trust takes a different approach. It treats access as a continuous decision that may be changed, restricted, or revoked if risk increases. This requires monitoring tools that can collect and analyze security events across the enterprise environment.

Security information and event management systems play an important role in this process. SIEM platforms collect logs and security events from different systems, including servers, endpoints, cloud platforms, firewalls, applications, identity systems, and network devices. Bhatt et al. (2014) explained that SIEM systems support security operations by helping organizations collect, correlate, and analyze event data. In a Zero Trust environment, SIEM can help identify suspicious logins, access violations, unusual privilege use, abnormal network traffic, and policy breaches.

Anomaly detection also supports continuous monitoring. Rather than relying only on known attack signatures, anomaly detection looks for behavior that differs from expected patterns. Ahmed et al. (2016) described network anomaly detection as a useful approach for identifying suspicious activity, particularly when attacks do not match known signatures. This is important for Zero Trust because many identity-based attacks use valid credentials and may not appear malicious at first glance. For example, a user account may log in successfully but then access unusual systems, download abnormal amounts of data, or attempt to connect from an unfamiliar location.

Machine learning can also support security analytics by identifying patterns in large volumes of security data. Buczak and Guven (2015) reviewed the use of data mining and machine learning methods for cybersecurity intrusion detection, showing that these methods can support classification, detection, and prediction of suspicious activity. In enterprise systems, machine learning may help detect abnormal login behavior, unusual API activity, suspicious device communication, or unexpected workload behavior. However, these tools should not be treated as perfect solutions. They require good data, careful tuning, human oversight, and integration with broader security processes.

Continuous monitoring is particularly important for cloud, IoT, and hybrid systems because these environments are dynamic. Cloud workloads can be created, modified, and removed quickly. IoT devices may operate in distributed locations. Hybrid systems may involve users and services moving between internal and external environments. Without continuous monitoring, organizations may lose visibility into who is accessing what, which devices are active, and whether behavior remains consistent with policy.

A strong Zero Trust system should therefore combine identity logs, device telemetry, access records, network activity, cloud monitoring, and threat intelligence. The goal is not only to detect attacks after they happen but also to identify early warning signs before damage spreads.

Continuous monitoring gives organizations the ability to respond quickly by challenging a user, limiting a session, blocking access, isolating a device, or triggering incident response.

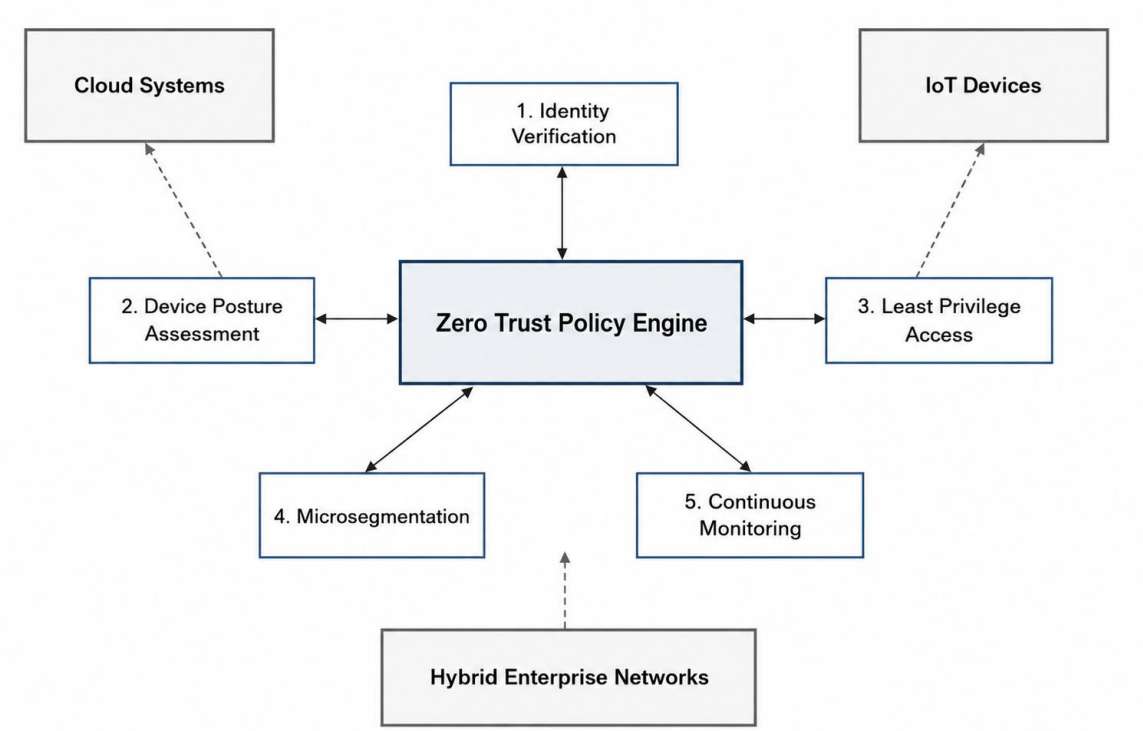

Figure 1. Conceptual Zero Trust Architecture for securing cloud, IoT, and hybrid enterprise systems.

5. Identity Threat Detection Framework

5.1 Identity-Based Attack Vectors

Identity-based attacks have become a major concern in modern cybersecurity because attackers often target the credentials, privileges, and access rights that allow users and systems to operate. In many cases, attackers do not need to break through a network perimeter directly. Instead, they obtain or abuse a valid identity and use it to enter the environment as if they were an authorized user. This makes identity-based threats difficult to detect because the attacker may appear legitimate during the early stages of an attack.

Credential theft is one of the most common identity-based attack vectors. Attackers may steal usernames, passwords, tokens, or session credentials through phishing, malware, credential stuffing, social engineering, or insecure storage. Once credentials are obtained, attackers can attempt to access systems without triggering traditional perimeter defenses. This problem

becomes more serious when accounts have excessive privileges or when multi-factor authentication is not properly enforced.

Phishing-based account compromise is also closely linked to identity threat. A successful phishing attack can give attackers access to email accounts, cloud platforms, business applications, or administrative portals. From there, they may reset passwords, create forwarding rules, impersonate users, or access sensitive files. In a hybrid enterprise environment, one compromised identity can expose both cloud and internal systems if access is not properly segmented and monitored.

Privilege escalation is another serious identity-based threat. Attackers may begin with a low-privilege account and then attempt to gain higher permissions. This may involve exploiting misconfigured roles, weak access policies, vulnerable systems, or excessive permissions attached to service accounts. Once higher privileges are obtained, attackers can disable controls, access confidential data, create persistence, or move deeper into the environment.

Insider misuse is also part of the identity threat landscape. Insider threats may involve malicious employees, careless users, contractors, or compromised legitimate accounts. Salem et al. (2008) explained that insider attack detection is challenging because insiders often have legitimate access to systems and may understand internal processes. Gheyas and Abdallah (2016) also showed that insider threat detection requires attention to behavioral patterns, access misuse, and predictive indicators. In Zero Trust environments, this is important because internal users are not automatically trusted.

Session hijacking, compromised service accounts, unauthorized API access, and lateral movement through valid credentials are also major risks. Service accounts and APIs are especially important in cloud and hybrid environments because they often support automated communication between applications and workloads. If these identities are poorly protected, attackers can use them to access systems without relying on traditional user accounts.

Dasu et al. (2023) emphasized the importance of risk-based authentication in defending against identity threats. This is because identity attacks often appear normal at first glance. A login may use the correct password, but the wider context may show risk. For example, the login may come from an unusual location, an unknown device, or a pattern that does not match the user's normal behavior. Identity threat detection therefore requires more than verifying credentials. It requires continuous analysis of behavior, context, privilege use, and access patterns.

5.2 Risk-Based Authentication

Risk-based authentication is an adaptive security approach that evaluates the risk of an access attempt before deciding whether to allow, deny, restrict, or challenge the user. Unlike static authentication, which applies the same login requirement to every situation, risk-based

authentication considers the context of each access request. This makes it highly compatible with Zero Trust Architecture, where trust is never assumed and access decisions are continuously evaluated.

In a risk-based authentication system, several indicators may be analyzed. These include the user's normal behavior, device reputation, geolocation, time of access, network source, login frequency, failed login attempts, type of resource being accessed, and sensitivity of the requested data. A low-risk login may proceed normally, while a higher-risk login may require additional verification, such as multi-factor authentication, step-up authentication, temporary restriction, or administrative review.

This approach is important because not all access attempts carry the same level of risk. For example, an employee logging in from a known device during normal working hours may present a lower risk than the same employee logging in from an unfamiliar country at midnight. Similarly, access to a public internal dashboard is not as sensitive as access to a privileged administrative console or customer database. Risk-based authentication allows security controls to adjust based on these differences.

Dasu et al. (2023) argued that risk-based authentication can help defend against identity threats by using contextual and behavioral signals to identify suspicious access attempts. This is especially useful in environments where attackers use stolen credentials. If the correct password is entered but the surrounding context appears unusual, the system can require additional verification before access is granted. In this way, risk-based authentication reduces dependence on passwords alone.

Risk-based authentication also supports user experience when implemented properly. Instead of forcing the highest level of authentication for every access attempt, organizations can apply stronger checks only when risk increases. This helps balance security and usability. Low-risk activities may remain smooth, while high-risk activities receive stronger protection. However, this balance depends on accurate risk scoring and careful policy design. If the system is too strict, users may experience unnecessary friction. If it is too weak, risky access may be allowed.

In Zero Trust Architecture, risk-based authentication should not be limited to the login stage. It should continue throughout the session. If a user begins behaving unusually after login, the system should be able to re-evaluate the session and take action. For example, it may require re-authentication, restrict access, alert security teams, or terminate the session. This reflects the Zero Trust principle that access is temporary, conditional, and subject to change.

Risk-based authentication becomes even more important in cloud, IoT, and hybrid enterprise systems. Cloud systems often involve remote access and distributed workloads. IoT systems involve large numbers of connected devices with varying trust levels. Hybrid systems include

users and services moving between internal and external environments. In all of these cases, risk-based authentication provides a flexible way to make access decisions based on real-time context rather than fixed assumptions.

5.3 Behavioral Analytics and Anomaly Detection

Behavioral analytics and anomaly detection are important parts of identity threat detection because many modern attacks do not immediately look like attacks. When attackers use valid credentials, they may bypass basic authentication checks and appear as legitimate users. The difference often lies in what they do after gaining access. They may access unusual systems, download large amounts of data, attempt privilege escalation, log in at unusual times, or communicate with systems that the real user rarely uses. Behavioral analytics helps identify these differences.

Anomaly detection is based on the idea that suspicious activity can be recognized by comparing current behavior with expected behavior. Ahmed et al. (2016) described anomaly detection as a method for identifying network activity that differs from normal patterns. In identity security, this principle can be applied to user behavior, device behavior, application behavior, and workload activity. For example, if a user who normally accesses only human resources files suddenly attempts to access source code repositories or financial databases, the system may flag the activity as suspicious.

Machine learning can strengthen anomaly detection by analyzing large and complex datasets. Buczak and Guven (2015) explained that data mining and machine learning methods can support cybersecurity intrusion detection by identifying patterns that may not be visible through manual analysis. In a Zero Trust environment, these techniques may help identify abnormal login behavior, unusual access sequences, suspicious API calls, and unexpected network activity. They can also support prioritization by helping security teams focus on high-risk alerts.

However, behavioral analytics and anomaly detection have limitations. Sommer and Paxson (2010) warned that applying machine learning to intrusion detection is difficult because real-world networks are open, dynamic, and unpredictable. Normal behavior changes over time, and attackers may adapt their techniques to avoid detection. A model trained on past behavior may not always detect new forms of attack. It may also generate false positives when legitimate users behave unusually for valid reasons.

Mishra et al. (2018) also noted that machine learning techniques for intrusion detection require careful design, feature selection, and evaluation. This is important because a poorly configured system can overwhelm security teams with too many alerts or miss subtle attacks. Behavioral analytics should therefore support human judgment rather than replace it completely. Security

teams still need to investigate alerts, tune detection models, review policies, and understand the business context behind user behavior.

In Zero Trust Architecture, behavioral analytics adds value by making access decisions more dynamic. Access is no longer based only on identity at the point of login. It is also based on continuing behavior during the session. If behavior remains normal, access may continue. If behavior becomes suspicious, access can be challenged, limited, or revoked. This allows organizations to respond to risk as it develops.

Behavioral analytics is also useful across cloud, IoT, and hybrid systems. In cloud environments, it can detect unusual administrative actions, abnormal API use, or unexpected data movement. In IoT environments, it can identify devices that suddenly communicate outside their normal patterns. In hybrid systems, it can help correlate behavior across on-premises systems, cloud platforms, remote endpoints, and identity providers. This makes it an important component of identity-centered Zero Trust security.

5.4 Insider Threat Detection

Insider threats remain one of the most difficult cybersecurity risks to manage because insiders already have some level of legitimate access. An insider may be an employee, contractor, administrator, vendor, or business partner. The threat may be intentional, such as data theft or sabotage, or unintentional, such as careless handling of credentials or accidental policy violations. In both cases, the risk is serious because insiders often understand the organization's systems, processes, and sensitive assets.

Zero Trust Architecture is useful for insider threat management because it rejects the assumption that internal users are automatically trustworthy. Under a traditional model, users inside the network may receive broad access once authenticated. Under Zero Trust, internal access is still verified, limited, monitored, and reviewed. This makes it harder for insiders or compromised internal accounts to misuse privileges without detection.

Salem et al. (2008) explained that insider attack detection is challenging because insiders may use authorized access to perform harmful actions. Unlike external attackers, they may not need to bypass security controls in obvious ways. They may simply access information they are allowed to see but use it for unauthorized purposes. This makes insider threat detection dependent on behavioral analysis, access monitoring, and policy enforcement.

Gheyas and Abdallah (2016) also showed that insider threat detection and prediction require careful analysis of behavior, activity patterns, and risk indicators. These indicators may include unusual file access, abnormal data transfers, repeated failed access attempts, changes in work patterns, attempts to access restricted resources, or unusual use of privileged accounts. In a Zero

Trust environment, these indicators should be linked to continuous monitoring and adaptive access controls.

Insider threat detection must also consider compromised legitimate accounts. In many cases, the person using the account may not be the real user. An attacker may steal credentials and then act as an insider. This creates a blurred line between external and internal threats. From the system's perspective, the activity may appear to come from an authorized identity. This is why identity threat detection must focus not only on who logs in but also on what the account does after access is granted.

Privilege misuse is a major part of insider threat risk. Administrators and high-privilege users often have access to critical systems, sensitive data, and configuration controls. If these privileges are abused or compromised, the damage can be severe. Zero Trust reduces this risk by enforcing least privilege, requiring stronger authentication for sensitive actions, monitoring administrative activity, and reviewing privileges regularly.

Organizations should also avoid treating insider threat detection as purely technical. It requires governance, policy, training, and clear response procedures. Employees should understand acceptable use rules, data handling requirements, and reporting procedures. Security teams should have processes for investigating suspicious activity without creating unnecessary distrust or violating privacy expectations. A balanced approach is needed because insider threat detection must protect the organization while respecting legitimate work behavior.

5.5 SIEM and Continuous Identity Monitoring

Security information and event management systems support identity threat detection by collecting and analyzing security events from different parts of the enterprise environment. In modern organizations, identity activity is spread across many systems: identity providers, cloud platforms, endpoint devices, firewalls, servers, applications, APIs, IoT networks, and remote access tools. Without a central monitoring capability, it becomes difficult to understand how identity activity connects across the enterprise.

Bhatt et al. (2014) described SIEM systems as important operational tools for collecting, correlating, and analyzing security information. In the context of Zero Trust, SIEM can help security teams detect suspicious logins, abnormal access behavior, policy violations, privilege misuse, unusual network activity, and signs of lateral movement. It can also provide the evidence needed for investigation and incident response.

Continuous identity monitoring means that identity activity is observed throughout the access lifecycle. Monitoring begins when an access request is made, continues while the session is active, and remains available for audit after the session ends. This is important because many attacks do not become visible at the moment of login. A user may authenticate successfully, but

suspicious activity may appear later. For example, the account may access an unusual system, attempt to download sensitive files, or perform administrative actions outside normal patterns.

SIEM supports this process by correlating events from multiple sources. A single event may not appear dangerous on its own, but several related events may reveal a threat. For example, a login from an unusual location, followed by access to sensitive files and an attempt to change security settings, may indicate account compromise. SIEM helps connect these signals so that security teams can respond more quickly.

In cloud environments, SIEM can collect logs from identity providers, cloud access management systems, storage services, virtual machines, and applications. In IoT environments, it can collect device activity, network flows, authentication events, and anomaly alerts. In hybrid enterprise systems, it can combine internal logs with cloud and remote access data. This makes SIEM valuable for organizations that need visibility across multiple environments.

However, SIEM is not effective by itself unless it is properly configured and supported by clear policies. Organizations must decide which logs to collect, how long to retain them, which alerts matter most, and how incidents should be escalated. Poorly configured SIEM systems can create too many alerts, making it difficult for security teams to identify real threats. Therefore, continuous identity monitoring should include alert prioritization, risk scoring, behavioral baselines, and regular tuning.

In a Zero Trust security model, SIEM works best when integrated with identity governance, access control, endpoint detection, cloud monitoring, and incident response. When suspicious activity is detected, the organization should be able to take action quickly. This may include requiring re-authentication, disabling a session, limiting account privileges, isolating a device, or launching an investigation. In this way, SIEM becomes more than a logging tool. It becomes part of an active identity threat detection and response framework.

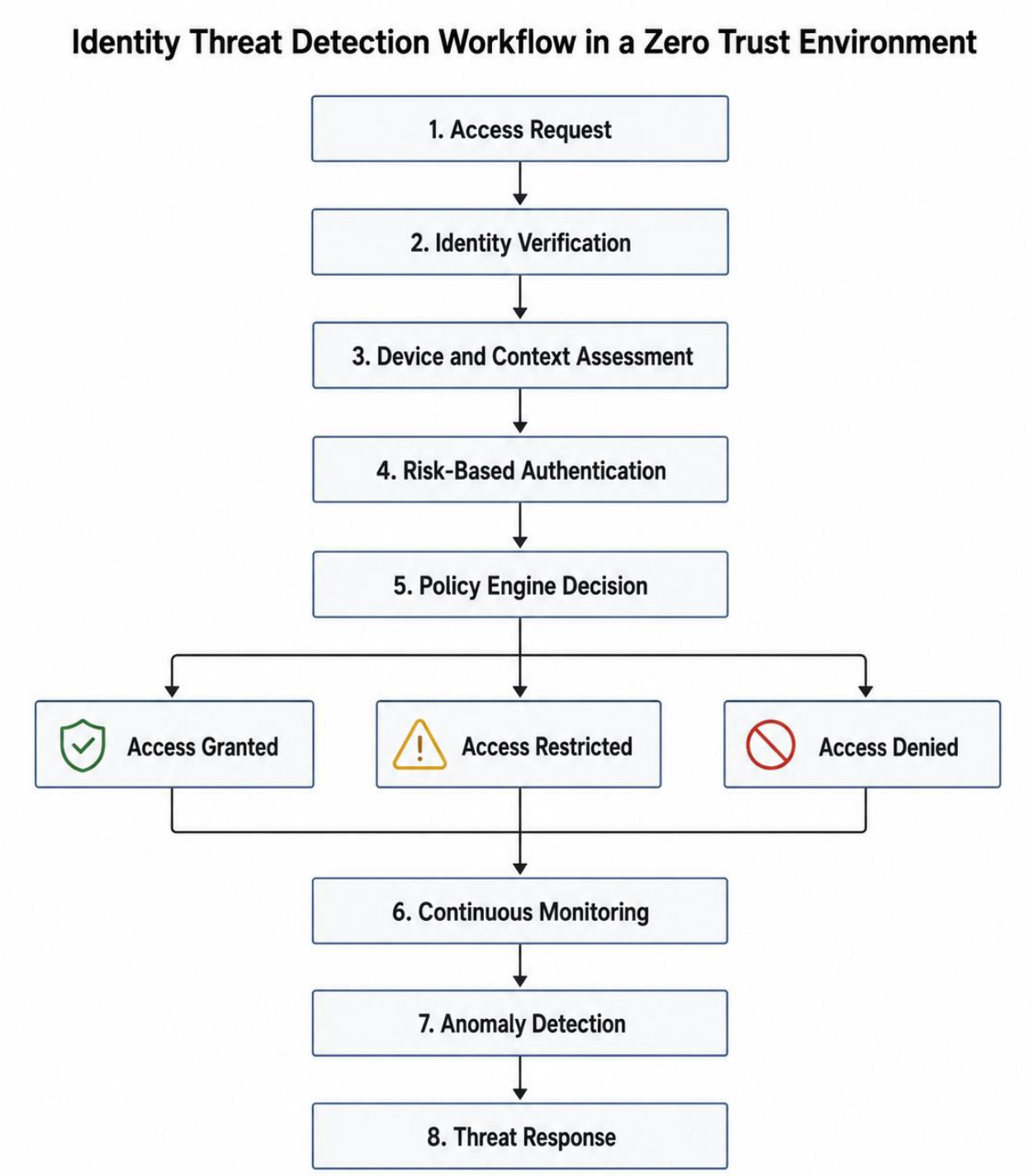

Figure 2. Identity threat detection workflow within a Zero Trust enterprise security environment.

6. Securing Cloud, IoT, and Hybrid Enterprise Systems

6.1 Cloud Security

Cloud computing has changed the way organizations store data, run applications, and deliver digital services. Instead of keeping all systems within a clearly defined internal network, many organizations now depend on public cloud platforms, private cloud environments, software-as-a-service applications, containers, virtual machines, and distributed workloads. This shift has created major benefits in terms of scalability, flexibility, and cost efficiency, but it has also introduced new security challenges that traditional perimeter-based defenses cannot fully address.

One of the most common risks in cloud environments is misconfiguration. Cloud systems are highly dynamic, and a small configuration error can expose sensitive data, open storage buckets to the public, or grant excessive privileges to users and services. Hashizume et al. (2013) noted that cloud environments create security concerns related to data protection, access control, availability, and virtualization. Similarly, Fernandes et al. (2014) explained that cloud environments are exposed to several security issues, including insecure interfaces, weak access control, data leakage, and risks associated with shared infrastructure. These concerns are particularly important in enterprise environments where multiple users, applications, and third-party services interact with cloud resources.

Insecure application programming interfaces also remain a major cloud security concern. APIs connect applications, users, services, and workloads, but poorly secured APIs can become entry points for unauthorized access or data exposure. Account hijacking is another serious issue because attackers often target cloud identities instead of attacking infrastructure directly. Once an attacker gains access to a legitimate account, especially an administrative or privileged account, it becomes easier to move across cloud resources while appearing as an authorized user. This makes identity protection a central part of cloud security.

Zero Trust Architecture strengthens cloud security by removing the assumption that a user, workload, or service should be trusted simply because it has passed an initial login or is operating within an approved environment. Instead, access must be verified continuously based on identity, device posture, risk level, and policy conditions. In a cloud setting, this means enforcing identity-based access, least privilege permissions, workload monitoring, encryption, and continuous policy enforcement. Tabrizchi and Kuchaki Rafsanjani (2020) emphasized that cloud security requires attention to threats, vulnerabilities, access control, data privacy, and monitoring. A Zero Trust approach responds to these concerns by ensuring that cloud access is not only granted carefully but also monitored throughout the session.

Least privilege is especially important in cloud environments because many breaches are made worse by excessive permissions. Users, administrators, applications, and service accounts should only receive the access needed for their specific functions. In the same way, cloud workloads should be monitored for unusual behavior, such as unexpected access requests, abnormal data transfer, or suspicious changes to system configurations. By combining identity governance, encryption, access control, and continuous monitoring, Zero Trust helps organizations reduce cloud exposure and detect threats before they spread across the wider enterprise environment.

6.2 IoT Security

The Internet of Things has expanded the digital attack surface of modern organizations. Enterprises now use connected sensors, cameras, smart devices, medical devices, industrial controllers, access systems, environmental monitors, and other network-enabled equipment. These devices support automation, operational efficiency, and real-time data collection, but they also introduce serious security risks. Unlike traditional computers, many IoT devices have limited processing power, weak built-in security, long replacement cycles, and poor patch management.

One of the most important IoT security challenges is weak authentication. Many devices are deployed with default passwords, shared credentials, or limited identity management features. This makes it easier for attackers to compromise devices and use them as entry points into wider networks. Roman et al. (2013) explained that distributed IoT environments create major privacy and security challenges because devices often operate in open, heterogeneous, and resource-constrained settings. Sicari et al. (2015) also emphasized that security, privacy, and trust remain central issues in IoT because connected devices exchange sensitive data and often interact with critical systems.

Insecure firmware is another major concern. Many IoT devices are not updated regularly, and some vendors stop providing security patches before the devices are removed from service. This leaves organizations exposed to known vulnerabilities. Poor communication security also creates risk, especially when devices transmit data without strong encryption or proper authentication. In industrial and enterprise settings, compromised IoT devices can be used for surveillance, disruption, lateral movement, or unauthorized access to sensitive networks.

Intrusion detection is therefore important for IoT environments. Raza et al. (2013) proposed real-time intrusion detection for IoT, showing that IoT networks require security approaches that are adapted to their limited resources and communication patterns. Mosenia and Jha (2016) further explained that IoT security must address threats across devices, communication channels, applications, and data. More recently, Al-Garadi et al. (2020) reviewed machine learning and deep learning methods for IoT security, showing that intelligent detection techniques can support threat identification in complex IoT environments.

Zero Trust can improve IoT security by treating every device as a security subject that must be identified, verified, monitored, and controlled. This means that IoT devices should not automatically receive broad network access after connection. Instead, each device should have a unique identity, follow secure onboarding procedures, and operate within a segmented network zone. If an IoT device begins communicating with unusual systems, sending abnormal traffic, or behaving outside its expected function, the organization should be able to detect and restrict that behavior.

Network segmentation is especially useful in IoT environments. Many IoT devices do not need direct access to enterprise databases, user workstations, or administrative systems. By placing devices in controlled network segments and enforcing policy-based communication, organizations can reduce the damage caused by a compromised device. Continuous monitoring and anomaly detection also help identify suspicious behavior early. In this way, Zero Trust does not remove all IoT risks, but it gives organizations a stronger structure for managing device identity, access, communication, and threat detection.

6.3 Hybrid Enterprise Security

Hybrid enterprise systems combine several environments at once. A typical organization may use on-premises servers, public cloud platforms, private cloud resources, SaaS applications, remote work tools, mobile devices, IoT endpoints, and third-party services. This arrangement reflects the reality of modern digital operations, but it also makes security management more difficult. The organization no longer controls one simple network boundary. Instead, it must protect users, devices, data, and applications across multiple locations and platforms.

One of the main challenges in hybrid environments is fragmented access control. Different systems may use different identity providers, authentication rules, permission models, and monitoring tools. This creates gaps in visibility and can make it difficult to know who has access to what. It also increases the risk of excessive privileges, orphaned accounts, inconsistent policies, and weak enforcement. Stergiou et al. (2018) discussed the need for secure integration between IoT and cloud computing, emphasizing that connected environments require careful attention to privacy, communication, and security controls.

Remote access also increases risk in hybrid enterprises. Employees, contractors, vendors, and administrators may connect from different locations, networks, and devices. Some may use managed corporate systems, while others may connect through personal or less secure endpoints. Without strong verification and monitoring, remote access can become a major path for credential theft, account misuse, and unauthorized entry into enterprise systems.

Zero Trust provides a practical approach for managing these risks because it applies consistent security principles across different environments. Instead of trusting access based on network location, Zero Trust requires identity verification, least privilege access, device assessment, and

continuous monitoring. Phiayura and Teerakanok (2023) argued that migration to Zero Trust requires a structured framework because organizations must align identity, access control, monitoring, policy enforcement, and security operations. Yeoh et al. (2023) also highlighted the importance of maturity assessment and critical success factors in Zero Trust cybersecurity, showing that implementation requires both technical capability and organizational readiness.

For hybrid enterprises, Zero Trust helps create a unified security posture. A user accessing a SaaS application, a cloud workload, an internal database, or an IoT management platform should be evaluated using consistent identity and risk-based rules. This does not mean that every system must use the same tool, but it does mean that access should be governed by a common security model. Identity governance, continuous monitoring, and microsegmentation allow organizations to reduce blind spots and limit the movement of attackers across systems.

Hybrid security also requires strong visibility. Security teams need to understand user activity, device behavior, cloud events, network traffic, and application access across multiple environments. Without this visibility, threats can remain hidden until they cause significant damage. By combining Zero Trust with identity threat detection, organizations can improve their ability to detect abnormal access behavior, enforce policy consistently, and respond quickly to suspicious activity.

6.4 Fog and Edge Security Considerations

Fog and edge computing extend cloud and IoT environments by moving data processing closer to the devices that generate the data. Instead of sending all information to a central cloud platform, edge and fog systems allow data to be processed near sensors, machines, users, or local gateways. This can reduce latency, improve performance, and support time-sensitive applications such as industrial automation, smart cities, healthcare monitoring, and connected transportation.

However, this distributed model also creates new security concerns. Edge and fog nodes may operate outside traditional data centers and may be deployed in locations with weaker physical and technical controls. They may connect to many IoT devices, process sensitive data, and communicate with cloud platforms. If these nodes are compromised, attackers may gain access to local data, manipulate device communication, or use the node as a bridge into wider enterprise systems.

Atlam et al. (2018) explained that fog computing supports IoT by bringing computation, storage, and networking closer to end devices, but this also creates concerns related to trust, authentication, privacy, and secure communication. Stergiou et al. (2018) also emphasized that IoT and cloud integration requires secure data exchange and protection across connected environments. These concerns become more complex when processing is spread across cloud, fog, and edge layers.

Zero Trust can support fog and edge security by requiring continuous device verification, secure communication, and distributed monitoring. Edge nodes should not be treated as automatically trusted simply because they are part of the enterprise architecture. They should be authenticated, monitored, patched, and governed by clear access policies. Communication between IoT devices, edge nodes, and cloud services should be encrypted and restricted to authorized flows.

A Zero Trust approach also helps ensure that compromised edge systems do not gain unrestricted access to the wider environment. Through segmentation and policy enforcement, organizations can limit what each edge node can access and what actions it can perform. Continuous monitoring can help detect abnormal traffic, unusual device behavior, or unexpected changes in edge workloads. As enterprises continue to adopt distributed computing models, securing fog and edge environments will become an important part of broader cloud, IoT, and hybrid enterprise protection.

Table 1: Security Challenges and Zero Trust Controls Across Enterprise Environments

Environment	Major Security Challenges	Relevant Zero Trust Controls	Supporting References
Cloud systems	Misconfiguration, account hijacking, insecure APIs, data leakage, shared infrastructure risks, and limited visibility	Identity-based access, encryption, workload monitoring, least privilege, and continuous policy enforcement	Hashizume et al. (2013); Fernandes et al. (2014); Tabrizchi and Kuchaki Rafsanjani (2020)
IoT systems	Weak authentication, insecure firmware, device constraints, poor patching, insecure communication, and large attack surfaces	Device identity, segmentation, secure onboarding, continuous monitoring, and anomaly detection	Roman et al. (2013); Sicari et al. (2015); Raza et al. (2013); Al-Garadi et al. (2020)
Hybrid enterprise systems	Fragmented policies, remote access risks, third-party exposure, inconsistent monitoring, and compliance complexity	Unified identity governance, continuous monitoring, least privilege, policy enforcement, and microsegmentation	Phiayura and Teerakanok (2023); Yeoh et al. (2023); Stergiou et al. (2018)
Fog and edge systems	Distributed nodes, localized processing risks, endpoint exposure, device trust issues, and insecure communication	Device verification, secure communication, edge monitoring, segmentation, and restricted access policies	Atlam et al. (2018); Stergiou et al. (2018)

7 Proposed Conceptual Framework

7.1 Framework Components

This article proposes a conceptual framework that integrates Zero Trust Architecture with identity threat detection for securing cloud, IoT, and hybrid enterprise systems. The framework is based on the idea that modern enterprise security should not depend on network location or one-

time authentication. Instead, security decisions should be based on verified identity, access context, device condition, behavioral risk, policy enforcement, and continuous monitoring.

The first component of the framework is the identity layer. This layer covers users, administrators, service accounts, IoT devices, APIs, and workloads. It is important because every access request begins with identity. In a modern enterprise environment, identity is not limited to human users. Applications, cloud workloads, connected devices, and automated services also require identities and permissions. Identity management therefore provides the foundation for deciding who or what is requesting access and whether that request should be trusted (Bertino & Takahashi, 2010).

The second component is the access control layer. This layer applies role-based access control, attribute-based access control, least privilege, and policy enforcement. Role-based access control remains useful because it assigns permissions according to organizational roles, while attribute-based access control allows access decisions to consider wider conditions such as user attributes, resource sensitivity, environmental context, and policy rules (Sandhu et al., 1996; Jin et al., 2012). In a Zero Trust setting, access control must be dynamic rather than static. Users and systems should not receive broad permissions that remain unchanged over time. Instead, access should be limited, reviewed, and adjusted according to need and risk.

The third component is the risk evaluation layer. This layer assesses the context of each access request. It considers factors such as device posture, user behavior, location, time of access, authentication strength, access history, and the sensitivity of the requested resource. Risk-based authentication is important here because it allows organizations to apply stronger controls when a request appears unusual or high risk. For example, an administrator logging in from an unfamiliar device or unusual location may be required to complete additional verification before access is granted (Dasu et al., 2023).

The fourth component is the threat detection layer. This layer uses anomaly detection, insider threat detection, SIEM, and intrusion detection to identify suspicious activity. It is not enough to approve access at the beginning of a session. The system must continue monitoring what happens after access is granted. If a user suddenly downloads unusual volumes of data, accesses restricted systems, or behaves differently from normal patterns, the threat detection layer should raise an alert or trigger a response. SIEM systems are particularly important because they collect and correlate security events across users, devices, networks, and applications (Bhatt et al., 2014).

The fifth component is the environment layer. This layer represents the different enterprise environments where Zero Trust controls must operate. These include cloud systems, IoT systems, edge nodes, and hybrid enterprise networks. Each environment has its own risks, but they must not be treated as separate security islands. Cloud systems require strong identity and workload governance, IoT systems require device trust and segmentation, and hybrid systems require

consistent access policies across on-premises and cloud platforms (Hashizume et al., 2013; Sicari et al., 2015; Stergiou et al., 2018).

The sixth component is the governance layer. This layer supports maturity assessment, compliance, policy review, monitoring, incident response, and continuous improvement. Zero Trust is not a one-time deployment. It requires planning, organizational readiness, technical integration, and regular evaluation. Phiayura and Teerakanok (2023) emphasized that migration to Zero Trust should follow a structured process, while Yeoh et al. (2023) showed that maturity assessment is important for understanding whether Zero Trust practices are actually effective in an organization.

Together, these six components create a security framework that places identity and risk at the center of enterprise protection. The framework is designed to help organizations move from static access control to continuous, adaptive, and evidence-based security.

7.2 Framework Operation

The proposed framework operates as a continuous security cycle. The process begins when a user, device, application, API, service account, or workload requests access to an enterprise resource. This resource may be located in the cloud, on-premises network, IoT environment, edge node, or SaaS platform. Instead of granting access based only on username and password, the framework first verifies the identity of the requester.

After identity verification, the framework evaluates the context of the request. This includes the device being used, the location of the request, the time of access, the sensitivity of the resource, the user's normal behavior, and the level of privilege being requested. This step is important because a valid identity does not always mean a safe request. A legitimate account may be compromised, or an authorized user may attempt to access resources beyond what is needed.

The next step is risk-based access decision-making. If the request is low risk and matches expected behavior, access may be granted with normal controls. If the request appears unusual, the system may require additional authentication, restrict access, limit session activity, or deny the request completely. This approach supports the Zero Trust principle of least privilege because access is not treated as a permanent right. It is treated as a conditional decision that depends on current risk.

Once access is granted, the framework continues to monitor the session. This is where identity threat detection becomes essential. SIEM tools, anomaly detection systems, intrusion detection techniques, and behavioral analytics can be used to identify suspicious activity during the session. For example, the system may detect abnormal data downloads, unusual login sequences, unauthorized privilege use, or communication with unexpected systems. If suspicious behavior is detected, the framework can update the risk score and trigger a response.

The response may include session termination, access restriction, administrator notification, account lockout, device isolation, or escalation to the incident response team. This continuous cycle makes the framework different from traditional access control models. Instead of assuming that access is safe once granted, the framework treats trust as temporary, conditional, and continuously evaluated.

Table 2: Components of the Proposed Zero Trust and Identity Threat Detection Framework

Framework Component	Function	Key Security Value	Supporting References
Identity layer	Verifies users, devices, workloads, APIs, and service accounts	Reduces unauthorized access by ensuring that every access request is tied to a known and verified identity	Bertino and Takahashi (2010); Dasu et al. (2023)
Access control layer	Applies RBAC, ABAC, least privilege, and policy enforcement	Limits privilege misuse and prevents unnecessary access to sensitive resources	Sandhu et al. (1996); Jin et al. (2012); Syed et al. (2022)
Risk evaluation layer	Evaluates context, behavior, device posture, access history, and resource sensitivity	Supports adaptive access decisions based on current risk rather than static permissions	Dasu et al. (2023); Ahmed et al. (2016)
Threat detection layer	Detects anomalies, insider threats, suspicious sessions, and intrusion patterns	Improves the ability to identify compromised accounts, abnormal behavior, and policy violations	Salem et al. (2008); Gheyas and Abdallah (2016); Bhatt et al. (2014)
Environment layer	Applies controls across cloud, IoT, edge, and hybrid enterprise systems	Supports consistent protection across distributed and interconnected environments	Hashizume et al. (2013); Sicari et al. (2015); Stergiou et al. (2018)
Governance layer	Supports maturity assessment, compliance, policy review, monitoring, and continuous improvement	Strengthens long-term resilience by making Zero Trust measurable, repeatable, and accountable	Phiayura and Teerakanok (2023); Yeoh et al. (2023)

8. Discussion

8.1 Benefits of Integrating Zero Trust and Identity Threat Detection

Integrating Zero Trust Architecture with identity threat detection offers a stronger approach to enterprise cybersecurity because it addresses both access control and threat visibility. Zero Trust reduces implicit trust by requiring users, devices, applications, and workloads to be verified before access is granted. Identity threat detection then extends this protection by monitoring how identities behave after access has been approved. This combination is important because many modern cyberattacks do not begin with obvious malware. They often begin with stolen credentials, compromised accounts, excessive privileges, or insider misuse.

A major benefit of this integration is stronger access governance. Organizations gain better control over who can access critical systems, what level of access they receive, and how that access is monitored. Buck et al. (2021) showed that Zero Trust research emphasizes the need to move away from automatic trust and toward continuous verification. Syed et al. (2022) also described Zero Trust Architecture as a comprehensive security model that depends on identity, policy enforcement, and ongoing validation. When identity threat detection is added to this model, organizations are better positioned to identify abnormal behavior that traditional access control may miss.

Another benefit is reduced lateral movement. In many attacks, the initial compromise is only the beginning. Attackers often use one account or device to move across the network in search of more valuable systems. Zero Trust limits this movement by enforcing least privilege and segmentation, while identity threat detection helps identify suspicious access patterns before the attacker reaches critical resources. This is especially important in cloud, IoT, and hybrid enterprise environments where systems are highly interconnected.

The integration also improves security visibility. Security teams can better understand identity behavior across cloud platforms, IoT systems, remote access tools, and enterprise applications. This visibility supports faster investigation and more accurate response. Yeoh et al. (2023) emphasized that Zero Trust success depends not only on technical controls but also on maturity, assessment, and organizational readiness. Identity threat detection supports this maturity by giving organizations measurable insight into access behavior, policy violations, and emerging risks.

8.2 Implementation Challenges

Although the integration of Zero Trust and identity threat detection offers clear benefits, implementation can be difficult. One major challenge is legacy infrastructure. Many organizations still depend on older systems that were not designed for continuous verification, identity-based access control, or modern monitoring. These systems may not support strong authentication, detailed logging, or integration with centralized identity platforms. As a result, applying Zero Trust controls across the entire enterprise can become technically complex.

Cost is another challenge. Implementing Zero Trust may require investment in identity management systems, multi-factor authentication, SIEM tools, endpoint security, network segmentation, cloud security platforms, and staff training. Adahman et al. (2022) noted that cost-effectiveness is an important issue in Zero Trust adoption because organizations must balance security improvements with financial and operational constraints. For smaller organizations, this can be a serious barrier.

Integration complexity is also a common problem. Cloud platforms, SaaS applications, IoT devices, on-premises networks, and remote access tools may all use different identity systems and security policies. Bringing these systems under one coherent Zero Trust model requires careful planning. Phiayura and Teerakanok (2023) argued that migration to Zero Trust should follow a structured approach because organizations need to align technology, processes, and security operations.

User friction is another practical concern. Stronger authentication and more frequent verification can improve security, but they may also frustrate users if poorly implemented. If employees are repeatedly interrupted by authentication requests or access restrictions, they may look for workarounds. For this reason, Zero Trust must be designed carefully so that security controls are risk-based and proportionate rather than unnecessarily disruptive.

Poor identity inventory is also a serious challenge. Many organizations do not have a complete understanding of all user accounts, service accounts, privileged accounts, APIs, devices, and workloads. Without this visibility, it is difficult to enforce least privilege or detect suspicious identity behavior. In IoT environments, unmanaged devices can make the problem worse because they may connect to the network without proper documentation or monitoring.

False positives can also weaken identity threat detection. Anomaly detection systems may flag legitimate behavior as suspicious, especially in organizations where work patterns vary widely. Too many false alerts can overwhelm security teams and reduce trust in the detection system. Yeoh et al. (2023) emphasized that maturity and readiness are important because Zero Trust requires not only tools but also governance, operational discipline, and continuous improvement.

8.3 Limitations of Threat Detection Technologies

Threat detection technologies are useful, but they are not perfect. Anomaly detection, machine learning, and intrusion detection systems can help identify suspicious behavior, but they also have limitations that organizations must recognize. One major limitation is false positives. Normal user behavior can change because of travel, new job responsibilities, emergency work, system updates, or business expansion. If detection systems are not carefully tuned, they may treat these legitimate changes as threats.

Another limitation is the difficulty of detecting unknown or subtle attack patterns. Some attackers deliberately behave slowly and carefully to avoid detection. They may use valid credentials, access systems during normal working hours, and imitate legitimate user behavior. This makes identity-based attacks harder to identify than attacks involving obvious malware or abnormal network traffic. Ahmed et al. (2016) explained that anomaly detection techniques face challenges related to accuracy, adaptability, and changing network behavior.

Machine learning also has practical limitations in cybersecurity. Buczak and Guven (2015) reviewed data mining and machine learning methods for intrusion detection and showed that these methods depend heavily on the quality of training data, feature selection, and evaluation conditions. Sommer and Paxson (2010) also warned that applying machine learning to network intrusion detection is difficult because real-world networks are open, changing, and complex. This means that models trained in one environment may not perform well in another.

Limited and biased datasets can also reduce detection accuracy. If a model is trained only on known attacks, it may struggle to detect new attack methods. If the data does not reflect the organization's actual environment, the model may produce unreliable results. Mishra et al. (2018) also noted that machine learning-based intrusion detection requires careful evaluation because performance can vary depending on the dataset, algorithm, and deployment context. Ferrag et al. (2020) further showed that deep learning approaches can support cybersecurity intrusion detection, but they require strong datasets and careful comparison before they can be trusted in operational settings.

For these reasons, identity threat detection should not be treated as a fully automated replacement for human judgment. It should support security analysts by identifying suspicious patterns, prioritizing risks, and providing useful context. Human review, governance, and incident response processes remain important, especially when dealing with high-impact access decisions or suspected insider threats.

8.4 Practical Implications for Enterprises

For enterprises, the practical value of Zero Trust lies in gradual and disciplined implementation. Organizations should not treat Zero Trust as a single product that can be purchased and installed. It is better understood as a security strategy that develops over time. A practical roadmap should begin with identity inventory. Organizations need to know which users, administrators, service accounts, devices, APIs, applications, and workloads exist before they can enforce meaningful access controls.

The next step is strengthening authentication. Multi-factor authentication should be applied first to high-risk accounts, privileged users, remote access systems, cloud platforms, and sensitive applications. After this, organizations should review access permissions and remove unnecessary privileges. Least privilege cannot work properly if accounts continue to hold broad access that is no longer needed.

Cloud configuration assessment should also be part of the early roadmap. Misconfigured cloud storage, excessive permissions, exposed APIs, and weak logging can create serious security gaps. Enterprises should review cloud identity and access management policies, enable logging, monitor workloads, and encrypt sensitive data. For IoT environments, organizations should

identify connected devices, remove unknown devices, segment device networks, and ensure that communication is properly secured.

SIEM integration is another important step. Security teams need centralized visibility across identity systems, cloud platforms, IoT networks, endpoints, and applications. SIEM tools can help correlate events and detect suspicious access behavior. Once basic visibility is established, organizations can move toward more advanced practices such as adaptive authentication, behavioral analytics, automated response, and continuous risk scoring.

Microsegmentation should also be introduced gradually. Enterprises can begin by segmenting high-risk systems, critical applications, IoT devices, and administrative environments. Over time, segmentation can be expanded to cloud workloads and hybrid networks. Phiayura and Teerakanok (2023) emphasized the importance of structured migration to Zero Trust, while Yeoh et al. (2023) showed that maturity assessment helps organizations evaluate progress and identify weaknesses.

In practical terms, enterprises should measure Zero Trust progress through clear indicators. These may include the percentage of users covered by multi-factor authentication, the number of privileged accounts reviewed, the level of cloud logging coverage, the number of unmanaged IoT devices discovered, the reduction in excessive permissions, and the speed of detecting suspicious identity behavior. This makes Zero Trust more accountable and helps organizations move from general security intention to measurable improvement.

9. Recommendations

Organizations should begin by treating identity as one of the most important security controls in modern enterprise protection. In cloud, IoT, and hybrid environments, access is no longer limited to users inside a fixed organizational network. It now includes employees, administrators, third-party users, service accounts, APIs, workloads, and connected devices. For this reason, identity should be managed as a core security boundary rather than as a basic login function. Strong identity governance can help organizations reduce unauthorized access, detect suspicious behavior, and control how users and systems interact with sensitive resources (Bertino & Takahashi, 2010; Dasu et al., 2023).

Organizations should also implement Zero Trust as a gradual security architecture rather than treating it as a single technology or product. Zero Trust requires changes in identity management, access control, monitoring, network segmentation, security policy, and organizational culture. A phased implementation allows organizations to assess their current maturity, identify critical assets, strengthen access policies, and improve visibility before moving to more advanced controls (Phiayura & Teerakanok, 2023; Yeoh et al., 2023). This approach is more realistic because many enterprises still operate with legacy systems, cloud platforms, remote access tools, and unmanaged devices that cannot be secured through one immediate deployment.

Least privilege access should be applied consistently across users, administrators, devices, APIs, and workloads. Every account or system should only receive the level of access required to perform its approved function. This reduces the damage that can occur when an account is compromised and limits the ability of attackers to move across enterprise systems. In practice, organizations should regularly review permissions, remove excessive privileges, restrict administrative access, and separate duties across sensitive systems (Syed et al., 2022; Yeoh et al., 2023).

Organizations should integrate both role-based access control and attribute-based access control into their Zero Trust strategy. Role-based access control is useful for assigning permissions according to job functions, while attribute-based access control provides more flexible decisions based on user identity, resource type, device posture, location, time, and risk level. Combining these models can help organizations make more accurate access decisions in complex cloud, IoT, and hybrid environments (Sandhu et al., 1996; Jin et al., 2012).

Risk-based authentication should be adopted for high-risk access scenarios. Instead of applying the same authentication process to every login attempt, organizations should evaluate the context of each access request. Factors such as device reputation, location, login time, user behavior, access history, and sensitivity of the requested resource should influence whether access is granted, denied, restricted, or challenged with additional verification. This strengthens Zero Trust because access decisions are based on real-time risk rather than static credentials alone (Dasu et al., 2023).

Continuous monitoring should also be made a central part of identity threat detection. Organizations should use security information and event management systems, behavioral analytics, and anomaly detection tools to monitor identity activity across cloud platforms, IoT devices, enterprise applications, and hybrid networks. These tools can help detect suspicious logins, privilege misuse, abnormal user behavior, and possible insider threats before they cause serious damage (Bhatt et al., 2014; Ahmed et al., 2016; Gheyas & Abdallah, 2016).

Microsegmentation should be used to reduce lateral movement within enterprise systems. Even when attackers compromise one account, device, or workload, they should not be able to move freely across the organization’s network. By dividing systems into smaller protected zones and enforcing access rules between them, organizations can limit the spread of attacks and protect critical resources more effectively (Syed et al., 2022; Zanasi et al., 2024).

Cloud configuration management and workload identity should also be strengthened. Many cloud security incidents are linked to misconfigured services, weak access policies, exposed APIs, and poor visibility over workloads. Organizations should enforce secure cloud configurations, monitor workload activity, protect API access, and apply identity-based controls to cloud services and machine identities. These practices are important for reducing data leakage,

account hijacking, and unauthorized access in cloud-based systems (Hashizume et al., 2013; Fernandes et al., 2014; Tabrizchi & Kuchaki Rafsanjani, 2020).

For IoT environments, organizations should secure devices through strong device identity, segmentation, lifecycle monitoring, and secure communication. IoT devices often have limited processing capacity, weak authentication, long service lives, and inconsistent patching. These weaknesses can expose enterprise systems to unauthorized access and network compromise. Therefore, each IoT device should be identified, monitored, segmented, and managed throughout its lifecycle (Roman et al., 2013; Sicari et al., 2015; Mosenia & Jha, 2016; Al-Garadi et al., 2020).

Finally, organizations should use maturity assessment to evaluate Zero Trust progress over time. Zero Trust implementation should be reviewed regularly to determine whether identity controls, access policies, monitoring systems, segmentation practices, and governance structures are improving. This helps organizations identify weaknesses, prioritize investment, and measure whether their security architecture is becoming more resilient (Yeoh et al., 2023). A maturity-based approach also ensures that Zero Trust becomes an ongoing security practice rather than a one-time implementation.

10. Conclusion

Cloud computing, IoT expansion, remote work, and hybrid enterprise systems have changed the way organizations design and manage cybersecurity. The traditional perimeter-based security model is no longer sufficient because users, devices, applications, and workloads now operate across distributed and constantly changing environments. In this context, protecting only the network boundary leaves organizations exposed to credential misuse, insecure devices, misconfigured cloud services, insider threats, and unauthorized access. Zero Trust Architecture offers a more suitable approach by removing implicit trust, verifying every access request, enforcing least privilege, and continuously monitoring activity across users, devices, workloads, and applications (Buck et al., 2021; Syed et al., 2022; Dhiman et al., 2024).

Identity threat detection strengthens Zero Trust by focusing on one of the most common paths used in modern cyberattacks: the misuse of legitimate identity. Attackers often rely on stolen credentials, compromised accounts, excessive privileges, and abnormal access behavior to bypass traditional controls. By using risk-based authentication, behavioral analytics, anomaly detection, SIEM monitoring, and insider threat detection, organizations can identify suspicious identity activity more effectively and respond before threats spread across enterprise systems (Bhatt et al., 2014; Ahmed et al., 2016; Gheyas & Abdallah, 2016; Dasu et al., 2023).

The proposed conceptual framework contributes to cybersecurity research by bringing together Zero Trust principles and identity-centered threat detection into a single model for cloud, IoT, and hybrid enterprise protection. The framework shows that effective security depends on the

interaction between identity verification, access control, device posture assessment, risk evaluation, continuous monitoring, threat detection, and governance. This integrated approach can help organizations reduce unauthorized access, limit lateral movement, improve visibility, and build stronger cyber resilience in modern enterprise environments.

Overall, Zero Trust should not be viewed as a quick technical upgrade but as a long-term security strategy. Its success depends on careful planning, strong identity governance, continuous monitoring, organizational commitment, and regular maturity assessment. As enterprise systems continue to become more distributed and identity-driven, organizations that combine Zero Trust Architecture with effective identity threat detection will be better positioned to protect critical assets, manage emerging risks, and respond to cyber threats in a more adaptive and resilient way.

References

1. Buck, C., Olenberger, C., Schweizer, A., Völter, F., & Eymann, T. (2021). Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust. Computers & Security, 110, 102436.
2. Syed, N. F., Shah, S. W., Shaghaghi, A., Anwar, A., Baig, Z., & Doss, R. (2022). Zero trust architecture (zta): A comprehensive survey. IEEE access, 10, 57143-57179.
3. Adahman, Z., Malik, A. W., & Anwar, Z. (2022). An analysis of zero-trust architecture and its cost-effectiveness for organizational security. Computers & Security, 122, 102911.
4. Phiayura, P., & Teerakanok, S. (2023). A comprehensive framework for migrating to zero trust architecture. Ieee Access, 11, 19487-19511.
5. Yeoh, W., Liu, M., Shore, M., & Jiang, F. (2023). Zero trust cybersecurity: Critical success factors and A maturity assessment framework. Computers & Security, 133, 103412.
6. Wylde, A. (2021, June). Zero trust: Never trust, always verify. In 2021 international conference on cyber situational awareness, data analytics and assessment (cybersa) (pp. 1-4). IEEE.
7. Dhiman, P., Saini, N., Gulzar, Y., Turaev, S., Kaur, A., Nisa, K. U., & Hamid, Y. (2024). A review and comparative analysis of relevant approaches of zero trust network model. Sensors, 24(4), 1328.
8. KOTA, S. K. (2022). A Real-World Deployment of an Enterprise Conversational AI Platform for Demand Generation and Lead Generation Using Guided Workflows with a Rasa-Based Chatbot. Frontiers in Computer Science and Artificial Intelligence, 1(1), 24-30.
9. Zanasi, C., Russo, S., & Colajanni, M. (2024). Flexible zero trust architecture for the cybersecurity of industrial IoT infrastructures. Ad Hoc Networks, 156, 103414.
10. Dasu, L. S., Dhamija, M., Dishitha, G., Vivekanandan, A., & Sarasvathi, V. (2023). Defending against identity threats using risk-based authentication. Cybernetics and Information Technologies, 23(2), 105-123.

11. Vallemoni, R. K. (2022). Authorization-to-settlement at scale: A reference data architecture for ISO 8583/ISO 20022 coexistence. Journal of Computer Science and Technology Studies, 4(1), 88-98.
12. Sandhu, R. S., Coyne, E. J., Feinstein, H. L., & Youman, C. E. (1996). Role-based access control models. Computer, 29(2), 38-47.
13. Jin, X., Krishnan, R., & Sandhu, R. (2012, July). A unified attribute-based access control model covering DAC, MAC and RBAC. In IFIP Annual Conference on Data and Applications Security and Privacy (pp. 41-55). Berlin, Heidelberg: Springer Berlin Heidelberg.
14. Bertino, E., & Takahashi, K. (2010). Identity management: Concepts, technologies, and systems. Artech House.
15. Gheyas, I. A., & Abdallah, A. E. (2016). Detection and prediction of insider threats to cyber security: a systematic literature review and meta-analysis. Big data analytics, 1(1), 6.
16. Ibimilua, A. F. (2008). The ideal design of a potentially safe community. Journal of Applied Security Research, 4(1-2), 129-140.
17. Salem, M. B., Hershkop, S., & Stolfo, S. J. (2008). A survey of insider attack detection research. Insider Attack and Cyber Security: Beyond the Hacker, 69-90.
18. Bhatt, S., Manadhata, P. K., & Zomlot, L. (2014). The operational role of security information and event management systems. IEEE security & Privacy, 12(5), 35-41.
19. Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A survey of network anomaly detection techniques. Journal of network and computer applications, 60, 19-31.
20. ALAMPALLY, J. (2024). Real-Time and Near-Real-Time Analytics in Healthcare Data Ecosystems. Journal of Computer Science and Technology Studies, 6(1), 314-324.
21. Nagraj, A. (2024). GraphQL in Wealth Management Platforms: Optimizing Data Access and Performance. British Journal of Multidisciplinary Studies, 2(1), 16-24.
22. Malone, K., Saveen, S., Stevens, C. M., McNeil, S., Malone, K. T., Sall, S., & McNeil, S. E. (2022). Successful treatment of catatonia: a case report and review of treatment. Cureus, 14(6).
23. Buczak, A. L., & Guven, E. (2015). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications surveys & tutorials, 18(2), 1153-1176.
24. Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. Journal of internet services and applications, 4(1), 5.
25. Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of network and computer applications, 34(1), 1-11.
26. Vallemoni, R. K. (2023). Merchant Onboarding and Risk Scoring: Data Governance, Master Data, and Golden-Record Strategies. Below the Content is Description.

27. Almorsy, M., Grundy, J., & Müller, I. (2016). An analysis of the cloud computing security problem. arXiv preprint arXiv:1609.01107.
28. Tabrizchi, H., & Kuchaki Rafsanjani, M. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. The journal of supercomputing, 76(12), 9493-9532.
29. Stergiou, C., Psannis, K. E., Kim, B. G., & Gupta, B. (2018). Secure integration of IoT and cloud computing. Future generation computer systems, 78, 964-975.
30. Ristenpart, T., Tromer, E., Shacham, H., & Savage, S. (2009, November). Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. In Proceedings of the 16th ACM conference on Computer and communications security (pp. 199-212).
31. Nagraj, A. (2022). Modernizing Legacy Banking Systems: Migration Strategies and Cost Optimization in Financial Enterprises. Frontiers in Computer Science and Artificial Intelligence, 1(1), 43-52.
32. MARASANI, Y. (2023). Machine Learning Models for Predicting Patient Treatment Switching Using Claims Data. Frontiers in Computer Science and Artificial Intelligence, 2(1), 59-66.
33. Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: state-of-the-art and research challenges. Journal of internet services and applications, 1(1), 7-18.
34. Fernandes, D. A. B., Soares, L. F. B., Gomes, J. V., Freire, M. M., & Inácio, P. R. M. (2014). Security issues in cloud environments: A survey. International Journal of Information Security, 13, 113–170. https://doi.org/10.1007/s10207-013-0208-7
35. Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. Computer networks, 57(10), 2266-2279.
36. Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. Computer networks, 76, 146-164.
37. Raza, S., Wallgren, L., & Voigt, T. (2013). SVELTE: Real-time intrusion detection in the Internet of Things. Ad hoc networks, 11(8), 2661-2674.
38. Al-Garadi, M. A., Mohamed, A., Al-Ali, A. K., Du, X., Ali, I., & Guizani, M. (2020). A survey of machine and deep learning methods for internet of things (IoT) security. IEEE communications surveys & tutorials, 22(3), 1646-1685.
39. Mosenia, A., & Jha, N. K. (2016). A comprehensive study of security of internet-of-things. IEEE Transactions on emerging topics in computing, 5(4), 586-602.
40. Atlam, H. F., Walters, R. J., & Wills, G. B. (2018). Fog computing and the internet of things: A review. big data and cognitive computing, 2(2), 10.
41. Sommer, R., & Paxson, V. (2010, May). Outside the closed world: On using machine learning for network intrusion detection. In 2010 IEEE symposium on security and privacy (pp. 305-316). IEEE.
42. ALAMPALLY, J. (2024). Enhancing data quality and trust in AI systems through robust data engineering. Frontiers in Computer Science and Artificial Intelligence, 3(1), 120-130.

43. Vallemoni, R. K. (2022). Canonical payment data models for merchant acquiring: Merchants, terminals, transactions, fees, and chargebacks. International Journal of Computer Science and Engineering (ISCSITR-IJCSE), 3(1), 42-66.
44. Mishra, P., Varadharajan, V., Tupakula, U., & Pilli, E. S. (2018). A detailed investigation and analysis of using machine learning techniques for intrusion detection. IEEE communications surveys & tutorials, 21(1), 686-728.
45. Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. Journal of Information Security and Applications, 50, 102419.