Advancing Zero Trust for SMEs: A Review of Short-Lived Certificates, MFA, and Lightweight Identity Solutions

Kenneth Nnadi[1], Yaw Agyekumhene Okrah[2], Jochebed Akoto Opoku[3]

[1]University of Oregon, USA
[2]Taskimpetus Inc- New Orleans, LA, USA
[3]Department of Telecommunication Engineering, Kwame Nkrumah University of Science and Technology, Ghana
[1]kennethnnadi14@gmail.com, [2]oagyekumhene@gmail.com, [3]opokujochebedakoto@gmail.com
Corresponding author: Jochebed Akoto Opoku

Abstract:
Small and medium-sized enterprises (SMEs) face growing cybersecurity threats but lack the financial and technical resources to implement complex security architectures. Traditional perimeter-based models fail in today's cloud-driven and remote work environments, leaving SMEs vulnerable to credential theft, phishing, and ransomware attacks. Zero Trust offers a promising alternative by enforcing continuous verification and least-privilege access; however, most implementations assume enterprise-scale infrastructure, making them impractical for SMEs. This review addresses that gap by focusing on three identity-centric mechanisms that enable Zero Trust adoption without excessive complexity: short-lived certificates, multi-factor authentication (MFA), and lightweight identity solutions. Short-lived certificates minimize credential exposure by limiting validity periods and reducing reliance on revocation processes. MFA improves identity security by reducing phishing risk and limiting damage from reused passwords. Lightweight identity platforms, such as cloud-based identity providers, centralize authentication and enforce policies with minimal administrative work. By synthesizing best practices and empirical findings, this paper presents how these measures can be combined into a practical, identity-centric Zero Trust approach suitable for SMEs. It evaluates security benefits, usability trade-offs, and deployment challenges, highlighting automation as a key enabler for reducing operational burden. The review concludes with adoption considerations and future directions, including decentralized identity and AI-driven risk scoring, offering SMEs a roadmap to achieve robust, identity-driven security within resource constraints.

Keywords: Multi-Factor Authentication, Zero Trust Architecture, Lightweight Identity Management, Identity-Centric Security, Short-Lived Certificates.

1. INTRODUCTION

Zero trust is a security concept that rejects implicit assumptions in a network and instead requires constant verification of all access requests, independent of user location, device, or network environment. Traditional perimeter-based approaches assume that users within the corporate network are trustworthy, resulting in systemic flaws when an attacker breaches the perimeter through phishing, stolen credentials, or compromised endpoints (Lee et al., 2025; Rose et al., 2020). Zero Trust mitigates these limitations by emphasizing identity-based controls rather than network location. Authentication and authorization are constantly reviewed using a variety of criteria, including user identity, device health, application sensitivity, and contextual risk (Mehra, 2024; Garbis & Chapman, 2021). The increasing adoption of cloud computing, software-as-a-service (SaaS), and remote work has reduced the effectiveness of perimeter-centric security (Ahmed et al., 2026 a,b). Organizational resources are now spread across hybrid and multi-cloud systems, making network boundaries leaky and challenging to establish (Borah, 2015; Kang et al., 2023). In this context, Zero Trust offers a framework for lowering blast radius, preventing lateral movement, and mitigating the impact of credential

compromise by requiring least-privilege access and ongoing authentication (Rose et al., 2020; Homoliak et al., 2019).

Small and medium-sized businesses (SMEs) confront cybersecurity challenges. They continue to be attacked by advanced malware despite a lack of financial, technical, and human resources comparable to large corporations (Tetteh-Kpakpah et al., 2025; Nnadi et al., 2025). Empirical studies reveal that SMEs are disproportionately affected by phishing, ransomware, and business email compromise attacks, owing to poorer identity controls and insufficient security monitoring capabilities (Bada et al., 2019; für Netz-und, 2021; Mansfield-Devine, 2022). Despite this increased risk, SMEs frequently use password-based authentication, shared credentials, and flat network designs, which multiply the impact of a single account compromise (Taşan-Kok, 2025; Mujtaba et al., 2025). Many Zero Trust implementations described in the literature presuppose enterprise-scale infrastructures, such as complicated public key infrastructures, specialized security operations centers, and ongoing threat intelligence feeds (Lee et al., 2025; Garbis & Chapman, 2021). Such assumptions are not consistent with SME realities, in which security tasks are usually handled by general IT personnel or external service providers. As a result, SMEs demand security solutions that prioritize automation, low administrative overhead, and user-friendly design while remaining true to Zero Trust principles (für Netz-und, 2021; Baig & Eskeland, 2021). Lightweight identity-centric controls, such as short-lived credentials, multi-factor authentication, and cloud-based identity services, show promise for balancing security efficacy and operational feasibility in SME environments.

This review focuses on identity-centered techniques that enable effective Zero Trust adoption for SMEs while avoiding enterprise-level complexity. It focuses on the role of short-lived certificates, multi-factor authentication (MFA), and lightweight identity solutions as basic controls for imposing continuous verification and least-privileged access. Prior evaluations of Zero Trust have focused mostly on architectural models, policy enforcement frameworks, or large-scale enterprise deployments, with little attention paid to SME-specific restrictions and usability issues (Rose et al., 2020; Homoliak et al., 2019; Kang et al., 2023). This study provides three contributions. First, it reviews studies on identity management, authentication techniques, and certificate-based security to determine their applicability for SME environments. Second, it weighs security benefits, usability trade-offs, and deployment complexity to highlight design decisions that reduce credential exposure and administrative overhead. Finally, it outlines research gaps in automation, user experience, and integration difficulties that are currently unexplored in SME-focused Zero Trust literature. This paper seeks to bridge the gap between Zero Trust theory and deployable security practice for resource-constrained businesses by combining disparate findings into a cohesive identity-centric perspective.

2. ZERO TRUST AND IDENTITY-CENTRIC SECURITY

Zero Trust has emerged as a transformative approach to cybersecurity, challenging traditional perimeter-based models that assume internal trust. This section explores why identity-centric security is foundational to Zero Trust and how it reshapes access control in modern environments. As organizations move toward cloud services and remote work, network boundaries have become porous, making identity the most reliable anchor for security decisions. We will examine the principles that underpin Zero Trust and their practical implications for SMEs, which often lack the resources for complex architectures. By understanding these principles, SMEs can prioritize controls that deliver strong security without excessive operational burden. The following subsections detail core Zero Trust concepts, identity's role as the new perimeter, and adoption differences between large enterprises and SMEs

2.1 Core Zero Trust Principles

Zero Trust is based on the premise that no user, device, or program should be implicitly trusted, even if it is part of an organizational network. Early Zero Trust formulations stressed the eradication of trust based on network location in favor of continual access request verification using contextual and identity-based signals (Lee et al., 2025). Later frameworks, especially NIST SP 800-207, formalize this notion by defining Zero Trust as an architecture that ensures least-privilege access, continuous authentication, and dynamic policy enforcement across all resources (Rose et al., 2020). Rather than depending on static credentials or one-time

authentication events, Zero Trust systems continuously assess trust based on identity traits, device posture, session behavior, and resource sensitivity.

The primary purpose of Zero Trust is to decrease the blast radius of breaches by prohibiting lateral migration after the first compromise. Empirical investigations of contemporary breaches reveal that attackers frequently use valid credentials to travel laterally within trusted networks, rendering perimeter measures ineffectual after initial access is acquired. Zero Trust addresses this by requiring micro-segmentation and per-request authorization, which ensures that access to one resource does not imply access to another. These concepts are especially important in systems dominated by cloud services and remote access, where traditional network boundaries are challenging to define and enforce (Homoliak et al., 2019, Panful et al., 2025 a,b,c). To contextualize these principles for resource-constrained environments, Table 1 summarizes core Zero Trust concepts and their practical implications for SMEs.

Table 1. Core Zero Trust principles and their implications for SMEs

Zero Trust principle	Description	Implications for SMEs
No implicit trust	No user or device is trusted by default	Design implies identity verification even for internal users
Least-privilege access	Users receive only the minimum necessary access	aim to reduce damage from compromised accounts
Continuous verification	Access is evaluated throughout a session	Encourages MFA and short-lived credentials
Assume breach	Systems are designed expecting compromise	Shifts focus on containment, not prevention
Identity-centric control	Identity is the primary security anchor	Favors cloud IAM and lightweight identity tools

2.2 Identity as the New Security Perimeter

As enterprise IT systems have evolved to cloud computing, SaaS apps, and remote work, identity has emerged as the primary control plane for security enforcement (Mehra, 2024; Rose et al., 2020). As a result, Zero Trust designs make identity, not network location, the primary determinant of access decisions. Identity-centric security is based on robust authentication, fine-grained authorization, and continuous identity validation. According to research, credential compromise is the most common initial access vector in modern assaults, primarily through phishing and credential reuse. Zero Trust architecture directly addresses this dominant attack surface by enhancing identity assurance with technologies such as MFA, certificate-based authentication, and context-aware access rules. Identity-centric approaches also allow for more granular policy enforcement by linking access privileges to user roles, device trust levels, and real-time risk signals, rather than static IP addresses or network zones (Garbis & Chapman, 2021). In Zero Trust systems, identification extends beyond human users to devices, workloads, and services. This broader definition of identity is crucial for cloud-native and API-driven contexts, where machine-to-machine communication is common and frequently inadequately verified using long-lived secrets (Kang et al., 2023). Identity-centric Zero Trust encourages the use of short-lived credentials, automated identity provisioning, and robust authentication for both human and non-human actors.

While positioning identity as the primary control plane strengthens access decisions in cloud and remote-first environments, it also concentrates risk; misconfigurations or credential compromise at the identity tier can propagate broadly across applications and services. To avoid turning identity into a single point of failure, Zero Trust treats strong identity as necessary but not sufficient. In practice, this means coupling robust authentication with continuous verification of sessions and context so that trust is re-evaluated throughout access, not granted once and assumed indefinitely. It also means enforcing least privilege and segmentation so that even a valid identity cannot move laterally without meeting granular policy checks. Together, these

measures ensure identity remains the "new perimeter" without becoming a monoculture of risk, aligning with Zero Trust's architectural intent of ongoing, risk-aware authorization rather than static, all-or-nothing trust.

2.3 Differences Between Enterprise and SME Zero Trust Adoption

While Zero Trust concepts are universally applicable, their execution varies significantly across large businesses and SMEs. Enterprise Zero Trust installations often presume the presence of specialized security teams, advanced monitoring infrastructure, and sophisticated policy orchestration platforms (Lee et al., 2025; Garbis & Chapman, 2021). These settings frequently combine Zero Trust with large-scale public key infrastructures, constant threat information feeds, and security operations centers capable of handling high operational complexity.

In contrast, SMEs face substantially tighter budgetary, expertise, and administrative limitations. Multiple studies have found that SMEs frequently lack formal identity governance mechanisms and rely extensively on password-based authentication and ad hoc access controls (Mujtaba et al., 2025; für Netz-und, 2021). As a result, directly implementing enterprise-grade Zero Trust architecture can add unnecessary complexity and even compromise security if systems are misconfigured or poorly managed. Researchers are increasingly emphasizing the need for simple, automated, and cloud native Zero Trust techniques that reduce operational overhead while maintaining key security assurances (Baig & Eskeland, 2021).

For SMEs, Zero Trust adoption means focusing on high-impact identity controls rather than implementing every architectural component defined in corporate frameworks. Lightweight identity solutions, cloud-based IAM platforms, MFA, and short-lived credentials enable SMEs to achieve Zero Trust without requiring costly on-premises infrastructure. This practical adaptation is consistent with previous guidelines promoting risk-based and resource-aware security architectures for smaller businesses (für Netz-und, 2021; Taşan-Kok, 2025).

3. COMMON ATTACK VECTORS TARGETING SMES

Small and medium-sized businesses (SMEs) are increasingly being targeted by cyber attackers, not because they are less valuable, but because they are more easily compromised. Empirical breach assessments continually reveal that SMEs are frequently targeted by phishing, ransomware, business email compromise (BEC), and malware-based intrusions, which can have serious operational and financial effects (Mansfield-Devine, 2022; für Netz-und, 2021). Unlike large organizations, SMEs generally lack layered defenses and continual monitoring, allowing attackers to achieve their goals using relatively easy approaches. Opportunistic attacks dominate this domain, with adversaries employing automated scanning, phishing campaigns, and credential-stuffing attacks at scale rather than custom exploits (Anderson et al., 2019).

Ransomware has become especially destructive to SMEs due to insufficient backup infrastructure and inadequate incident response skills. According to research, SMEs are less likely to have offline backups or tested recovery strategies, increasing the risk of ransom payment and protracted outage (Seng et al., 2024; für Netz-und, 2021). Email-based assaults remain the most prevalent first access vector, owing to email's continued use as a principal communication channel and the widespread use of password-based authentication without extra precautions (Bada et al., 2019). These attack vectors take advantage of not just technical flaws, but also organizational and human issues, such as inadequate security awareness training and informal access management methods.

These attack patterns explain why identity-centric protections outperform network-based controls for SMEs. The most successful breaches begin with phishing, credential reuse, or account takeover. As a result, the user or service identification, rather than the internal network boundary, serves as the primary control point. Stronger identity assurance directly addresses these concerns. MFA, shorter credential lives, and centralized authentication all help to eliminate the need for passwords and session trust. Perimeter protections suffer when an attacker utilizes valid credentials within the network. In reality, identity-focused restrictions limit the attacker's window of opportunity by limiting the duration of credential validity. They also impede lateral movement through least-privilege access. Continuous verification aids in maintaining control over the course

of a session. This strategy works effectively for SMEs, especially when monitoring resources are limited and the blast radius must be restricted.

3.1 Identity-Based Attacks and Credential Abuse

Identity-based attacks are currently the primary method by which attackers compromise SME environments. Large-scale breach investigations routinely demonstrate that a majority of successful attacks include stolen or misused credentials, particularly in cloud and hybrid environments (Mansfield-Devine, 2022; Roy et al., 2021). Phishing attacks aimed at SMEs are extremely effective because attackers only need one valid credential to breach perimeter security and gain access to many internal and cloud-based resources. Once credentials are compromised, attackers can impersonate legitimate users, making detection much more difficult (Homoliak et al., 2019).

Credential reuse and long-lived credentials exacerbate this issue. SMEs frequently reuse passwords across services and rely on static credentials that are valid for long periods of time, giving attackers a larger window of opportunity (Florêncio & Herley, 2010). In setups that lack multi-factor authentication or contextual access controls, attackers can easily escalate privileges, move laterally, and deploy ransomware or data exfiltration tools. Identity abuse is not restricted to human users; service accounts, API keys, and machine identities are commonly over-privileged and inadequately managed, resulting in new attack routes that SME administrators are rarely aware of (Kang et al., 2023). These realities demonstrate why Zero Trust designs prioritize identity assurance, credential minimization, and continuous verification. Organizations can mitigate the impact of identity breaches by decreasing credential durations and ensuring robust authentication, even when initial access is granted (Rose et al., 2020).

3.2 Practical Constraints: Cost, Skills, and Infrastructure

Despite the elevated threat level, SMEs have substantial constraints that influence their security posture. Cost remains a major barrier, since many modern security solutions are priced and developed for enterprise systems (Mujtaba et al., 2025). Small and medium-sized enterprises (SMEs) usually rely on small IT teams or external managed service providers, which limits their ability to build and maintain complicated security architecture. As a result, security procedures are frequently reactive, fragmented, and geared toward compliance rather than risk mitigation (für Netz-und, 2021).

Skills shortages exacerbate these issues. According to research, SMEs struggle to recruit and retain cybersecurity personnel, resulting in reliance on default configurations and limited policy tailoring (Baig & Eskeland, 2021). Infrastructure constraints are also important, especially for enterprises that are migrating to cloud services without revamping their identity and access policies. Legacy applications, a lack of centralized identity management, and limited automation capabilities make it difficult to apply uniform security policies across people, devices, and services (Taşan-Kok, 2025).

These limits highlight the need for security techniques that reduce administrative overhead while mitigating the most common attack vectors. Identity-centric Zero Trust controls, such as MFA, short-lived credentials, and cloud-based identity platforms, directly address dominant SME vulnerabilities while adhering to practical constraints like cost, skills, and infrastructure.

Table 2. Common SME cyber threats, attack methods, and impacts

Threat category	Primary attack method	Typical SME impact
Phishing	Deceptive emails capturing credentials	Account compromise, data exposure
Ransomware	Malicious payload via email or RDP	Business disruption, financial loss
Business email compromise	Spoofed or hijacked email accounts	Fraud, financial theft
Credential stuffing	Reused passwords across services	Unauthorized access to cloud systems

Malware	Drive-by downloads or attachments	System downtime, data loss
Insider misuse	Misuse of legitimate credentials	Data leakage, compliance violations

4. SHORT-LIVED CERTIFICATES IN ZERO TRUST

Short-lived certificates are cryptographic credentials with deliberately brief validity periods, typically ranging from minutes to hours, rather than months or years. Unlike passwords, which rely on shared secrets that can be easily guessed or phished, certificate-based identity uses asymmetric cryptography, ensuring authentication depends on possession of a private key rather than knowledge of a static credential. They are used to authenticate users, devices, services, or workloads without relying on static secrets such as passwords or long-lived private keys. In Zero Trust architectures, short-lived certificates serve as dynamic identity assertions that are continuously renewed based on successful authentication and policy evaluation (Rose et al., 2020; Sakimura et al., 2021). The lifecycle of a short-lived certificate generally begins with identity verification through an identity provider, often combined with MFA or device attestation. Once verified, a certificate is issued automatically and used for mutual authentication to access resources. Upon expiration, the certificate becomes invalid, requiring re-authentication before access can continue.

While certificates in Zero Trust architecture are intentionally short-lived, the associated private keys may remain long-lived if securely stored, reducing operational complexity without weakening security. This lifecycle aligns closely with Zero Trust principles because it treats access as temporary and conditional rather than persistent. Unlike traditional public key infrastructure (PKI) deployments, where certificates may remain valid for years, short-lived certificate systems minimize reliance on revocation mechanisms such as certificate revocation lists (CRLs) or online certificate status protocol (OCSP) checks, which are often complex and unreliable in practice (Wang et al., 2020). By design, compromise impact is bound by the certificate's short validity window, making credential theft significantly less valuable to attackers.

4.1 Security Advantages over Long-Lived Certificates

The primary security advantage of short-lived certificates lies in their reduced attack window. Long-lived certificates and static credentials allow attackers extended periods to exploit stolen keys, often without detection, particularly in environments with limited monitoring capabilities such as SMEs (Mansfield-Devine, 2022). Studies of credential misuse show that attackers frequently retain access for weeks or months before being discovered, especially when credentials do not expire automatically (Florêncio & Herley, 2010). Short-lived certificates sharply constrain this dwell time, forcing attackers to re-authenticate frequently and increasing the likelihood of detection or denial.

Short-lived certificates also reduce the operational and security risks associated with revocation. Traditional PKI assumes that compromised certificates can be revoked promptly, but real-world evidence demonstrates that revocation mechanisms are inconsistently enforced and often ignored by clients (Wang et al., 2020). By contrast, short-lived certificates expire naturally, eliminating dependence on revocation infrastructure. In Zero Trust systems, this enables stronger enforcement of least privilege and continuous verification, as certificates can be scoped narrowly to specific resources and privileges (Rose et al., 2020; Kang et al., 2023).

4.2 Certificate Automation and Management

The practical viability of short-lived certificates depends heavily on automation. Manual certificate issuance and renewal processes are infeasible when certificates expire frequently, making automated identity verification, issuance, and rotation essential components of Zero Trust architectures (Sakimura et al., 2021; Kang et al., 2023). Modern implementations leverage automated protocols and identity-aware systems that issue certificates dynamically after successful authentication, often integrating with cloud identity providers and workload orchestration platforms.

Automation not only reduces administrative burden but also improves security by eliminating human error, which remains a major cause of certificate misconfiguration and key leakage (für Netz-und, 2021). Research indicates that automated credential rotation significantly reduces the likelihood of unnoticed credential compromise and mismanagement, particularly in environments without dedicated security teams (Borah,

2015). For SMEs, automation transforms certificate-based authentication from an enterprise-only mechanism into a deployable Zero Trust control, provided the underlying tooling abstracts complexity away from administrators.

4.3 SME Adoption Challenges

Despite their security advantages, short-lived certificates present adoption challenges for SMEs. The most significant barrier is the perceived complexity of PKI and certificate management, which has historically been associated with enterprise-scale infrastructure and specialized expertise (Mujtaba et al., 2025). SMEs may lack familiarity with certificate-based authentication and may rely instead on password-centric systems that appear simpler to manage. Without appropriate automation and integration, short-lived certificates can introduce operational friction and authentication failures.

Cost and tooling limitations further influence adoption. While open-source and cloud-native solutions have reduced entry barriers, SMEs must still invest in identity platforms capable of issuing and validating certificates at scale (für Netz-und, 2021). Legacy applications that do not support certificate-based authentication may also restrict deployment options, requiring hybrid approaches that combine certificates with traditional credentials. These challenges underscore the importance of lightweight identity solutions that integrate short-lived certificates seamlessly into existing SME workflows, aligning strong security guarantees with operational feasibility.

5. MULTI-FACTOR AUTHENTICATION (MFA) FOR SMES

Authentication remains one of the most critical components of any security architecture, and for SMEs, it is often the weakest link. This section introduces multi-factor authentication (MFA) as a practical and highly effective control for reducing identity-related risks. MFA strengthens security by requiring multiple forms of verification, making credential theft significantly less damaging. For SMEs, which frequently rely on password-only systems, MFA offers a cost-effective way to align with Zero Trust principles without major infrastructure changes. We will explore the fundamentals of MFA, its role in Zero Trust, and the trade-offs SMEs must consider when deploying it. Real-world examples and mitigation strategies for common MFA bypass techniques will also be discussed.

5.1 MFA Fundamentals and Authentication Factors

Multi-factor authentication (MFA) is an authentication mechanism that requires users to present two or more independent forms of evidence to verify their identity before granting access. These factors are commonly classified into three categories: knowledge-based factors, such as passwords or PINs; possession-based factors, including hardware tokens or mobile devices; and inherence-based factors, which encompass biometric characteristics (Cherekar, 2025; Pandey et al., 2023). The security rationale behind MFA is that compromising multiple independent factors simultaneously is significantly more difficult than stealing a single credential, particularly in environments dominated by phishing and credential reuse attacks.

In SME environments, authentication has historically relied on single-factor, password-based mechanisms due to their simplicity and low cost. However, extensive empirical research demonstrates that passwords alone provide insufficient protection against modern attacks, as users frequently reuse passwords across services and choose low-entropy credentials that are vulnerable to guessing and credential-stuffing attacks (Florêncio & Herley, 2010; Kollek, 2025). MFA directly addresses these weaknesses by introducing additional verification layers that remain effective even when passwords are compromised. As cloud adoption increases among SMEs, MFA has become one of the most accessible and impactful controls for strengthening identity assurance without requiring extensive infrastructure changes.For example, an SME using a cloud-based SaaS platform for accounting or CRM can implement MFA by requiring employees to log in with a password plus a mobile app push notification. Similarly, remote administrative access to internal systems can be protected by combining a password with a hardware token or biometric check, ensuring that even if credentials are phished, attackers cannot gain entry without the second factor.

5.2 MFA as a Zero Trust Control

Within Zero Trust architectures, MFA is not merely an optional enhancement but a foundational control for enforcing continuous verification. Zero Trust explicitly assumes that credentials may be compromised and therefore requires strong authentication at every access point, regardless of network location (Rose et al., 2020). MFA supports this model by reducing reliance on static credentials and enabling risk-based authentication decisions that consider user identity, device posture, and contextual signals such as location or behavior (Mehra, 2024; Garbis & Chapman, 2021).

Research indicates that MFA significantly reduces the success rate of account takeover attacks, particularly those based on phishing and credential stuffing (Pandey et al., 2023; Mansfield-Devine, 2022). In Zero Trust deployments, MFA is often enforced not only at initial login but also during sensitive actions, such as privilege escalation or access to high-value resources. For SMEs, this layered enforcement is particularly valuable because it compensates for limited monitoring and incident response capabilities. By integrating MFA with cloud-based identity providers, SMEs can approximate Zero Trust outcomes by ensuring that access decisions are continually revalidated rather than implicitly trusted.

5.3 Usability, Cost, and Deployment Trade-Offs

Despite its security benefits, MFA adoption introduces trade-offs related to usability, cost, and deployment complexity. User friction remains one of the most frequently cited barriers to MFA adoption, as additional authentication steps can disrupt workflows and reduce user satisfaction (Baig & Eskeland, 2021). Studies on usable security show that authentication mechanisms perceived as inconvenient are more likely to be bypassed or resisted by users, undermining their effectiveness (Kollek, 2025). For SMEs, where IT policies are often informally enforced, balancing security strength with usability is critical.

Cost considerations also influence MFA deployment decisions. Hardware-based tokens and biometric systems typically offer strong security but may be prohibitively expensive or logistically challenging for SMEs, especially those with remote or distributed workforces (Mujtaba et al., 2025). Software-based MFA solutions, such as push notifications or one-time passwords delivered via mobile apps, provide a more cost-effective alternative but may be vulnerable to certain attack techniques if not carefully configured.

5.4 MFA Failures and Bypass Techniques

Although MFA substantially improves security, it is not immune to attack. Research has documented several techniques that adversaries use to bypass or weaken MFA protections, particularly in environments with limited security awareness or monitoring (Ometov et al., 2018). Phishing attacks that proxy authentication sessions in real time can capture MFA tokens or approvals, allowing attackers to authenticate as legitimate users despite MFA enforcement (Pandey et al., 2023). Similarly, push-based MFA systems are vulnerable to "push fatigue" attacks, where repeated authentication requests pressure users into approving malicious login attempts (Baig & Eskeland, 2021).

Other weaknesses arise from poor implementation practices, such as fallback to single-factor authentication, over-reliance on SMS-based OTPs, or lack of contextual checks during MFA validation (für Netz-und, 2021). These failures underscore the importance of combining MFA with additional Zero Trust controls, including device trust evaluation, short-lived credentials, and behavioral monitoring. Table 3 summarizes common MFA attack techniques and corresponding mitigation strategies relevant to SME environments.

It is important to note that these weaknesses arise primarily from poor implementation practices rather than inherent flaws in MFA itself; when deployed correctly with phishing-resistant factors and robust policies, MFA remains one of the most effective controls for preventing credential-based attacks.

Table 3. Common MFA attacks and mitigation strategies

MFA attack technique	Description	Mitigation strategy
Phishing with MFA proxy	Real-time capture of MFA responses	FIDO2/WebAuthn, phishing-resistant MFA
Push fatigue	Repeated push requests to induce approval	Rate limiting, user training
SIM swapping	Hijacking SMS-based MFA	Avoid SMS MFA, use app-based or hardware MFA
MFA downgrade	Forced fallback to single-factor auth	Enforce mandatory MFA policies
Token replay	Reuse of intercepted OTPs	Short validity windows, contextual checks

6. LIGHTWEIGHT IDENTITY SOLUTIONS

Identity management is often overlooked in SMEs, yet it is central to achieving Zero Trust. Traditional enterprise IAM systems are complex and resource-intensive, making them impractical for smaller organizations. This section examines lightweight identity solutions that simplify authentication and policy enforcement while maintaining strong security guarantees. These solutions leverage cloud-native platforms, automation, and usability-focused design to reduce administrative overhead. By adopting lightweight identity systems, SMEs can centralize authentication, enforce least privilege, and integrate seamlessly with cloud applications. The subsections will define lightweight identity, explore cloud-based IAM services, and analyze their limitations and mitigation strategies

6.1 Defining Lightweight Identity for SMEs

Identity and access management (IAM) techniques are used to implement lightweight identity systems. They offer robust authentication, and authorization guarantees and also want to reduce deployment complexity, costs, and administrative overhead. This differs from standard enterprise identity and access management systems. These systems frequently rely on on-premises directories and may entail complicated public key infrastructures and considerable policy engineering. Lightweight identity solutions prioritize cloud-native operation, automation, and usability (Mehra, 2024; Garbis & Chapman, 2021). For SMEs, "lightweight" does not imply lower security but a lower operating strain. These solutions simplify the effort required to run identities securely and frequently disguise cryptographic complexity and policy enforcement behind managed services. This enables enterprises with less security experience to implement current identity-centric policies. According to research on SME cybersecurity, identity management is one of the weakest control areas. However, it is also one of the most critical areas to address, and many SMEs employ ad hoc user provisioning, shared accounts, and static credentials (Mujtaba et al., 2025; Netz-und, 2021). Lightweight identity solutions fill these gaps. They centralized authentication and support fine-grained access control. Furthermore, they interact well with cloud apps typically utilized by SMEs. In a Zero Trust environment, lightweight identity platforms serve as the primary trust broker, and they make access decisions based on identity assurance, context, and policy. They do this instead of using network location (Rose et al., 2020).

6.2 Cloud-Based IAM and Directory Services

Cloud-based IAM and directory services form the foundation of most lightweight identity solutions. These platforms provide centralized user directories, authentication services, and policy enforcement without requiring on-premises infrastructure. Empirical studies show that cloud IAM adoption significantly improves security posture for small organizations by enabling consistent enforcement of authentication policies across diverse applications and devices (Taşan-Kok, 2025; Kang et al., 2023). By outsourcing identity infrastructure management to cloud providers, SMEs can reduce maintenance costs while benefiting from continuous security updates and high availability.

From a Zero Trust perspective, cloud IAM platforms enable identity to act as the primary security perimeter. Authentication requests are evaluated centrally, often incorporating MFA, device trust signals, and contextual

risk assessments before access is granted (Rose et al., 2020). Directory services within these platforms support lifecycle management functions such as user onboarding, role assignment, and deprovisioning, which are critical for enforcing least privilege and reducing the risk of orphaned accounts. However, reliance on cloud IAM also introduces dependencies on vendor availability and correct configuration, reinforcing the need for careful policy design even in lightweight deployments (Baig & Eskeland, 2021).

6.3 Security and Operational Limitations

Despite their advantages, lightweight identity solutions introduce security and operational limitations that must be considered carefully. Centralizing identity services increases the impact of misconfiguration, as incorrect policies or excessive privileges can propagate across multiple applications simultaneously (Taşan-Kok, 2025). Studies on usable security indicate that administrators in small organizations often prioritize convenience over strict policy enforcement, which may undermine the theoretical security benefits of centralized IAM (Baig & Eskeland, 2021). Vendor dependency is another concern, as cloud IAM platforms represent a single point of control and potential failure. Outages, service changes, or pricing shifts can disproportionately affect SMEs with limited bargaining power (für Netz-und, 2021). These risks are addressed in in the next section through an integrated Zero Trust approach that combines lightweight identity platforms with MFA and short-lived certificates, ensuring centralized control without creating single points of failure.

7. INTEGRATED ZERO TRUST ARCHITECTURE FOR SMES

This section explains how SMEs can combine short-lived certificates, MFA, and lightweight identity solutions into a unified Zero Trust framework. It emphasizes identity as the trust anchor, MFA for strong authentication, and ephemeral credentials for ongoing access. Automation is highlighted as critical for reducing administrative overhead, while continuous verification and context-aware policies ensure adaptive, least-privilege access. The approach balances strong security with SME constraints by centralizing identity management and enforcing dynamic policies without enterprise-level complexity.

7.1 Combining Certificates, MFA, and Identity

An effective Zero Trust architecture for SMEs emerges not from isolated controls, but from the coordinated integration of identity management, multi-factor authentication, and short-lived credentials into a unified access control framework. Identity serves as the primary trust anchor, while MFA strengthens identity assurance at authentication time, and short-lived certificates provide ephemeral, cryptographically strong credentials for ongoing access. Together, these mechanisms operationalize the Zero Trust assumption that access should be temporary, contextual, and continuously validated rather than implicitly trusted (Rose et al., 2020; Garbis & Chapman, 2021).

In practical SME deployments, this integration typically begins with a centralized cloud-based identity provider that authenticates users using MFA. Upon successful authentication and policy evaluation, the system issues short-lived certificates or tokens that are scoped to specific resources and privileges. These credentials are then used for mutual authentication between users, devices, and services, enabling fine-grained access control without exposing long-lived secrets (Sakimura et al., 2021; Kang et al., 2023). This approach significantly reduces the attack surface by ensuring that even if credentials are intercepted, their usefulness is limited in scope and time. For SMEs, the key architectural advantage lies in automation: certificate issuance, rotation, and revocation are handled transparently by the identity platform, minimizing administrative overhead while maintaining strong security guarantees.

7.2 Policy Enforcement and Continuous Verification

Policy enforcement is the mechanism through which Zero Trust principles are translated into operational security decisions. In an integrated Zero Trust architecture, access policies are defined centrally and enforced consistently across applications, devices, and users. These policies encode conditions such as required authentication strength, permitted devices, time-of-day restrictions, and resource sensitivity (Mehra, 2024; Rose et al., 2020). Unlike traditional access control models, where policy enforcement is often static and

network-based, Zero Trust policies are evaluated dynamically at each access request and continuously throughout the session.

Continuous verification is particularly important in SME environments, where monitoring capabilities may be limited, and detection delays are common. Research shows that attackers frequently maintain persistence by exploiting long-lived sessions and static credentials that are rarely revalidated (Mansfield-Devine, 2022). By enforcing re-authentication, certificate renewal, or contextual re-evaluation at defined intervals or upon risk changes, Zero Trust architectures limit attacker dwell time and reduce the likelihood of lateral movement (Homoliak et al., 2019). For SMEs, continuous verification does not require constant user interaction; instead, it is achieved through background checks such as certificate expiration, device posture reassessment, and policy re-evaluation, preserving usability while strengthening security.

7.3 Access Decisions Based on Identity, Device, and Context

In Zero Trust systems, access decisions are multi-dimensional and context-aware, relying on a combination of identity attributes, device trust signals, and environmental context. Identity attributes include user roles, authentication strength, and credential freshness, while device signals may encompass operating system version, security posture, or management status (Rose et al., 2020). Contextual factors such as geographic location, network characteristics, and behavioral patterns further inform risk-based access decisions (Borah, 2015). This layered evaluation enables more precise enforcement of least privilege compared to binary allow-or-denied models.

For SMEs, context-aware access control provides a way to compensate for limited perimeter defenses and monitoring infrastructure. Studies indicate that many successful SME breaches occur because access controls fail to adapt to changing risk conditions, such as compromised devices or anomalous login behavior (für Netz- und, 2021). By integrating identity, device, and context into a single decision pipeline, Zero Trust architectures allow SMEs to deny or restrict access dynamically when risk increases, even if initial authentication was successful. This adaptive capability is central to reducing the impact of credential compromise and aligns closely with the practical realities of SME threat environments.
Table 4 maps core Zero Trust principles to concrete controls that SMEs can realistically implement using integrated identity-centric architectures.

Table 4. Mapping Zero Trust principles to practical SME controls

Zero Trust principle	Practical SME control	Enabling technology
Never trust, always verify	Mandatory MFA for all access	Cloud IAM, MFA
Least privilege	Role- and resource-scoped access	Centralized identity policies
Assume breach	Short-lived credentials	Certificate automation
Continuous verification	Session re-evaluation and renewal	Context-aware access control
Identity as perimeter	Centralized authentication	Cloud-based IdP
Minimize blast radius	Micro-segmentation	Policy enforcement points

8. CHALLENGES, GAPS, AND OPEN ISSUES

Zero Trust adoption in SMEs involves both practical implementation challenges and unresolved research questions. While identity-centric controls provide measurable security benefits, their effectiveness in small and medium-sized organizations is constrained by financial limitations, legacy infrastructure, usability concerns, and limited operational capacity. Prior studies note that many Zero Trust models are implicitly designed around enterprise-scale assumptions, leaving SMEs with guidance that is conceptually sound but operationally difficult to implement (Rose et al., 2020). This section distinguishes between practitioner challenges, research gaps, and open issues that remain insufficiently addressed in current literature.

8.1 Practitioner Challenges

Cost remains a dominant challenge for SMEs adopting Zero Trust architectures. Although cloud-based identity services reduce capital expenditure, subscription pricing, tiered feature models, and add-on security

services introduce long-term cost uncertainty. Empirical analyses show that SMEs often delay or partially implement Zero Trust controls due to concerns about recurring costs and unpredictable scaling expenses (Fürst & Netz, 2021; Mensah, F., 2024). Vendor lock-in further exacerbates this issue, as tightly coupled identity platforms increase switching costs and reduce architectural flexibility over time (Taşan-Kok, 2025). Legacy systems present a persistent barrier to identity-centric Zero Trust adoption. Many SMEs operate older applications that lack support for modern authentication standards such as SAML, OAuth, or certificate-based access. These systems often rely on static credentials and coarse-grained authorization, forcing organizations to maintain parallel security models that undermine architectural consistency (Mehra & Kumar, 2024). As temporary compatibility solutions accumulate, technical debt increases, expanding the attack surface and weakening Zero Trust enforcement.

User adoption also significantly influences Zero Trust effectiveness. Studies in authentication usability consistently demonstrate that insufficient training, unclear communication, and poorly designed MFA workflows lead to resistance, misuse, or circumvention of controls (Baig & Eskeland, 2021; Kollek et al., 2025). SMEs frequently lack structured security awareness programs, increasing the likelihood that users perceive Zero Trust measures as obstacles rather than protections. Without usability-focused design and targeted training, identity controls may fail to deliver their intended risk reduction.

Identity centralization introduces additional operational risk. While centralizing authentication and policy enforcement simplifies access management, it also magnifies the impact of configuration errors or service outages. Research highlights that misconfigurations in identity providers can create organization-wide access failures, particularly when compensating controls and staged policy validation are absent (Rose et al., 2020). For SMEs with limited security staffing, managing this concentration of risk remains challenging.

Limited monitoring capacity further shapes Zero Trust deployment in SME environments. Unlike large enterprises, SMEs often lack continuous security monitoring or dedicated incident response teams, leading to delayed detection and extended attacker dwell time. Consequently, Zero Trust implementations in SMEs must rely more heavily on preventive controls such as short-lived credentials, session re-evaluation, and continuous authentication rather than post-compromise detection.

8.2 Research Gaps

Despite increasing Zero Trust adoption, several research gaps persist, particularly for SME contexts. Automation is widely recognized as essential for sustaining Zero Trust, yet the literature provides limited prescriptive guidance on lightweight automation frameworks suitable for small teams. Areas such as certificate issuance, credential rotation, and identity lifecycle management remain underexplored for organizations without specialized security personnel (Mensah, F., 2024).

Usability-focused Zero Trust research remains limited. Existing studies tend to emphasize cryptographic strength and protocol security while giving insufficient attention to user experience and operational friction. There is a lack of empirical evaluation of MFA flows, continuous authentication mechanisms, and certificate-based access models that balance phishing resistance with usability in SME environments (Baig & Eskeland, 2021; Kollek et al., 2025).

Hybrid deployment models for legacy integration also represent a significant research gap. While incremental modernization is frequently recommended, formalized migration playbooks that preserve Zero Trust principles in mixed environments are scarce. Research has yet to establish validated architectural patterns for integrating legacy applications through gateways, protocol translation, or conditional access without weakening overall security posture (Mehra & Kumar, 2024).

Risk-adaptive access control represents another underdeveloped area. Although AI-driven authentication and dynamic risk scoring are increasingly discussed, most evaluations focus on large enterprises with extensive telemetry and analytics infrastructure. The cost, data requirements, explainability, and operational feasibility of these approaches for SMEs remain largely unexplored (Mensah, F., 2024).

Machine-identity lifecycle management at SME scale is similarly underrepresented. While short-lived credentials and mutual authentication are central to Zero Trust, practical guidance on issuance frequency, scope, renewal cadence, and monitoring remains fragmented. Existing work rarely addresses how SMEs can operationalize these practices without increasing complexity or administrative overhead (Rose et al., 2020).

8.3 Open Issues and Future Study Priorities

The convergence of practitioner challenges and research gaps highlights several open issues that warrant further investigation. Cost–benefit models are needed to help SMEs quantify the return on investment of Zero Trust adoption across licensing costs, automation effort, and reductions in breach impact. Vendor-neutral reference architectures should be developed to define minimal, interoperable identity-centric building blocks that reduce long-term lock-in risk.

Further work is required to establish validated usability patterns for MFA and certificate-based authentication that reduce friction while maintaining phishing resistance. Legacy-compatible modernization playbooks must be formalized to support phased Zero Trust adoption in mixed environments. In addition, lightweight risk-adaptive policy mechanisms should be evaluated for feasibility in SME contexts, with explicit consideration of operational constraints (Taşan-Kok, 2025).

Finally, outcome-oriented evaluation frameworks are needed to assess Zero Trust effectiveness in SMEs. Metrics such as attacker dwell time, lateral movement containment, credential lifetime reduction, and session renewal efficacy should be standardized and empirically tested in realistic SME deployments. Addressing these open issues is essential for translating Zero Trust from an enterprise-oriented concept into a practical and sustainable security strategy for small and medium-sized organizations (für Netz-und, 2021).

9. FUTURE DIRECTIONS

As SMEs continue to adopt identity-centric Zero Trust architectures, emerging technologies offer opportunities to strengthen security and reduce operational complexity. However, these innovations are still evolving and present both promise and uncertainty. This section explores future directions that could reshape Zero Trust implementation, including decentralized identity models, AI-driven authentication, and ongoing standardization efforts. Each of these approaches introduces potential benefits such as enhanced privacy, adaptive risk scoring, and improved interoperability, but they also carry limitations related to maturity, tooling, and integration feasibility. For SMEs, understanding these trends is critical for strategic planning, ensuring that adoption decisions remain grounded in practical realities rather than speculative expectations.

9.1 Decentralized Identity and Verifiable Credentials

Decentralized identity (DID) and verifiable credentials represent a promising evolution of identity-centric security models. These approaches shift identity control from centralized providers to cryptographically verifiable credentials held by users or devices, reducing reliance on single trust authorities (Allen et al., 2020). For SMEs, decentralized identity could reduce vendor dependency while enhancing privacy and interoperability within Zero Trust frameworks. However, it is important to note that DID adoption remains largely experimental for SMEs, with limited tooling and integration support currently available. Organizations should approach these technologies cautiously, viewing them as future-oriented options rather than immediate solutions."

9.2 AI-Driven Authentication and Risk Scoring

Artificial intelligence and machine learning are increasingly applied to authentication and access control through behavioral analysis and dynamic risk scoring. Research suggests that AI-driven models can detect anomalous behavior more effectively than static rules, enabling adaptive authentication decisions that strengthen Zero Trust enforcement without increasing user friction (Homoliak et al., 2019). For SMEs, these techniques offer the potential to compensate for limited security monitoring resources.

9.3 Standardization and Policy Evolution

Ongoing standardization efforts will play a critical role in shaping the future of Zero Trust adoption. Frameworks such as NIST SP 800-207 provide foundational guidance, but further refinement is needed to address SME-specific deployment patterns and interoperability challenges (Rose et al., 2020). Policy evolution must also consider regulatory requirements, privacy concerns, and cross-border data access, particularly as SMEs increasingly operate in global digital ecosystems.

CONCLUSION

In conclusion, this review outlines identity-centric Zero Trust measures that offer SMEs a practical and effective approach to strengthening cybersecurity, despite resource limitations. The analysis confirms that short-lived certificates significantly reduce credential exposure by limiting validity periods and eliminating the need for complex revocation mechanisms. Multi-factor authentication (MFA) is one of the most impactful and accessible controls, and it helps prevent phishing and limits damage from credential reuse. These attacks are common in SME environments. Lightweight identity solutions can also help. Cloud-based IAM platforms centralize authentication and enforce policies. They do this without needing enterprise-scale infrastructure. This reduces admin workload and improves security consistency. Collectively, these mechanisms operationalize Zero Trust principles such as continuous verification, least privilege, and identity as the primary security perimeter. Automation is identified as a critical enabler, transforming certificate management and policy enforcement from complex tasks into streamlined processes suitable for SMEs. However, adoption challenges remain, including cost constraints, legacy system integration, and user resistance, which must be addressed through phased deployment, usability-focused design, and training. Looking forward, emerging technologies such as decentralized identity and AI-driven risk scoring offer promising avenues for enhancing Zero Trust in SME environments. By embracing these identity-driven controls and planning for future innovations, SMEs can achieve a level of cyber resilience comparable to larger enterprises, reducing the impact of credential-based attacks and improving overall security posture within practical resource constraints.

REFERENCES:

1. Ahmed, Z., Filani, A., Osifowokan, A. S., & Hutchful, N. (2025). The Impact of Data Breaches in US Healthcare: A Cost-Benefit Analysis of Prevention vs. Recovery.
2. Ahmed, Z., Osifowokan, A. S., Filani, A., & Donkor, A. A. Comprehensive analysis of cyber attacks and data breaches in the US health sector: Identifying vulnerabilities and developing proactive defense strategies.
3. Anderson, R., Barton, C., Bölme, R., Clayton, R., Ganán, C., Grasso, T., ... & Vasek, M. (2019). Measuring the changing cost of cybercrime.
4. Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour?. *arXiv preprint arXiv:1901.02672*.
5. Baig, A. F., & Eskeland, S. (2021). Security, privacy, and usability in continuous authentication: A survey. *Sensors*, *21*(17), 5967.
6. Borah, C. K. (2015). Cyber war: the next threat to national security and what to do about it? by Richard A. Clarke and Robert K. Knake.
7. Cherekar, R. (2025, February). Comparative Analysis of Password Alternatives for Enterprise Authentication: A Case Study. In *2025 IEEE 4th International Conference on AI in Cybersecurity (ICAIC)* (pp. 1-8). IEEE.
8. für Netz-und, E. U. A. (2021). *Cybersecurity for SMEs: challenges and recommendations*. ENISA.
9. Garbis, J., & Chapman, J. W. (2021). *Zero trust security: An enterprise guide* (p. 324). Berkeley, CA: Apress.
10. Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y., & Ochoa, M. (2019). Insight into insiders and it: A survey of insider threat taxonomies, analysis, modeling, and countermeasures. *ACM Computing Surveys (CSUR)*, *52*(2), 1-40.
11. Kang, H., Liu, G., Wang, Q., Meng, L., & Liu, J. (2023). Theory and application of zero trust security: A brief survey. *Entropy*, *25*(12), 1595.
12. Kollek, T. (2025). Putting Paranoia into Practice: Information Security for Ethnographers in Authoritarian Contexts. *Communist and Post-Communist Studies*, 1-21.

13. Lee, S., Huh, J. H., & Woo, H. (2025). Security System Design and Verification for Zero Trust Architecture. *Electronics*, *14*(4), 643.
14. Mansfield-Devine, S. (2022). Verizon: Data breach investigations report.
15. Mehra, T. (2024). The Critical Role of Role-Based Access Control (RBAC) in securing backup, recovery, and storage systems. *International Journal of Science and Research Archive*, *13*(01), 1192-1194.
16. Mensah, F. (2024). Zero trust architecture: A comprehensive review of principles, implementation strategies, and future directions in enterprise cybersecurity. *International Journal of Academic and Industrial Research Innovations (IJAIRI)*, *10*, 339-346.
17. Mujtaba, A., Alam, A., & Kamran, M. (2025). Cybersecurity challenges in small and medium enterprises: A scoping review. *Journal of Cyber Security and Risk*, *2025*(3), 89-102.
18. Nnadi, K., & Opoku, J. A. (2025). *Cybersecurity curriculum alignment with industry needs: A literature review of educational models integrating labs, certifications, and research*. *Sarcouncil Journal of Engineering and Computer Sciences*, *4*(12), 1–20. https://sarcouncil.com/2025/12/cybersecurity-curriculum-alignment-with-industry-needs-a-literature-review-of-educational-models-integrating-labs-certifications-and-research
19. Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-factor authentication: A survey. *Cryptography*, *2*(1), 1.
20. Pandey, P., Shukla, S., & Chaurasiya, P. K. (2023, December). Loopholes of Two-Factor Authentication and the Rise of Multi-factor Authentication. In *International Conference on Future Power Network and Smart Energy Systems* (pp. 185-207). Singapore: Springer Nature Singapore.
21. Panful, B., Apaflo, B., & Hutchful, N. (2025). *Cyber-physical systems under threat: A case-study review of recent SCADA attacks in the U.S. utility sector*. *Sarcouncil Journal of Engineering and Computer Sciences*, *4*(12), 104–117. https://sarcouncil.com/2025/12/cyber-physical-systems-under-threat-a-case-study-review-of-recent-scada-attacks-in-the-us-utility-sector
22. Panful, B., Apaflo, B., & Hutchful, N. (2026). *From compliance to culture: Assessing organizational cybersecurity readiness in public vs. private U.S. utility companies*. *EPRA International Journal of Research & Development (IJRD)*, *11*(1). https://doi.org/10.36713/epra25731
23. Panful, B., Apaflo, B., Filani, A., Nnadi, K., & Hutchful, N. (2025). *Human factor vulnerabilities in energy industry cybersecurity: Assessing employee awareness and behavior in breach prevention*. *International Journal for Multidisciplinary Research (IJFMR)*, *7*(6), 1–18. https://www.ijfmr.com/papers/2025/6/63932.pdf
24. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. *Zero trust architecture. NIST SP 800-207, 2020*.
25. Roy, A., Banerjee, A., & Bhardwaj, N. (2021). A study on Google Cloud Platform (GCP) and its security. *Machine Learning Techniques and Analytics for Cloud Security*, 313-338.
26. Sakimura, N., Bradley, J., & Jones, M. (2021). RFC 9101: The OAuth 2.0 Authorization Framework: JWT-Secured Authorization Request (JAR).
27. Seng, Y. J., Cen, T. Y., bin Mohd Raslan, M. A. H., Subramaniam, M. R., Xin, L. Y., Kin, S. J., ... & Sindiramutty, S. R. (2024). In-depth analysis and countermeasures for ransomware attacks: Case studies and recommendations.
28. Taşan-Kok, T. (2025). Navigating the city: Role of property-market intelligence channels in urban governance networks. *European Urban and Regional Studies*, *32*(2), 197-220.
29. Tetteh-Kpakpah, C., Adjaottor, S., & Donkor, A. A. MITIGATING CYBER THREATS THROUGH CYBERSECURITY AUDITS AND ADAPTIVE DEFENSE: A CASE STUDY ON FINANCIALIN STITUTIONS. *Chief Editor*.
30. Wang, Z., Lin, J., Cai, Q., Wang, Q., Zha, D., & Jing, J. (2020). Blockchain-based certificate transparency and revocation transparency. *IEEE Transactions on Dependable and Secure Computing*, *19*(1), 681-697.